Cuadernillo de análisis sobre:

Estudio sobre las implicaciones jurídicas del uso de cómputo en la nube por el sector público mexicano.

Recopilación de estándares y buenas prácticas de fuente internacional

Autores:

Ezequiel González Matus

Liliana Martín Herrera

Coordinador del proyecto:

Israel Santos Flores

Contenido

Introducción

Este es un estudio regulatorio acerca de los servicios de cómputo en la nube desde una perspectiva de derecho comparado.

El enfoque comparado es una herramienta metodológica que permite comprender mejor los fenómenos jurídicos de nuestro tiempo, más cuando estos corresponden a ámbitos del dinámico desarrollo tecnológico.

El análisis comparado ayuda a situar en tiempo y espacio nuestro objeto de estudio, sin abandonar la visión jurídica. En particular, al abordar la temática de la regulación de la *nube*, la perspectiva comparada ilustra sobre la evolución y el estado actual, en términos globales, de la construcción jurídica de un aspecto altamente sofisticado de la tecnología.

Analizaremos jurisdicciones lejanas, inmersas en distintas circunstancias económicas, culturales y desde luego científicas. Ello nos permitirá identificar dilemas y tendencias, con el propósito de generar alternativas jurídicamente viables para la implementación de la nube en el sector público de México.

La *Nube*, a la que la literatura especializada -jurídica y no jurídica- alude también como *Cómputo en la nube*, *Cloud* o *Cloud computing*, es un fenómeno jurídico novedoso. La economía, la gestión del gobierno, el intercambio comercial y la vida cotidiana tienen una profunda dependencia en la información y los datos. Por ello, un estudio académico de corte jurídico sobre la nube necesita aproximarse al fenómeno jurídico a partir de la comprensión de su alcance en la realidad humana de nuestro siglo.

Por tales motivos seguiremos las siguientes líneas de estudio:

a) El concepto de nube en su entendimiento jurídico, pero también en sus distintas formas de implementación práctica.

b) Los dilemas jurídicos implicados en el uso de la nube en general y en particular para el sector público, como destacadamente son la libre

circulación de datos y los derechos de las personas respecto del uso de sus datos personales.

c) Los sistemas o modelos regulatorios desarrollados en jurisdicciones relevantes, dentro de las cuales realizaremos un análisis regional de América del Norte, Europa y Asia.

Como resultado, presentaremos conclusiones y recomendaciones que estimamos razonables para la implementación de la nube en el sector público mexicano.

Una premisa fundamental que debemos subrayar es esta: la regulación de la nube ha tenido un preeminente desarrollo en ámbitos del *soft law*, es decir en espacios de regulación industrial y sectorial, mediante la implementación de estándares tecnológicos y de cumplimiento; mientras que en el terreno legislativo ha tenido una evolución más pausada, que ciertamente con no poca frecuencia se ve rebasada por los avances informáticos y tecnológicos.

En realidad, el estado regulatorio de la nube indica que actualmente en el mundo no predominan las leyes sobre la nube, sino reglas sectorizadas sobre la implementación del cómputo en la nube; y ordenamientos en materia de privacidad y protección de datos que eventualmente imponen condiciones para el uso de la nube.

No tenemos duda de que el reto regulatorio es uno de los más complejos de nuestro tiempo, pues sustancialmente consiste en generar normas jurídicas estables y certeras, para regir un ámbito tecnológico por naturaleza dinámico, multiterritorial y en constante expansión.

Reconocemos que no hay modelos regulatorios únicos ni soluciones legales definitivas, pero también asumimos que la perspectiva de derecho comparado proporcionará herramientas útiles para que los agentes del sector público analicen las distintas aproximaciones jurídicas a nuestro objeto de estudio y eventualmente puedan implementar el modelo más eficaz para responder a las necesidades y circunstancias de México.

Conceptos fundamentales.

En 2021 el uso de la nube a nivel global está presente en los sectores público y privado, como los servicios tecnológicos, financieros, educativos y de salud, la gestión gubernamental, las telecomunicaciones, el comercio y la industria en general.[1]

La nube implica elementos como redes, servidores, equipos de almacenamiento, aplicaciones y servicios a través de Internet, mediante un esquema de pago por uso.

La definición más relevante y acreditada de la nube es la que proviene de NIST, es decir del *National Institute of Standards and Technology,* de los Estados Unidos de América,[2] que conceptualiza al cómputo en la nube como un modelo tecnológico que permite el acceso ubicuo, adaptado y bajo demanda a un conjunto compartido de recursos de computación configurables, que pueden ser rápidamente provisionados y liberados con un esfuerzo de gestión reducido o interacción mínima con el proveedor del servicio.

En una acepción más asequible, los servicios utilitarios de cómputo en la nube entrañan la idea de recursos tecnológicos prestados a través de Internet, ajustables a las necesidades del usuario tanto en su alcance como en su costo. En ello, desde luego, está implicada una relación jurídica contractual entre el prestador del servicio y el usuario de la nube.

Conforme al concepto de NIST, la nube tiene cinco características esenciales, tres modelos de servicio y cuatro modelos de implementación.

Así, las características esenciales del cómputo en la nube son las siguientes:

---

[1] Flexera. *2021 State of the Cloud Report*. 2021.
[2] Mell, Peter y Grance, Timothy. *The NIST Definition of Cloud Computing.* National Institute of Standards and Technology. U.S. Department of Commerce. E.U.A. 2011.

On-demand self-service* o *autoservicio bajo demanda; que significa que un consumidor puede aprovisionar unilateralmente, para sí mismo, las capacidades informáticas que desea, como son el tiempo del servidor y el almacenamiento en red; sin requerir interacción humana con el proveedor del servicio.

Broad network access* o *acceso amplio a la red; que quiere decir que las capacidades de la nube están disponibles a través de la red y se accede a ellas a través de mecanismos estándar como por ejemplo, teléfonos móviles, tabletas, computadoras portátiles y estaciones de trabajo.

Resource pooling* o *agrupación de recursos; esto es que los recursos informáticos del proveedor se agrupan para atender a varios consumidores mediante un modelo de múltiples inquilinos, con diferentes recursos físicos y virtuales asignados dinámicamente de acuerdo con la demanda de cada consumidor.

Rapid elasticity* o *elasticidad rápida; que significa que las capacidades de la nube se pueden aprovisionar y liberar elásticamente, en algunos casos automáticamente, para escalar rápidamente de acuerdo con la demanda.

Measured service* o *servicio medido; lo que quiere decir que los sistemas en la nube controlan y optimizan automáticamente el uso de recursos, de acuerdo al tipo de servicio (por ejemplo, almacenamiento, procesamiento, ancho de banda y cuentas de usuario activas). Además, el uso de recursos se puede monitorear, controlar y reportar, proporcionando transparencia tanto para el proveedor como para el consumidor del servicio.

Por otro lado, también conforme a NIST, los tres modelos de servicio de la nube son:

Software as a Service (SaaS)* o *Software como servicio (SaaS); que consiste en que la capacidad proporcionada al consumidor es para

utilizar las aplicaciones del proveedor que se ejecutan en una infraestructura en la nube.

Platform as a Service (PaaS)* o *Plataforma como servicio (PaaS); que es la capacidad proporcionada al consumidor para implementar en la infraestructura de la nube aplicaciones creadas o adquiridas por el consumidor, pero que sean compatibles con el proveedor de la nube.

Infrastructure as a Service (IaaS) o Infraestructura como servicio (IaaS); que es la capacidad proporcionada al consumidor para el procesamiento, almacenamiento, redes y otros recursos informáticos donde el consumidor puede implementar y ejecutar software arbitrario, que puede incluir sistemas operativos y aplicaciones; es decir que el consumidor tiene control sobre los sistemas operativos, el almacenamiento y las aplicaciones implementadas.

Finalmente, NIST postula la existencia de cuatro modelos de implementación de la nube:

***Private cloud* o Nube privada**, que es un modelo en el que la infraestructura de la nube se proporciona para uso exclusivo de una sola organización.

***Community cloud* o Nube comunitaria**, que consiste en que la infraestructura de la nube está provista para uso exclusivo, pero compartido, de una comunidad específica de consumidores, que tienen cometidos comunes.

***Public cloud* o Nube pública**, que es el modelo en el que la infraestructura de la nube está provista para uso abierto del público en general.

***Hybrid cloud* o Nube híbrida**, que constituye un modelo en el que la infraestructura de la nube es resultante de una composición de dos o más infraestructuras distintas (privadas, comunitarias o públicas) que se mantienen como entidades únicas, pero que están unidas por una tecnología

estandarizada o patentada que permite la portabilidad de datos y aplicaciones.

La nube, sin duda, reduce las barreras de entrada a la tecnología. En el ámbito gubernamental, el cómputo en la nube es un factor de implementación efizaz y eficiente de programas públicos; mientras que en el sector privado la nube facilita el intercambio de bienes y servicios.

El proceso de transición de modelos de infraestructura propia o *in-house* hacia la implementación del cómputo en la nube, recibe el nombre de *cloud migration.*

Esa transformación tecnológica, bien en entidades públicas o privadas, generalmente acontece en forma gradual; lo que permite que las organizaciones adopten los servicios y los beneficios de la nube por fases que responden a sus propias necesidades de desarrollo y a su dinámica de aprendizaje interno.

La generalidad de los referentes en la materia indica que los beneficios principales de la nube son los siguientes:

- Reducción de costos.
- Multialquiler de servicios.
- Operaciones mejoradas.
- Tecnologías de seguridad avanzadas.
- Control de la privacidad.
- Software libre.
- Sistemas distribuidos geográficamente.
- Transferencia de riesgos al proveedor de servicios de la nube.
- Ahorro de tiempo.
- Disponibilidad y continuidad mejoradas.
- Escala masiva.
- Virtualización.
- Transparencia.
- Crecimiento de negocios.

Además, dentro de los factores que distinguen la seguridad de la nube se encuentran los siguientes, de acuerdo con la *Asia Cloud Computing Association*:[3]

a) Altos niveles de encriptación.

b) Los centros de datos de los proveedores de servicios de nube cuentan con múltiples niveles de seguridad física y lógica, así como controles de acceso.

c) Los proveedores de servicios de nube usualmente tienen capacidad de actualizar sus esquemas de seguridad.

En particular, por lo se refiere a la materia de nuestro estudio, la implementación de la nube en el sector público permite a las agencias de gobierno optimizar su gasto en tecnologías de la información y enfocar sus esfuerzos en la prestación de servicios públicos.

La discusión, sin embargo, va más allá de costos y seguridad de la información.

Poner en marcha la nube en el sector público implica el desarrollo de normas jurídicas, pero sobre todo el reconocimiento y despliegue de políticas públicas alineadas a la política pública denominada "*Cloud first*".

En el análisis de fuentes internacionales destacan siete principios postulados por la *Asia Cloud Computing Association* (*ACCA*) como premisas para asentar el uso de la nube en el sector público. Se trata de postulados agrupados en tres rubros, de la siguiente manera:[4]

1. La protección del gobierno.

Los principios postulados en este aspecto tienen el propósito de resolver las inquietudes de los gobiernos nacionales acerca de la seguridad de la información

[3] Asia Cloud Computing Association. From vision to procurement: principles for adopting cloud computing in the public sector. 2019. Página 10.
[4] Asia Cloud Computing Association. *From vision to procurement: principles for adopting cloud computing in the public sector*. 2019.

alojada en la nube, el tratamiento de datos personales y el cumplimiento de las leyes en materia de privacidad:

Principio 1.- Seguridad

Este es un principio conforme al cual se enfatiza que la seguridad de los sistemas de tecnología de la información es esencial para desplegar soluciones en la nube por parte de las entidades de gobierno.

Principio 2.- Privacidad e información personal.

Bajo la premisa de que las entidades gubernamentales poseen gran cantidad de información personal, las soluciones que aporta la nube representan un incremento a las medidas de protección y control necesarias para contar con la confianza de los ciudadanos. Los gobiernos, por tanto, requieren garantías en el sentido de que los derechos a la privacidad y protección de datos se encuentran a salvo en el uso de la nube por parte del sector público.

Principio 3.- Disponibilidad, integridad y resiliencia.

La nube resuelve, a la par, la necesidad de los órganos públicos de contar con información disponible en tiempo real y la exigencia de la ciudadanía de que su propia información se mantiene en un entorno confiable y recuperable.

2. **La facilidad de la transición hacia la nube**.

En este tópico, dos principios sirven como guía para alinear las normas jurídicas internas con los parámetros internacionales de cumplimiento regulatorio:

Principio 4.- Cumplimiento regulatorio y de estándares globales.

Los servicios en la nube deben ser evaluados en su calidad y confiabilidad, tomando como punto de referencia estándares internacionales.

Principio 5.- Responsabilidad.

Conforme a este principio, los proveedores de servicios de nube pueden apoyar a los gobiernos en la vigilancia y transparencia de los recursos públicos destinados a la implementación de la nube.

3. La justificación de la nube en el sector público: ¿por qué la nube?

Finalmente, para comprender las oportunidades que ofrece la nube en la transformación del sector público, la *ACCA* plantea dos principios:

Principio 6.- Accesibilidad e inclusión.

En general, el uso de la nube en el sector público puede entenderse como la puerta de entrada a beneficios de largo plazo que implican una transformación radical en la prestación de los servicios públicos, que pueden ser extendidos a un mayor número de personas. Este es el fenómeno denominado "*democratización de las tecnologías de la información*".

Principio 7.- Sustentabilidad.

Finalmente, el uso de la nube en el sector público abona a reducir el consumo de energía en los servicios de tecnología y emisiones de carbón, colaborando así con compromisos internacionales relativos a la gestión ambiental.

Los servicios de cómputo en la nube, por otro lado, no están exentos de riesgos fácticos y jurídicos.

En términos de Peter Mell[5], la computación en la nube tiene ventajas y desventajas de seguridad, pues el modelo de computación en la nube promueve la disponibilidad de servicios a través de su modelo de arquitectura distribuida; sin embargo, este mismo modelo presenta desafíos de confidencialidad e integridad de los datos al agrupar recursos de *hardware* para su uso por múltiples partes.

Los riesgos que usualmente están aparejados al uso de la nube, se pueden agrupar como sigue:

a) Riesgos relativos a la seguridad de la información, en donde se sitúan aquellos como fallas en los sistemas de seguridad establecidos por proveedores de la nube, ataques de Malware o software malicioso, brechas

[5] https://www.nist.gov/news-events/news/2009/05/nist-defining-expanding-world-cloud-computing

de privacidad, pérdida de datos, falta de destrucción o eliminación de la información personal al final de la relación contractual con el proveedor de la nube.

b) Riesgos derivados de las ubicaciones de almacenamiento. Esta clase de riesgos se presentan cuando la información se almacena en regiones geográficas con leyes de privacidad laxas, de modo que los proveedores de la nube tienen pocos controles de seguridad que no cumplen con los estándares establecidos por las autoridades locales.

c) Riesgos legales, que usualmente emanan de cláusulas contractuales deficientes o del incumplimiento de normas de *Compliance* o debida diligencia en el tratamiento de la información por parte del proveedor de la nube.

Desde la perspectiva jurídica, puede decirse que tres pilares sustentan el desarrollo e implementación del cómputo en la nube: a) cumplimiento regulatorio; b) seguridad; y c) privacidad.

La construcción jurídica de la nube implica, entonces, que los proveedores de los servicios se ajusten invariablemente a las normas legales y a las directrices sectoriales y que puedan dar cuenta de ello a los usuarios de la nube. La estandarización por parte de las propias industrias es un elemento central en el régimen de cumplimiento del *Cloud Computing*.

La edificación del modelo jurídico también requiere que los proveedores implementen satisfactoriamente medidas de seguridad de la información alojada en la nube; y que las mismas sean reflejadas contractualmente.

Además, la cimentación del esquema jurídico debe asegurar la implementación de reglas de privacidad, que aporten certeza a los usuarios y a terceras personas acerca del tratamiento de su información personal.

Los servicios de cómputo en la nube, por lo tanto, hacen necesario el desarrollo de un modelo regulatorio complejo, dinámico y altamente especializado,

que responda a los beneficios esperados y a los riesgos latentes en esta rama de la tecnología.

> Los dilemas jurídicos implicados en el uso de la nube en general y en particular para el sector público.

La nube plantea dilemas jurídicos sustantivos, que se relacionan con su concepto, su diseño regulatorio y su aplicación. Se trata de cuestiones que, si bien son novedosas en el terreno del análisis legal, emanan directamente de la alta complejidad tecnológica de los servicios de cómputo en la nube. Estamos en un espacio jurídico donde los dilemas jurídicos son constantes y por lo general no tienen respuestas únicas.

Un primer espacio de análisis en que se enfoca la literatura especializada tiene que ver con la movilidad de los datos en la nube; es decir la libre circulación de los datos en el espacio global, multiterritorial, en que habita la nube.

La segunda cuestión jurídicamente relevante es el tratamiento de los datos personales una vez que ingresan a la nube. Esto significa que para el derecho resulta relevante conocer y resolver cómo ha de ser gestionada la información de las personas en un entorno transaccional prácticamente ilimitado en términos geográficos.

Aquí es donde nuestro estudio reconoce que la problemática jurídica tiene un ineludible punto de toque con la realidad económica: el comercio internacional depende cada vez más del flujo de toda clase de información -financiera, demográfica, personal, industrial, tecnológica, etc.- lo que hace necesario que la nube se afiance como un mecanismo eficaz y seguro para las operaciones globales.

Libre circulación de datos y multiterritorialidad.

La libre circulación de datos es una condición necesaria para la operación de la nube. Este componente es al mismo tiempo una necesidad de índole económico y un requerimiento de orden regulatorio.

La premisa fundamental del análisis es esta: en el entorno global, el uso de la nube implica que la información -datos personales, económicos, estadísticos, gubernamentales, etc.- por lo general se alberga en jurisdicciones separadas; y en la mayoría de los casos, en naciones distintas al país de origen de la información. Es prácticamete inviable pensar que los proveedores de servicios de cómputo en la nube desarrollen infraaestructura en cada país para alojar la información ahí generada.

Es decir, los proveedores de servicios de nube suelen almacenar la información en varias locaciones diferenciadas, bien de manera regional o global, lo cual les permite mejorar su funcionalidad y eficiencia. Por ello, la operación los servicios de cómputo en la nube requiere que la información se encuentre jurídicamente habilitada para circular entre países o regiones.

Permitir el libre flujo de datos a través de las fronteras tiene un impacto positivo en la economía global. Un informe de febrero de 2016 del *McKinsey Global Institute*, estimó que los flujos de datos transfronterizos contribuyeron con casi 2.8 billones de dólares a la economía global en 2014 al permitir el flujo de bienes, servicios y otros recursos. Además, dicho informe estima que esta cifra podría alcanzar los 11 billones de dólares para 2025.[6]

Un ejemplo regional es el *Tratado de Libre Comercio México, Estados Unidos, Canadá* (TMEC), que expresamente reconoce el libre flujo transfronterizo de datos para los propósitos de intercambio comercial digital que persigue el Capítulo 19 .

[6] http://www.ift.org.mx/sites/default/files/dgci_estudio-cloud_computing.pdf

Los flujos de información juegan un papel central en la gestión y seguridad del intercambio de bienes y servicios. Prácticamente todas las industrias se basan en la red global y en la circulación transfronteriza de datos; que son justamente los habilitadores de tecnologías digitales como el *Big Data* y el *Cloud Computing*.

Los países que permiten el libre flujo de datos tienen, sin duda, una ventaja competitiva al acceder a tecnología de vanguardia, lo que a su vez impacta positivamente en la modernización de los servicios comerciales y del sector público. En cambio, los países que restringen los flujos de datos y el comercio digital sufren una clara desventaja competitiva.

Ahora bien, hay que reconocer que una vez que ciertos datos o información cruzan una frontera nacional, es sumamente complejo el reto de garantizar su protección bajo leyes y regulaciones extranjeras.

Aquí es donde adquieren relevancia dos conceptos: la *soberanía de datos* y el *requisito de localización de los datos*.

El primero de ellos, la *soberanía de datos,* se refiere a la idea de que la información o los datos alojados en la nube por principio están sujetos a la legislación del lugar en el que fueron recabados.

El riesgo aparejado a este primer concepto se expresa así: una vez alojada la información en la nube y resguardada en una jurisdicción distinta a la de su recaudación, surge el riesgo de que pueda ser sustraida. Por ello, ciertas posturas restrictivas plantean reglas conforme a las cuales la información alojada en la nube se mantenga bajo una única jurisdicción, a saber, la del país en donde se recaban los datos.

Por otra parte, cuando se habla del *requisito de localización de los datos* debe entenderse que en algunos países se ha estipulado la exigencia de localización de los datos, lo que se traduce en la obligación de que cierta información permanezca en determinado espacio territorial. La justificación de ello -se dice- está en la necesidad de custodiar la información respecto de fenómenos eventualmente

adversos, como pueden ser los desastres naturales o los daños causados por la actividad humana.

Visto en términos prácticos, estos son elementos que dificultan el funcionamiento eficaz y eficiente de la economía basada en la carretera de los datos.

Las restricciones de flujo de datos transfronterizos pueden adoptar varias modalidades, como las siguientes:

- Que los datos no se puedan transferir fuera de las fronteras nacionales.
- Que los datos se puedan transferir fuera de las fronteras nacionales, pero se deba mantener una copia a nivel nacional.
- Que se requiera el consentimiento previo antes de que se permitan las transferencias globales.

Las naciones promotoras de medidas restrictivas del flujo de datos, argumentan que persiguen cinco finalidades:

a) La privacidad de los datos.
b) La ciberseguridad.
c) La aplicación de la ley local.
d) Proteger a las empresas nacionales de la competencia extranjera.
e) Nivelar el campo de juego en la competencia económica entre jugadores digitales y no digitales.

El problema se expresa con claridad en términos de la *Asia Cloud Computing Association*: los requisitos de soberanía de datos y localización, en casi cualquier forma, tienen el potencial de impactar negativamente el crecimiento, la inversión extranjera directa, el desarrollo social y la productividad económica.[7]

[7] Asia Cloud Computing Association. *Cross-Border data Flows: A review of the regulatory enablers, blockers, and key sectoral opportunities in five asian economies: India, Indonesia, Japan, the Philiphines, and Vietnam.* 2018.

Dicha asociación sostiene que los requisitos de localización de datos a menudo se promulgan debido a la obligación de los gobiernos de proteger la privacidad de los ciudadanos y los datos confidenciales. Este es el caso de los sectores financiero y sanitario, por ejemplo.

Las principales preocupaciones jurídicas en relación con el flujo transfronterizo de datos implican tres tramos de control regulatorio: a) si las leyes de la jurisdicción donde se recopilaron los datos permiten el flujo hacia otras jurisdicciones; b) si las leyes de la jurisdicción donde se recopilaron los datos son aplicables a la transferencia de datos hacia otra jurisdicción; y c) si las leyes de la jurisdicción destino presentan riesgos o beneficios adicionales para la protección de la información.[8]

Tales puntos de incertidumbre adquieren mayor relevancia tratándose del flujo transfronterizo de datos sensibles.

La respuesta jurídica más eficaz parece apuntar en dos sentidos: que los gobiernos nacionales se encaminen hacia el facilitamiento jurídico del libre flujo de datos y que los proveedores de servicios de cómputo en la nube garanticen contractualmente que los datos se almacenarán y procesarán solo dentro de jurisdicciones específicas, con alcances suficientes para proteger la información y la propiedad de la misma por parte de la entidad contratante.

En particular, en el caso del sector público, no puede perderse de vista que los gobiernos contratantes de servicios de nube necesitan tener la seguridad de que la información está protegida respecto de terceras personas de naturaleza privada, pero también de otros gobiernos nacionales.

Finalmente, en lo que respecta al uso de la nube en el sector público, es relevante el planteamiento de *Amazon Web Services* a partir de la premisa de que el factor de residencia de los datos lleva aparejados ciertos riesgos de seguridad.

---

[8] Wayne A. Jansen, NIST. Cloud Hooks: Security and Privacy Issues in Cloud Computing
https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906716

En este aspecto, el enfoque de *Amazon Web Services* sugiere seis puntos que los gobiernos nacionales habrían de considerar respecto a la seguridad asociada con la residencia de los datos:[9]

1. Desarrollar políticas y requisitos que permitan el uso de instalaciones de procesamiento de datos fuera del país si los datos se procesan y almacenan en un entorno de nube de hiperescala moderno y altamente seguro. Los clientes también pueden elegir ubicaciones con leyes de protección de datos coherentes con las suyas propias, donde ya existan acuerdos de transferencia de datos.

2. Alinear las políticas nacionales y los requisitos reglamentarios con el principio de libre movimiento de datos a través de las fronteras, para equilibrar eficazmente los objetivos de modernización de la seguridad, la economía y la tecnología de la información.

3. Evaluar modelos de transferencia de datos, como el sistema de normas de privacidad transfronteriza de la Cooperación Económica Asia-Pacífico y cláusulas contractuales estandarizadas, que han sido aprobadas por las autoridades de protección de datos de la Unión Europea y que pueden utilizarse en acuerdos entre proveedores de servicios y clientes para garantizar que cualquier dato personal que salga del Espacio Económico Europeo será transferido de conformidad con el Reglamento General de Protección de Datos.

4. Asegurar que los proveedores de servicios de nube y los contratistas externos demuestren controles de seguridad sólidos para hacer frente al acceso no autorizado de terceros a los datos, a través de acreditaciones de terceros reconocidas internacionalmente (por ejemplo, estándares ISO).

[9] Amazon Web Services. Data Residency, 2020. https://d1.awsstatic.com/whitepapers/compliance/Data_Residency_Whitepaper.pdf

5. Clasificar los datos y definir las funciones y responsabilidades de manejo de datos para determinar las obligaciones de protección de datos apropiadas para cada parte. Los gobiernos deben seleccionar el modelo de implementación de nube apropiado de acuerdo con sus necesidades específicas, el tipo de datos que manejan y el perfil de riesgo. Para el conjunto de datos más específico y clasificado en el nivel más alto de sensibilidad, los gobiernos pueden encontrar opciones híbridas más adecuadas. Los gobiernos también deberían considerar aprovechar la norma ISO 27018 para definir las funciones del controlador y procesador de datos. Los gobiernos pueden trabajar con los proveedores de servicios de nube para comprender y aplicar adecuadamente las responsabilidades de protección de datos para el controlador frente al procesador para cada uno de los modelos de servicio en la nube.

6. Asegurar que el cliente comprenda e implemente los servicios de seguridad para el cifrado de datos.

7. Participar en esfuerzos bilaterales y multilaterales de asistencia judicial recíproca, de modo que se equilibren las necesidades gubernamentales de obtener de manera expedita la evidencia necesaria en las investigaciones y enjuiciamientos, con el derecho de un individuo a la privacidad.

Derechos de las personas respecto del uso de sus datos personales.

Una cuestión inherente al uso de los servicios de cómputo en la nube es el tratamiento de datos personales. En este campo de la regulación, la figura jurídica que se ve inmiscuida en el uso de la nube es la transferencia internacional de datos personales.

Las vertientes de análisis que, entonces, nos interesan para el presente estudio, son dos: a) la implementación de acciones para custodiar el derecho

fundamental a la protección de datos; y b) la clasificación de los datos por parte de las entidades del sector público.

En principio, para proteger los datos en la nube -y así también amparar el derecho fundamental de sus titulares- las mejores prácticas indican que primero es necesario determinar el grado de sensibilidad de los datos personales y el impacto que probablemente se generaría en caso de que los datos se vean comprometidos, perdidos o mal utilizados.

En otros términos, asumiendo que los datos alojados en la nube normalmente residirán en un entorno extranjero y que tales datos eventualmente pueden ser considerados sensibles por las leyes de protección de datos, se hace necesario establecer mecanismos jurídicos -contractuales o regulatorios- por medio de los cuales se evalúe la naturaleza de los datos, se controle el acceso a los mismos, se garanticen las medidas de seguridad físicas y tecnológicas, se restrinja el traslado hacia terceros no autorizados y se prevea la eliminación de la información personal, por parte del proveedor de servicios, al final del compromiso contractual.

La clasificación de datos es un paso fundamental en la gestión de los riesgos aparejados a la nube.

Ahora bien, en la clasificación de los datos por parte de las entidades del sector público, debemos tener en consideración que las agencias gubernamentales se asumen como propietarios de los datos que serán alojados en la nube, de modo que se convierten en los responsables de clasificarlos y, por lo tanto, de determinar el modelo de nube, el esquema de servicios y las características de seguridad que esperan que cumpla su proveedor de *Cloud Computing*.

La *ratio* de la decisión del sector público para la implementación de la nube está en buena medida -si bien no es la única directriz- en la clasificación de la información que eventualmente será gestionada en la nube, pues es justamente ésta la que puede quedar expuesta a riesgos jurídicos y fácticos.

Desde luego, la clasificación de datos que relicen las agencias públicas repercute de manera directa en el derecho a la protección de datos personales de

la ciudadanía, pues por lo general serán los datos de los individuos los que serán tratados en la nube.

En este contexto, se puede decir que existen dos modelos relevantes de clasificación de datos del sector público: Estados Unidos y Reino Unido.

Por un lado, el gobierno de Estados Unidos utiliza un esquema de clasificación de tres niveles para la información de seguridad nacional, que se basa en el impacto que podría tener su divulgación para la seguridad nacional:

Información confidencial, es decir aquella cuya divulgación no autorizada puede general un daño a la seguridad nacional.

Información secreta, que consiste en aquella cuya divulgación no autorizada puede general un daño serio a la seguridad nacional.

Información ultrasecreta, o sea aquella cuya divulgación no autorizada puede general un daño excepcionalmente grave a la seguridad nacional.

Además, el modelo norteamericano también utiliza el término *datos no clasificados* para referirse a cualquier dato que no corresponda a alguno de los tres niveles de clasificación antes indicados. Incluso dentro de los datos *no clasificados* existen etiquetas secundarias para información sensible, como "*Solo para uso oficial*" e "*Información no clasificada con*trolada", que restringen su divulgación al público o al personal no autorizado.

Por su parte, en Reino Unido se sigue la siguiente clasificación de la información:

Oficial, que corresponde a operaciones y servicios comerciales de rutina, algunos de los cuales podrían tener consecuencias perjudiciales si se pierden, son robados o publicados en los medios; pero no representa un perfil de amenaza elevado.

Secreto, es decir información muy sensible que justifica medidas de protección reforzadas para defenderse de amenazas altamente capaces.

Alto secreto, que consiste en la información más sensible, que requiere de los niveles más altos de protección contra las amenazas más graves.

Aquí conviene hacer una precisión importante: la información que puede ser alojada en la nube puede consistir en datos personales o en información diversa. Por ello el ejercicio de clasificación de la misma por parte de las agencias gubernamentales constituye tanto un paso en la tutela del derecho fundamental a la protección de datos personales, como también un eslabón en las acciones de defensa de la seguridad nacional.

En términos amplios, la clasificación de los datos permite a las organizaciones estatales evaluar y mitigar los riesgos asociados con diferentes tipos de datos y con los distintos grados de amenazas.

Como se puede advertir, los dilemas de orden jurídico que acompañan al uso de la nube tienen una correspondencia directa con las características tecnológicas de ésta, con la naturaleza de la información, su ubicación y transferencia, pero también con los riesgos inherentes para el sector público.

En este sentido, la implementación de los servicios de cómputo en la nube debe responder a los dilemas jurídicos que se han expuesto, desde una óptica de libre tránsito de datos, clasificación de los datos, protección de los datos y mitigación de riesgos jurídicos y fácticos.

El enfoque clave para los gobiernos nacionales está en diseñar espacios de regulación que logren gestionar los riesgos ya apuntados, para propiciar un nivel aceptable de beneficios económicos y sociales derivados del uso de la nube.

Los sistemas o modelos regulatorios desarrollados en jurisdicciones relevantes.

El crecimiento del mundo digital ha modificado el intercambio global de bienes y servicios, impactando en el marco regulatorio.

El crecimiento del mundo digital permite almacenar y procesar enormes cantidades de datos, personales y no personales, a través de procesos automatizados. En un principio, la legislación se enfocó en la protección de datos personales, sin embargo, no debemos olvidar que la mayoría de las bases de datos cuentan con datos compuestos -personales y no personales-. Aunque cada uno tiene reglas distintas, ambos se deben regular para garantizar fines legítimos en su tratamiento.

Para efectos del presente estudio es necesario identificar las mejores prácticas y procesos exitosos de regulación e implementación del uso de la nube en el sector público en otros países. Los procesos de estandarización de requisitos para garantizar la seguridad de la información. No se debe ignorar la experiencia de otras regiones ya que su aprendizaje será fundamental para implementar exitosamente el uso de la nube en México. Especialmente para encontrar un balance entre innovación tecnológica y protección de derechos fundamentales.

Panorama regulatorio global.

El funcionamiento de la nube ha motivado que organizaciones internacionales y líderes nacionales propongan estándares comunes y regulaciones homogéneas que favorezcan el libre comercio, la innovación tecnológica y, especialmente, un mismo parámetro de protección para el procesamiento de datos sin limitar el flujo de datos.

A continuación, se analizarán algunos de estos esfuerzos internacionales.

La Organización para la Cooperación y el Desarrollo Económicos (OCDE) fue de las primeras organizaciones en emitir directrices sobre las consecuencias de la era digital y las nuevas tecnologías que se empezaban a utilizar a nivel mundial. Las directrices sobre protección de la privacidad y flujos transfronterizos de datos personales, conocidas como directrices de privacidad, fueron adoptadas en 1980 como guías generales aplicables al procesamiento de datos personales. Se buscó identificar los principios aplicables a estas operaciones sin mencionar una tecnología en específico para garantizar su flexibilidad ante el contexto de innovación[10]. También emitió una Declaración sobre flujos de datos transfronterizos con un enfoque más político sobre las implicaciones de las nuevas tecnologías y el compromiso de los países firmantes de adoptar soluciones comunes. Otro instrumento relevante es la Declaración ministerial sobre la protección de la privacidad de las redes globales, donde la OCDE reconoció los beneficios de garantizar la privacidad de la información procesada en redes globales y la importancia de generar confianza en las nuevas tecnologías. Un elemento indispensable para impulsar el desarrollo tecnológico era evitar restricciones innecesarias en los flujos transfronterizos de datos personales. Es importante reconocer el trabajo de la OCDE para identificar los principios fundamentales que años después serían retomados en regulaciones nacionales y políticas públicas de implementación de la nube.

En 2015, la Unión Internacional de Telecomunicaciones (UIT)[11], de la cual México es parte, emitió la Recomendación UIT-T X.1601 para analizar las amenazas y los problemas de seguridad en el contexto de la computación en la nube. La implementación de esta recomendación es voluntaria, pero ofrece

[10] https://www.oecd.org/sti/ieconomy/15590267.pdf
[11] Es un organismo especializado de las Naciones Unidas. Está conformado por 193 Estados Miembros y más de 900 empresas, universidades y organizaciones regionales e internacionales. Su función es coordinar, a escala mundial, el uso compartido del espectro, promover la cooperación internacional para la asignación de órbitas de satélite, mejorar la infraestructura de telecomunicaciones en el mundo en desarrollo y fijar las normas mundiales que fomentan la interconexión continua de una amplia gama de sistemas de comunicaciones.

estrategias para identificar los riesgos y amenazas de gran utilidad para todo agente que quiera transitar hacia esta tecnología. De acuerdo con esta recomendación, la gestión de la seguridad de los servicios de la nube es fundamental para una transición exitosa. Este esfuerzo de regulación universal se enfoca en la mitigación de riesgos.

Cuatro años después, en la reunión anual del Foro Económico Mundial, el primer ministro de Japón, Shinzo Abe, declaró que la era digital exigía regulaciones internacionales homogéneas que permitieran el flujo transfronterizo de datos y garantizaran los derechos de privacidad y protección de datos personales. Para él, esto únicamente sería posible si todos los países trabajaban coordinadamente para establecer normas comunes que impulsaran la innovación sin afectar los derechos de las personas. Se propuso crear la iniciativa "*Data Free Flow with Trust*" (DFFT)[12].

En esta reunión, se aprobó el proyecto "*Osaka Track*"[13] que demostraba el compromiso de los países firmantes, México uno de ellos, en promover el análisis de políticas públicas y regulación internacional que impulsaran la economía digital y permitieran aprovechar el potencial del procesamiento de información a gran escala.

La digitalización es un fenómeno que ha transformado las economías y sociedades en todo el mundo. Las autoridades tienen un papel fundamental para asegurar que el uso de las nuevas tecnologías se realice de forma ordenada y respetando los derechos de las personas.

En la reunión del grupo G20 de 2019, se retomó la iniciativa *DFFT*. Los líderes de los países participantes coincidieron en que el desarrollo de las nuevas tecnologías digitales y la confianza no deben contraponerse. Impulsar ambos

12 https://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20_Flows_2020.pdf

13 https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/pdf/special_event/en/special_event_01.pdf

proyectos debe ser un objetivo de la comunidad internacional. Reconocieron que el libre flujo de datos promueve la innovación y un desarrollo sustentable. Por esto se deben solucionar los retos sobre propiedad intelectual, protección de datos personales y privacidad a través de marcos regulatorios internacionales que den seguridad jurídica a los usuarios y proveedores del servicio de la nube. La regulación debe enfocarse en los estándares de protección y no en la localización de los servidores o el domicilio de las empresas. De esta manera, los usuarios podrán confiar en el uso de las tecnologías y los proveedores serán responsables de cumplir con los mismos estándares sin importar su domicilio[14].

Aplicar la visión de la iniciativa *DFFT* en la redacción de leyes y políticas públicas nacionales debería ser una de las prioridades de los gobiernos, ya que su incorporación a esta nueva etapa de la era digital repercutirá en su crecimiento económico y desarrollo social.

La Organización Internacional de Estandarización (ISO) también se unió a estos esfuerzos de regulación internacional y ha publicado una diversidad de materiales relativos a los servicios en la nube. Para los propósitos del presente estudio, interesa destacar los siguientes:

- **ISO/IEC 29100:2011 (Estándares de privacidad)**

  Define los estándares y términos comunes que deben cumplir los actores que utilicen tecnologías de la información para procesar información personal.

- **ISO/IEC 27001:2013 (Seguridad de la información)**

  Establece los elementos para desarrollar, implementar, monitorear y actualizar un programa de gestión de riesgos de la información dentro de una organización, sin importar su tamaño o naturaleza.

  Analizar los riesgos de la información en posesión de una organización es de gran utilidad dentro de una política de implementación de la nube ya que

[14] https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust

permite identificar las necesidades de la organización y el tipo de nube que mejor cumple con sus objetivos.

- **ISO/IEC 27017:2015 (Seguridad de la nube)**

  Es una guía para la implementación de controles de seguridad que deben cumplir los usuarios/clientes y proveedores del servicio de la nube. Estos controles dependerán de la información que se procese a través de la nube, el análisis de riesgo de la organización y las obligaciones legales o contractuales por lo que debe hacerse un estudio específico para cada caso.

- **ISO/IEC 27018:2019 (Privacidad de la nube)**

  Se enfoca en medidas de seguridad y controles que deben implementarse para salvaguardar la confidencialidad de los datos personales procesados o transferidos a través de los servicios de la nube.

  Esta guía es aplicable para organizaciones públicas y privadas, sin importar su tamaño, y se enfoca en servicios de nube pública. La utilidad de este documento es que se puede utilizar como un marco regulatorio común, en materia de protección de datos personales, para todos los proveedores del servicio de la nube pública, sin importar su domicilio o la localización de sus servidores.

- **ISO/IEC 27701:2019 (Administración de la privacidad de a información)**
  Es una extensión del ISO/IEC 27001. Especifica los requisitos para implementar y dar seguimiento a las medidas de seguridad dentro de una organización para garantizar la confidencialidad de los datos personales.

Estos esfuerzos, iniciativas e instrumentos permiten identificar los elementos mínimos que deben cumplir los servicios de la nube para cumplir con estándares internacionales homogéneos. Su cumplimiento no libera a proveedores y usuarios de cumplir con las legislaciones nacionales, pero es un primer paso para eliminar las disparidades regulatorias y fomentar la confianza en los servicios de la nube.

América del Norte

Esta región es de especial importancia para el estudio porque impacta directamente en las actividades comerciales y políticas de México. La innovación tecnológica es un factor determinante para impulsar el crecimiento de la zona, especialmente porque los principales proveedores del servicio de la nube tienen su sede en Estados Unidos, a pesar de que sus centros de almacenamiento y procesamiento de datos se encuentren en otros continentes. Esta situación propició la aprobación de normas jurídicas que delimitaran los derechos y obligaciones de usuarios y proveedores independientemente de la localización física de su infraestructura.

A continuación, se analizará el marco regulatorio de la región que incide en la adopción del uso de la nube.

Tratado entre México, Estados Unidos y Canadá (T-MEC)

La intensa relación comercial que existe entre los países que integran la región propició la firma de tratados con el objetivo de disminuir las diferencias regulatorias, estableciendo principios y estándares comunes que deben cumplir las regulaciones nacionales.

El tratado más emblemático es el Tratado de Libre Comercio de América del Norte (TLCAN), firmado en 1992 entre México, Estados Unidos de América y Canadá para impulsar el intercambio comercial, cultural y migratorio de la región.

Después de más de dos décadas, fue necesario actualizar su contenido. En 2020 entró en vigor el nuevo T-MEC. Uno de los principales cambios fue reconocer la importancia de las tecnologías de la información como herramienta transversal para el desarrollo de los sectores industriales y la relevancia de los datos para la implementación de políticas públicas.

También se estableció la obligación de garantizar la protección de los datos personales en cualquier operación[15] y se reconocieron los principios de proporcionalidad, calidad de datos, limitación de uso y transparencia en su tratamiento.

Un tema relevante, para efectos del presente estudio, es que se prohibió establecer un requisito de localización de instalaciones informáticas para la realización de negocios, privilegiando los flujos transfronterizos de datos[16]. En caso de ser necesaria una restricción a estos flujos, los países deberán justificarla con base en una política pública.

Por último, se reconoció la importancia de promover los datos abiertos gubernamentales ya que fomentan la competitividad e innovación en los sectores productivos. Esto significa que los datos deben estar disponibles en un formato legible por máquina y que puedan ser buscados, recuperados, utilizados, reutilizados y redistribuidos.

Estados Unidos

La adopción temprana de las nuevas tecnologías en el sector público estadounidense fue uno de los detonadores del crecimiento de esta industria.

Desde 2011 se aprobó el programa *Federal Risk and Authorization Management Program (FedRAMP)*[17] que ofrecía herramientas a las autoridades federales para conocer el costo-beneficio y riesgo de adoptar la nube. A partir de este momento, se impulsó la adopción de nuevas tecnologías en el ámbito público enfocándose en la seguridad y protección de la información.

Al igual que en el caso europeo, al estandarizar los requerimientos legales y fomentar la transparencia de los servicios contratados, se incrementó la confianza de las autoridades en las nuevas tecnologías. Otra herramienta útil fue la certificación que otorga el programa a los proveedores que se someten a su proceso

[15] Artículo 19.8 del T-MEC
[16] Artículos 19.11 y 19.12 del T-MEC
[17] https://www.fedramp.gov/federal-agencies/

de revisión y monitoreo. También se creó un mercado de productos digitales que han sido utilizados por agencias gubernamentales para fomentar su adopción por nuevos agentes.

Uno de los mayores éxitos de este programa es que se utilizó como intermediario entre proveedores y el sector público, disminuyendo los costos de adopción y negociación de los contratos.

Tres años después se aprobó la *Federal Information Technology Acquisition Reform Act (FITARA).* Esta ley significó el primer gran esfuerzo del gobierno estadounidense para renovar y mejorar los servicios de tecnología de la información del gobierno federal[18]. Su objetivo era consolidar y optimizar los centros de datos gubernamentales a través de la adopción de nuevas tecnologías, transparentar la operación de los centros de datos y mejorar la gestión de riesgos[19].

La transición hacia la adopción de la nube y el uso compartido de servicios digitales en el gobierno federal se fortaleció con el *Memorandum Data Center Optimization Initiative (M-16-19, DCOI)*. En este documento, el director federal de información exigía a las dependencias federales desarrollar estrategias para la consolidación de los centros de datos, incrementar su eficiencia, mejorar la seguridad, disminuir los costos y consolidar la transición hacia el uso de nuevas tecnologías[20].

En el sistema jurídico estadounidense, los precedentes judiciales son un mecanismo fundamental para la actualización del marco regulatorio. Las tecnologías se encuentran en un proceso de constante innovación por lo que los jueces muchas veces se enfrentan a vacíos legales que deben interpretar. En la adopción del uso de la nube, el juicio *Microsoft Corp. v. United States (2018)* es muy importante para entender el desarrollo de esta tecnología y los retos que enfrentan las autoridades para cumplir con sus atribuciones en la era digital.

---

[18] https://management.cio.gov/
[19] https://www.cio.gov/policies-and-priorities/FITARA/
[20] https://datacenters.cio.gov/policy/m-16-19/

En 2013, *Microsoft* impugnó una orden del FBI para entregar correos electrónicos relacionados con una investigación de narcotráfico guardados en servidores ubicados en Irlanda. *Microsoft* alegó que la ley utilizada como fundamento legal no era aplicable para información almacenada fuera de los Estados Unidos y que las leyes de Irlanda le prohibían entregarla. *Microsoft* buscaba que el Departamento de Justicia estadounidense negociara directamente con el gobierno irlandés a través de los instrumentos diplomáticos existentes.

En primera instancia, los jueces determinaron que la ley sí tenía competencia extraterritorial por lo que debía entregar la información. *Microsoft* apeló la decisión y logró la invalidación del requerimiento de información. Como respuesta, el Departamento de Justicia solicitó a la Suprema Corte de Justicia que conociera del caso. Durante la substanciación del juicio, el Congreso aprobó la ley *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)* que modificaba la ley utilizada para el requerimiento de información y resolvía las dudas sobre la obligación de las empresas, con servidores fuera del territorio, de entregar información a autoridades estadounidenses. Ambas partes solicitaron que la Suprema Corte desechara el caso porque la aprobación de la nueva ley.

Este asunto fue muy importante porque definió los límites del derecho a la privacidad, el alcance del marco regulatorio estadounidense fuera de su territorio y las implicaciones del uso de tecnologías como centros de datos y la nube.

La *Cloud Act* es una ley federal aprobada en 2018. Su principal objetivo fue permitir a las autoridades federales requerir información de empresas estadounidenses sin importar dónde resida físicamente la información o los servidores que la almacenan. Esta obligación no es absoluta y los proveedores de servicios tecnológicos pueden cuestionar o rechazar estas peticiones si consideran que no cumplen con las reglas de protección de datos personales del país donde residen los servidores o centros de datos.

También se prevé la firma de acuerdos bilaterales para asegurar una mayor protección de datos personales y libertades de sus ciudadanos a la par de fortalecer los mecanismos de coordinación para combatir la delincuencia y el terrorismo. Los

mecanismos diplomáticos tradicionales, como los Tratados de asistencia legal mutua, son muy lentos y burocráticos. La globalización de la actividad criminal exige una respuesta más eficiente para combatirla, estos acuerdos bilaterales buscan ser una solución.

La actualización del marco regulatorio es indispensable para garantizar que las autoridades puedan cumplir con sus obligaciones, especialmente en la persecución de delitos. Las nuevas tecnologías están al alcance de todos, incluidos los grupos delictivos, por lo que las leyes deben contemplar las nuevas modalidades de tratamiento de datos para salvaguardar la seguridad pública y privilegiar el estado de derecho.

Esta ley buscó establecer un equilibrio entre la protección de la privacidad y la seguridad nacional en el marco de las nuevas tecnologías y formas de operar de las empresas.

El primer acuerdo en firmarse bajo la *Cloud Act* fue el Acuerdo Reino Unido-EUA *"Bilateral Data Access Agreement"*. Su objetivo fue permitir a las autoridades solicitar directamente a los proveedores la información -evidencia digital- necesaria en ambos países. Los requerimientos deben cumplir ciertas condiciones y garantizar los principios de protección de datos personales[21].

A través de la coordinación, se buscó combatir organizaciones criminales y terroristas sin afectar el flujo transfronterizo de datos. Este mecanismo aseguró eficiencia en el desempeño de las funciones estatales y a la par garantizó un estándar de protección alto de los derechos de privacidad y protección de datos personales de los ciudadanos.

[21] 21 Thoughts and Questions about the UK-US CLOUD Act Agreement: (and an Explanation of How it Works – with Charts), Theodore Christakis, European Law Blog, 2019 https://europeanlawblog.eu/2019/10/17/21-thoughts-and-questions-about-the-uk-us-cloud-act-agreement-and-an-explanation-of-how-it-works-with-charts/

En 2019, con la publicación del *MEMORANDUM Update to Data Center Optimization Initiative (M-19-19, DCOI)* cambió el enfoque. Después de años de buscar una infraestructura más eficiente que significó la clausura de muchos centros de datos, el gobierno decidió que era momento de analizar los servicios que se estaban utilizando y el proceso de actualización de las agencias y servicios gubernamentales[22].

A nivel local, es importante resaltar la ley *California Privacy Rights Act (CPRA)*, aprobada en 2020 y entrará en vigor en 2023. Este es el más reciente -y extenso- esfuerzo estadounidense por incrementar la protección de la información obtenida y procesada a través de medios electrónicos[23].

Principalmente, impone nuevos requisitos a los responsables del tratamiento de datos y empodera a sus titulares[24]. Incorpora principios de la regulación europea como los derechos ARCO y reconoce la obligación de transparentar las transferencias de datos y su uso. También se prevé la creación de una agencia responsable de proteger la privacidad y datos de las personas.

Para evitar reformar posteriores que retrocedan en la protección de los datos personales se incluyó una cláusula -*one way ratchet*- que únicamente permite reformas para fortalecer la privacidad de los usuarios y prohíbe cualquier modificación que la debilite.

Por último, es importante recordar que existen legislaciones sectoriales que regulan el tratamiento de datos personales que pueden incidir en la adopción de la nube. Por ejemplo, la ley *Health Insurance Portability and Accountability Act (HIPAA)*[25]*.* Es una ley federal aprobada en 1996 que protege la confidencialidad de la información médica de los pacientes y especifica las medidas de seguridad y

[22] https://datacenters.cio.gov/policy/
[23] https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html
[24] https://pro.bloomberglaw.com/brief/the-far-reaching-implications-of-the-california-consumer-privacy-act-ccpa/
[25] https://www.cdc.gov/phlp/publications/topic/hipaa.html

obligaciones de los encargados de procesar la información. Si alguna dependencia gubernamental con acceso a esta información decide implementar el uso de la nube, el servicio deberá cumplir con los estándares establecidos en esta ley.

Con fundamento en estos textos normativos, el gobierno estadounidense impulsó la adopción de la nube como una política pública de mejora e innovación en el sector público. Su implementación también ha evolucionado, cambiando de enfoques para adecuarse a la nueva realidad y tecnologías.

Estrategia Federal del uso de la nube

- *Cloud first*

En 2011, el gobierno federal identificó que la información en su poder estaba fragmentada, en sistemas poco amigables, duplicados e ineficientes. Ante esta situación, decidieron que la adopción del uso de la nube sería la forma de transformar y mejorar el servicio público. El uso de la nube tenía gran potencial como herramienta para la sistematización de datos y rápida respuesta a los ciudadanos. Además, al ser más eficiente reducía los costos del uso de tecnologías permitiendo que esos recursos se utilizaran en otros programas de mayor impacto social.

La política *Cloud first* significa que ante una situación siempre se debe analizar como primera opción una solución basada en la nube. El objetivo fue acelerar la adopción de la nube en todo el sector público antes de la adquisición de nuevos activos.

Con la publicación de esta estrategia, las oficinas gubernamentales realizaron un análisis de sus programas de tecnologías de la información e identificaron el proceso adecuado para la migración hacia la nube.

También se establecieron los pasos a seguir para la implementación de la nueva tecnología. Por ejemplo, identificar qué servicios debían migrar, analizar los servicios de los proveedores para asegurar que cumplieran con el marco regulatorio y capacitar a los operadores para aprovechar al máximo la tecnología.

La adopción de estándares homogéneos fue una de las prioridades de esta política. Reglas claras y uniformes fomentan la libre competencia, dan mayor seguridad para el sector público y facilitan la portabilidad de los servicios. Para este proceso de definición, la *National Institute of Standards and Technology (NIST)* desempeñó un papel fundamental. Este instituto estuvo en constante comunicación con expertos, agencias internacionales y proveedores para conocer sus opiniones y lograr un consenso sobre los estándares.

Otro elemento muy importante de esta política fue reconocer las diferencias entre las oficinas y agencias gubernamentales. A pesar de que esta estrategia obliga a todo el sector público federal, se privilegió la implementación personalizada de los servicios de la nube de acuerdo con los requisitos de cada oficina.

- *Cloud Smart*

Una vez consolidado el uso de la nube en la administración pública federal, fue necesario actualizar el enfoque para lograr mayores ahorros, seguridad y servicios más rápidos. Con la información recabada sobre los primeros procesos de adopción de la nube se pudieron generar manuales con las mejores prácticas y recomendaciones. Esta segunda etapa -2019- de la transformación del servicio público permitió aprovechar la experiencia -y errores- de los primeros programas.

Esta estrategia creó una guía para el sector público con herramientas para explotar el potencial de esta tecnología. A través de una lista de acciones se buscó actualizar los programas, políticas y recursos del gobierno. Se enfocó en implementar la transformación tecnológica con una visión transversal y se basó en tres pilares: seguridad, obtención del servicio y fuerza de trabajo[26].

Cada oficina gubernamental debía valorar el impacto del uso de la nube en el trabajo diario, la seguridad de la información y en los usuarios. La modernización del servicio público no debía ser el único objetivo al definir la estrategia de implementación de las nuevas tecnologías. La calidad en los servicios, los derechos

[26] https://cloud.cio.gov/strategy/

de los ciudadanos y los efectos del uso de la nube deben ser incorporados como factores relevantes en el proceso de decisión.

Ejemplos de adopción de los servicios de la nube en el sector público estadounidense

Para incentivar su uso, el gobierno desarrolló *Cloud.gov*. Esta plataforma cuenta con un servicio de la nube tipo PaaS para ayudar a los entes gubernamentales a actualizar sus servicios y mejorar la experiencia del usuario sin preocuparse por la infraestructura de los servidores. Este servicio se logró en colaboración con Amazon Web Services y cuenta con servicios de código abierto que garantizan su portabilidad a otros proveedores del servicio de la nube. Este proyecto busca reducir los costos de la adopción de la nube en el sector público[27].

Otros ejemplos exitosos de adopción del uso de la nube en oficinas gubernamentales son la nube *Nasa Nebula* y la nube de la *Federal Election Commission (FEC)*.

La *Nasa Nebula*[28] es una nube comunitaria que permite el acceso de investigadores a servicios tecnológicos de bajo costo y grandes bases de información. Este proyecto ha disminuido los tiempos destinados a la búsqueda de información, fortaleciendo el desarrollo académico.

La *FEC* decidió hospedar su portal de internet en la plataforma *Cloud.gov*. Al mover su información a la nube, ahorró 85% de los costos anuales destinados al mantenimiento de la página y les permitió estar preparados para los momentos de mayor tráfico. El siguiente proyecto será migrar a la nube el sistema de rendición de cuentas sobre los gastos de campaña[29].

Canadá

[27] https://cloud.gov/
[28] https://www.nasa.gov/open/nebula.html
[29] https://cloud.gov/docs/customer-stories/fec/

El gobierno de Canadá ha impulsado la adopción de servicios tecnológicos privados que mejoren la interacción de los ciudadanos con las oficinas gubernamentales[30].

Para garantizar una transformación ordenada se determinó que primero se implementaría el uso de la nube en sistemas con información no clasificada. Por ejemplo, sistemas con información pública, información generada por el gobierno, metadata e información científica.

Un ejemplo de éxito fue la adopción de esta tecnología en los sistemas penitenciarios. La información procesada a través de la nube no era clasificada, pero permitía optimizar el funcionamiento de las instalaciones y subsanar deficiencias en los servicios técnicos.

Desde 1985 se aprobó el marco normativo en materia de protección de datos personales y acceso a la información que actualmente se utiliza. La *Access to Information Act* reconoció la obligación de las instituciones federales de rendir cuentas y actuar con transparencia para promover el debate respecto al ejercicio público. Su equivalente en materia de protección de datos personales fue la *Privacy Act* cuyo objetivo era garantizar la privacidad y protección de los datos personales en posesión de instituciones gubernamentales. El contenido de ambas leyes es muy similar a la legislación mexicana.

A partir de este marco general se aprobaron legislaciones específicas para regular las nuevas tecnologías. Por ejemplo, en 2017 se publicó la directriz *Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN)*[31] que estableció los requisitos de seguridad que debían cumplir los servicios de nube. Uno de ellos es determinar claramente los roles y

[30] https://www.canada.ca/en/shared-services/news/2018/02/cloud_computing.html
[31] https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/direction-secure-use-commercial-cloud-services-spin.html

responsabilidades de las partes contratantes, proveedores y oficinas gubernamentales.

Esta directriz es vinculante para organizaciones que desean contratar servicios comerciales de nube y oficinas de gobierno con información protegida nivel B y nivel A, si se justifica un riesgo en particular.

El uso de nuevas tecnologías, como la nube, puede implicar la transferencia de información gubernamental a servidores fuera del territorio canadiense y, por lo tanto, sujetos a otras regulaciones. Por esta razón, el gobierno canadiense emitió la directriz *Direction for Electronic Data Residency: IT Policy Implementation Notice (ITPIN)*[32] aplicable a cualquier programa, servicio o proyecto que almacene o transfiera información protegida nivel B, nivel C e información clasificada[33]. Dada la naturaleza de la información, se determinó que ésta únicamente puede ser almacenada y procesada en territorio canadiense o en oficinas gubernamentales en el exterior, por ejemplo, embajadas.

Canada Cloud Adoption Strategy

Publicada en 2016 y actualizada en 2018, se creó como una política con acciones específicas que debían cumplir las agencias gubernamentales para la adopción de la nube. En primer lugar, al igual que en el caso estadounidense, se implementó la estrategia *Cloud first*. También se exigió a los encargados de su implementación garantizar los derechos de privacidad y protección de datos

---

[32] https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/direction-electronic-data-residency.html

[33] En Canadá se estableció un sistema de clasificación de la información:

- Información protegida nivel A, información sensible personal, industrial o gubernamental.
- Información protegida nivel B, información con mayor grado de sensibilidad.
- Información protegida nivel C, información muy sensible que podría poner en riesgo la vida de las personas, la economía o la seguridad nacional.
- Información confidencial, secreta o ultrasecreta, información muy sensible que podría poner en riesgo la vida de las personas, la economía o la seguridad nacional.

personales de los titulares. Además, se impulsó la creación de una plataforma comunitaria donde distintos proveedores pudieran ofrecer sus servicios y las oficinas gubernamentales pudieran adquirirlos con la tranquilidad de que el gobierno había realizado un análisis de riesgo y negociado los términos contractuales para asegurar el cumplimiento del marco regulatorio[34].

Para el gobierno canadiense, el proceso de actualización del sector público debe ser visto como un proceso en constante movimiento y debe planearse con objetivos a largo plazo para garantizar un cambio sostenible, eficaz y eficiente. Por ejemplo, en 2011 se buscó consolidar los correos electrónicos, redes y servidores públicos en la oficina *Shared Services Canada (SSC*). Un año después, como resultado de un informe sobre el estado de las tecnologías de la información en el gobierno de Canadá, se concluyó que se debía modificar el modelo de inversión para sustituir las aplicaciones y software utilizado.

El diálogo con expertos y proveedores privados fue fundamental para desarrollar esta estrategia y asegurar el cumplimiento de sus objetivos. Uno de los cambios que se hicieron en los procesos de actualización de la estrategia fue resaltar la importancia de utilizar la nube pública como el modelo ideal para el sector público y únicamente utilizar una modelo de nube privada para información secreta o clasificada. Esta política reitera el principio de localización dentro del territorio de la información protegida nivel B, nivel C o clasificada, en cumplimiento de la directriz *ITPIN*.

Para explotar las ventajas del uso de la nube en el sector público, esta política pública recomienda la utilización de una nube pública con servicio Saas.

En concordancia con esta estrategia, autoridades de diferentes niveles de gobierno colaboraron para crear una nube comunitaria para el sector público

---

34 https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/government-canada-cloud-adoption-strategy.html

(Canadian public sector community cloud CPSCC). Este espacio compila servicios de nube pública con medidas de seguridad autorizados por el gobierno canadiense.

Este mercado digital no tiene como objetivo ser el único medio para la contratación de servicios de la nube, únicamente pretende simplificar el proceso de contratación y proveer al sector privado con estándares de seguridad homogéneos.

Una de las ventajas para el sector privado es que una vez incluido su servicio en esta plataforma, diversas agencias gubernamentales pueden adquirir el servicio sin tener que someterse a una nueva auditoría. Otro beneficio de la *CPSCC* es que al tener un representante gubernamental que interactúa con los proveedores incrementa su poder de negociación, asegurando mejores condiciones contractuales para el sector público.

Además, la transparencia en las herramientas utilizadas y las soluciones tecnológicas implementadas favorece el intercambio de información entre autoridades fomentando la adopción de enfoques similares y recopilación de mejores prácticas.

En conclusión, en ambos países se ha impulsado la adopción del servicio de la nube desde el sector público como una herramienta de transformación y mejora. A través de estrategias y políticas públicas, los gobiernos han establecido los principios y procesos que deben adoptar las oficinas gubernamentales para aprovechar el potencial de la nueva tecnología sin vulnerar los derechos fundamentales de las personas. En ambos países se regulan las reglas y obligaciones para el tratamiento de datos -diferenciando cuando se trate de datos personales o confidenciales- y no el funcionamiento de una tecnología en específico. Con este enfoque se evita la rápida desactualización del marco normativo.

Europa

La creación de la Unión Europea (UE)[35], como comunidad política y de derecho, impulsó la homologación del marco regulatorio de la región. Los países integrantes de la UE reconocieron las ventajas de tener reglas claras y homogéneas.

El tratamiento de datos no fue la excepción. Los esfuerzos nacionales para garantizar estándares altos de protección fueron superados por las nuevas tecnologías, como el uso de la nube, que permitían almacenarlos o procesarlos en centros de datos ubicados en otros países o continentes. Ante esta situación, las instituciones europeas emitieron normas generales vinculantes que obligan a los responsables del tratamiento a cumplir con estos estándares sin importar la tecnología utilizada o la residencia de sus servidores.

La tendencia regulatoria en Europa ha sido privilegiar la libre circulación de datos[36] e implementar una regulación basada en principios. El objetivo es evitar que la regulación se vuelva obsoleta con el desarrollo de nuevas tecnologías. Si se salvaguarda la privacidad y confidencialidad de la información y se garantiza que su tratamiento sea conforme a los derechos fundamentales, la tecnología que se utilice únicamente será relevante en cuestiones de eficiencia.

Para comprender el alcance e implicaciones jurídicas del uso de la nube se deben analizar los derechos, obligaciones y principios aplicables a los datos y a los responsables de su tratamiento.

A continuación, se analizará la evolución del marco normativo de la nube y su implementación como política pública en los países europeos.

---

[35] Se fundó el 1 de noviembre de 1993.

[36] En concordancia con las cuatro libertades de circulación: mercancías, servicios, personas y capitales establecidas como fundamento de la UE.

Con la fundación de la Unión Europea se privilegió la libertad de prestación de servicios y de establecimiento de actores comerciales dentro del territorio de la UE. En el artículo 56[37] del Tratado de Funcionamiento de la Unión Europea (TFUE) se prohibieron las restricciones a la libre prestación de servicios, lo cual incluye los servicios de tratamiento de datos. Además, se reconoció el principio de libertad de establecimiento en cualquier territorio de la UE[38], por ejemplo, de centros de datos.

Estas libertades podrían ser consideradas como fundamento del principio de libre circulación de datos en el marco regulatorio europeo que incentiva la implementación del uso de la nube en los sectores público y privado.

El Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108)[39], aprobado en 1981, es el marco regulatorio para el tratamiento automatizado de datos personales de mayor alcance y "*el único instrumento internacional jurídicamente vinculante en el ámbito de la protección de datos*"[40]. Sus disposiciones son aplicables a cualquier tratamiento de datos personales realizado por actores públicos o privados en los países integrantes del Consejo Europeo y otros que no pertenecen a esta institución pero que lo han ratificado[41], como México.

Este documento ha sido utilizado en todo el mundo como referente para emitir legislaciones nacionales en materia de protección de datos personales; promoviendo un proceso de homologación de los principios básicos aplicables al tratamiento de datos y, en consecuencia, al uso de la nube.

---

[37] Artículo 56 de la versión consolidada, anteriormente el artículo 49 del Tratado constitutivo de la Comunidad Europea (TCE).
[38] Artículo 49 de la versión consolidada del TFUE, anteriormente el artículo 43 del TCE.
[39] https://rm.coe.int/1680078b37
[40] Manual de legislación europea en materia de protección de datos. Edición de 2018, p.28
[41] Hasta el momento ha sido ratificado por 55 países. México lo ratificó en junio de 2018.

En un principio, este Convenio tuvo como objetivo garantizar un estándar mínimo de protección de datos personales. Sin embargo, el desarrollo de tecnologías de la información, el crecimiento del mundo digital y la globalización del procesamiento de datos obligaron al Consejo Europeo a emitir, en 2001, un Protocolo Adicional y expandir su regulación. Los cambios se centraron en: garantizar la eficacia del Convenio y regular el flujo transfronterizo de datos entre países firmantes. A partir de este momento, se resaltó la necesidad de mejorar el marco regulatorio para beneficiar la innovación y el desarrollo tecnológico.

El reconocimiento del principio de libre circulación de datos fue el primer paso regulatorio para incentivar el uso de la nube en el sector público y privado. La protección de los datos personales podría garantizarse a través de otras acciones y medidas por lo que resultaba excesivo limitar la transferencia de datos y exigir la presencia física de servidores en territorio nacional.

Este Convenio se redactó con base en principios jurídicos[42] y no en procedimientos específicos para evitar que el desarrollo tecnológico lo convirtiera rápidamente en un documento obsoleto. Sin embargo, fue necesaria su actualización para incluir nuevos principios que garantizaran una mejor protección de datos y mejores mecanismos de seguimiento a la implementación del Convenio. En 2018, se abrió a firma el nuevo protocolo de adición. Los principales cambios fueron[43]:

- Se estableció la obligación de los Estados miembro de garantizar la protección de los datos personales de cualquier persona, sin importar su nacionalidad o residencia, cuando se realice un proceso de tratamiento de datos en su jurisdicción. También se reconoció la relación entre derecho a la privacidad, protección de datos personales y otros derechos fundamentales.

[42] https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet
[43] https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8

- Los principios del Convenio se deben aplicar a cualquier tratamiento de datos sin importar si son automatizados o manuales. Estos principios deben ser aplicados incluso en información relacionada con seguridad nacional.
- Los Estados deben aprobar los cambios legislativos necesarios para cumplir con las disposiciones del Convenio. También se prevé un mecanismo de seguimiento y evaluación para comprobar que las medidas implementadas cumplan con los estándares exigidos.
- Se reforzó el principio de proporcionalidad como fundamento para el tratamiento de datos personales y los criterios que debe cumplir el consentimiento del titular.
- El catálogo de datos sensibles se extendió para incluir los datos genéticos y biométricos.
- Se incluyó la obligación de notificar las brechas de seguridad que pudieran afectar seriamente el ejercicio de derechos o libertades fundamentales.
- Aumentó la exigencia de transparencia y rendición de cuentas en el procesamiento de datos.
- Se ampliaron los derechos de los titulares para asegurar un mayor control sobre su información.
- Se determinó que los encargados del tratamiento de datos son responsables del cumplimiento de las normas en materia de protección de datos personales (Principio de responsabilidad proactiva).
- Las transferencias de datos fuera de las fronteras de los Estados Parte únicamente se podrán realizar si se comprueba que el país receptor cumple con estándares similares o superiores de protección de datos personales.
- Se estableció una obligación de crear autoridades nacionales con poder de supervisión, investigación y difusión de los principios de protección de datos personales y buenas prácticas.
- Las autoridades nacionales deben cooperar con sus contrapartes en otros Estados Miembro.

En conclusión, el Convenio 108 estableció las directrices que las regulaciones en la Unión Europea debían seguir en materia de protección de datos personales. Al permitir el flujo transfronterizo de datos personales se impulsó el proceso de adopción de las nuevas tecnologías de la información y comunicación, como el cómputo en la nube, en muchos Estados miembros.

Como resultado del incremento en los flujos transfronterizos de datos, el desarrollo de nuevas tecnologías que permiten el tratamiento de un mayor volumen de datos y la necesidad de generar confianza en el mercado digital a través de un marco regulatorio unificado, en 2016, se aprobó el Reglamento General de Protección de Datos (*RGPD, Reglamento UE 2016/679*[44]). Al ser un reglamento, no requiere de la aprobación de leyes nacionales para su incorporación al orden jurídico; su contenido es vinculante y directamente aplicable. Dadas las implicaciones para las empresas obligadas por esta nueva regulación se estableció un periodo de transición de dos años en los que debían adoptar los cambios necesarios.

La implementación de normas más estrictas empoderó a la ciudadanía frente a las empresas que recolectaban y procesaban sus datos exigiendo una mayor rendición de cuentas y responsabilidad de las empresas[45]. Este proceso de homologación también simplificó la operación de las empresas, generándoles importantes ahorros.

El Reglamento aseguró el respeto de los derechos ARCO[46] y fomentó la transparencia en el tratamiento de datos[47]. Garantizar herramientas eficaces para la protección de los datos personales, beneficia a las personas ya que adquieren conciencia de la importancia de salvaguardar su información.

---

[44] https://www.boe.es/doue/2016/119/L00001-00088.pdf

[45] https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_es

[46] Derecho de acceso, rectificación, cancelación y oposición.

[47] https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/gdpr-fabric-success-story_es

Las autoridades nacionales son las responsables de investigar y sancionar cualquier violación a esta normativa. Las sanciones pueden ser: advertencias, órdenes para rectificar o borrar información, restricción o prohibición del tratamiento de datos e, incluso, sanciones económicas que pueden llegar hasta el 4% del volumen de negocios mundial de la empresa sancionada.

Desde mayo 2018 a noviembre 2019, 22 autoridades nacionales encargadas de garantizar la protección de datos personales aplicaron 785 multas[48]. Esto nos demuestra que el Reglamento es un instrumento jurídico "vivo" con implicaciones directas en las relaciones entre responsables y titulares de los datos.

Otro elemento importante, y que podría ser implementado en México, es la adopción de códigos de conducta que describen y especifican la aplicación del RGPD en los distintos sectores industriales. Estas herramientas favorecen la aplicación del reglamento, respetando las particularidades de los sectores sin menoscabo de la privacidad de los titulares.

El principio de libre circulación de datos personales en la UE se consolidó. Para realizar una transferencia a un tercer país[49] u organización internacional se debe contar con la evaluación de adecuación de la Comisión Europea. Las decisiones de adecuación están sujetas a un control continuo y se pueden modificar, suspender o derogar si cambian las condiciones[50].

El tercer país u organización internacional debe contar con garantías adecuadas para la protección de datos personales. Por ejemplo, un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos, normas corporativas vinculantes, cláusulas tipo de protección de datos, códigos de conducta y mecanismos de certificación.

---

[48] https://ec.europa.eu/info/sites/default/files/gdpr_factsheet-09_en.pdf
[49] País que no forma parte de la UE, independientemente de que forme parte del Convenio 108.
[50] https://www.boe.es/doue/2016/119/L00001-00088.pdf

En conclusión, el Reglamento estableció reglas más estrictas para los responsables del tratamiento de datos personales sin prohibir el flujo transfronterizo de datos o la utilización de nuevas tecnologías como la nube y expandió los derechos de los titulares para garantizar que su consentimiento sea libre e informado.

El debate público se ha enfocado en la protección de datos personales por el impacto que una vulneración podría tener en los titulares. Sin embargo, existe un gran volumen de datos no personales que diariamente son recabados y procesados a nivel mundial. Esta información es muy importante para la toma de decisiones y debe ser regulado de acuerdo con sus características.

Para este tipo de información -no personal- se aprobó el *Reglamento (UE) 2018/1807 (Free Flow of non-personal Data)*[51]

La finalidad de este reglamento es establecer reglas coherentes con la protección de datos personales bajo el principio de libre circulación de datos no personales en la Unión. Se busca preservar la libertad de las empresas para establecer sus oficinas o servidores en cualquier lugar de la UE sin estar sujetos a requisitos de localización.

Nuevamente, se busca homologar la legislación de la UE para disminuir los costos en el mercado digital y "*eliminar obstáculos al comercio y distorsiones de la competencia como consecuencia de las divergencias existentes entre las normativas nacionales*"[52].

Tres principios se reforzaron a través de este instrumento jurídico:

- La libre circulación de datos no personales en la UE.
- La disponibilidad de los datos no personales para las autoridades competentes.

---

[51] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32018R1807&from=ES

[52] Reglamento (UE) 2018/1807, párrafo 7.

- La portabilidad de datos.

La interacción de este reglamento y el RGPD es muy importante porque en la práctica, se procesan conjuntos compuestos de datos, integrados por datos personales y no personales. No existe una obligación de separar los datos, pero sí de armonizar su tratamiento para garantizar el mayor nivel de protección.

Una de las principales razones de los actores, públicos y privados, para retrasar la adopción de la nube es el riesgo de dependencia con un proveedor. Para mitigar este riesgo, la legislación exige que los proveedores utilicen códigos interoperables que permitan la portabilidad de datos, facilitando a los usuarios decidir qué servicio y proveedor contratar.

Para consolidar este principio, reconocido en el Reglamento 2018/1807, la Comisión Europea impulsó la creación de un grupo conformado por usuarios y proveedores de servicios de la nube llamado Switching Cloud Providers and Porting Data (*SWIPO*). El objetivo de este grupo fue crear códigos de conducta que cumplan con los requerimientos de portabilidad de datos no personales establecidos en el artículo 6 del Reglamento[53].

A través de esta iniciativa se buscó establecer guías para garantizar la interoperabilidad de los sistemas y permitir la portabilidad de la información entre proveedores. Esta iniciativa está abierta para que cualquier organización se adhiera a sus códigos y se comprometa a cumplir con sus estatutos.

Es importante diferenciar las finalidades de los tratamientos de datos personales ya que tienen implicaciones y regulaciones distintas.

El RGPD es aplicable para cualquier tratamiento de datos personales en la UE -o fuera si los titulares son residentes o nacionales de la región- salvo que el tratamiento sea realizado por "*autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas*

[53] https://swipo.eu/

para la seguridad pública"[54]. En estos casos la legislación aplicable es la *Directiva (UE) 2016/680*[55]. El término "autoridades" no sólo se refiere a organismos públicos sino a cualquiera que se le hayan otorgado facultades de autoridad u obligaciones en la materia. Por ejemplo, las instituciones financieras.

Esta directiva establece las garantías mínimas que deben cumplir los Estados miembros, pero no elimina a las legislaciones nacionales que incluso pueden contemplar estándares más altos de protección.

El principio de proporcionalidad se fortaleció, exigiendo que las autoridades especifiquen y justifiquen su decisión; sin que se permita la interconexión de la totalidad de la información.

La cooperación internacional en la prevención y combate de delitos es un elemento clave que justifica la transferencia de información confidencial entre autoridades. Los intercambios de información con la Organización Internacional de Policía Criminal (Interpol) también son regulados por esta directiva.

Se reforzaron los principios de licitud, lealtad y transparencia como ejes de cualquier tratamiento de datos personales y se reconoció la importancia de garantizar los derechos ARCO.

Un elemento muy importante que distingue el tratamiento regulado en esta directiva frente al RGPD es que al ser autoridades investigando delitos, el consentimiento del titular no constituye un fundamento jurídico para el tratamiento.

También prevé la transferencia a terceros países u organizaciones internacionales, pero deberán acreditar un nivel de protección adecuado y la información transferida no podrá utilizarse o almacenarse para otros fines.

---

[54] Directiva (UE) 2016/680, párrafo 11.

[55] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L0680&from=ES

Cualquier procesamiento automatizado de datos que tenga efectos jurídicos adversos para el titular podrá ser impugnado para exigir la intervención humana y el punto de vista del interesado.

En caso de violación de estas disposiciones, los afectados deberán recibir una compensación efectiva por el perjuicio sufrido y se incluyeron sanciones para los responsables, sin importar si son personas físicas, jurídicas, del sector público o privado.

En este instrumento jurídico, el libre tránsito de datos se permite -e incentiva- porque la toma de decisiones informadas es fundamental para la prevención y sanción de delitos que pueden poner en riesgo los derechos fundamentales de otras personas.

En un principio, la *Directiva 2009/136/CE*[56] *(EU ePrivacy Regulation or Cookie Law)* se enfocaba en asegurar un servicio universal de los servicios de comunicación, accesibles para personas con discapacidad, a un precio asequible y con libre acceso a líneas de emergencia. Debido a la naturaleza de los servicios, esta directiva se enfocaba, principalmente, en operadores tradicionales de telecomunicaciones. Sin embargo, su texto se encuentra en constante revisión y en 2009 se modificó para exigir el consentimiento de los usuarios previo a la instalación de *cookies*. De ahí el nombre con el que comúnmente se le identifica.

En los últimos años, nuevas tecnologías han ganado relevancia generando un desfase entre esta regulación y la realidad del almacenamiento y procesamiento de datos. En 2017 se inició un nuevo proceso de modernización.

Los principales cambios son:

- Que la Directiva se convierta en Reglamento y sea vinculante para todos los países de la UE, evitando distorsiones regulatorias por las legislaciones nacionales.

---

56 https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32009L0136&from=en

- Incrementar el rango de aplicación de esta normativa para incluir a proveedores de servicios de comunicación tradicional, desarrolladores de aplicaciones móviles, mensajería instantánea, proveedores de correos electrónicos y empresas de publicidad en línea.
- Regular el uso de *cookies*, transparentar su alcance y favorecer un consentimiento informado.
- Garantizar la privacidad del contenido de las comunicaciones y el metadata[57]. El metadata debe ser anónimo.
- El principio de confidencialidad debe ser el eje rector de cualquier tratamiento de datos, incluso el automatizado.

Esta reforma busca consolidar el marco regulatorio de las telecomunicaciones y la protección de datos personales. Nuevamente, se enfatiza en la necesidad de garantizar la privacidad de las personas y asegurar el tratamiento de datos con fines legítimos sin importar la tecnología utilizada[58].

En este contexto regulatorio y reconociendo los grandes beneficios que genera la adopción de nuevas tecnologías como la nube, los países de la región han publicado códigos de conductas y manuales para acelerar su implementación, especialmente en el sector público.

En 2013, ENISA[59] publicó la *Guía de buenas prácticas para la implementación de la nube en el sector público (Good Practice Guide for securely deploying Governmental Clouds).* Este es un documento muy útil para entender las implicaciones del uso de la nube en el sector público ya que analiza los distintos esquemas de nube gubernamental que han adoptado 23 países de la UE. El objetivo de la guía es ayudar a los Estados miembro a desarrollar una estrategia de implementación de la nube, entender los obstáculos existentes, proponer soluciones

[57] Datos sobre los datos.
[58] https://digital-strategy.ec.europa.eu/en/policies/digital-privacy
[59] La Agencia de la Unión Europea para la Ciberseguridad es un centro de conocimiento especializado que ayuda a sus integrantes a estar preparados para prevenir, detectar y dar respuesta a problemas de seguridad de la información.

y reconocer las mejores prácticas para lograr una implementación similar de la tecnología en la región.

De acuerdo con la guía, la adopción de una nube gubernamental puede fortalecer el contexto de seguridad de los datos, simplificar las interacciones con los ciudadanos y facilitar la implementación de las políticas públicas de la nube.

La nube ofrece los mismos servicios para sector público y privado pero los objetivos -de cada sujeto- son distintos. Una nube gubernamental debe impulsar la estandarización de servicios para aumentar su eficiencia y disminuir los tiempos de respuesta a los ciudadanos. Debe ser vista como una herramienta para la rendición de cuentas y para mejorar el acceso de los ciudadanos a los servicios gubernamentales.

El documento clasifica a los países de acuerdo con su enfoque hacia la implementación de la nube:

- Primeros en utilizarla. Tienen una estrategia para implementar el uso de la nube y han tomado decisiones específicas para implementar una nube gubernamental (Reino Unido, Francia).
- Bien informados. Tienen una estrategia pero la implementación está en etapa de desarrollo (Países Bajos, Alemania, Irlanda, Bélgica)
- Innovadores. No tienen una estrategia clara para implementación de la nube gubernamental pero ya cuentan con algunos servicios que utilizan la nube (Italia, Austria, Portugal, Eslovenia).
- Dudosos. No tienen una estrategia ni servicios relevantes que utilicen la nube (Malta, Chipre, Polonia, Rumania).

En 2018 se aprobó otra guía - *Guía para la implementación de la nube en las instituciones y órganos europeos*[60]- para facilitar la adopción de la nueva tecnología en las autoridades de la UE. Este documento desarrolló herramientas para conocer

[60]https://edps.europa.eu/data-protection/our-work/publications/guidelines/guidelines-use-cloud-computing-services-european_en

los riesgos del tratamiento masivo de datos, el plan de trabajo que deben cumplir para una transición exitosa hacia la nube y qué requisitos se deben establecer en los contratos con proveedores para garantizar la protección de los datos que serán procesados y almacenados a través de la nube.

Esta guía se enfoca en la adquisición de servicios de la nube a través de proveedores privados, por lo que se recalca la importancia de establecer cláusulas contractuales sólidas que especifiquen las responsabilidades de cada parte. También se insistió en la necesidad de aclarar en el contrato que el proveedor debe colaborar con las instituciones para garantizar los derechos ARCO.

Se sugirió adoptar la nube gradualmente para dar tiempo a los encargados de su operación de capacitarse en el uso de la herramienta y se propuso iniciar con operaciones de datos con menor riesgo, datos no personales, hasta asegurar que el servicio cumpla con los controles necesarios.

Esta guía puede ser de gran utilidad para autoridades gubernamentales que inician la transición al mundo digital ya que detalla los elementos y garantías que se deben incluir en los contratos con los proveedores de la nube.

Otra recomendación de la guía es adoptar una estrategia común para todo el gobierno. Esto implica, entre otras cosas, nombrar a una autoridad o institución como la encargada de negociar los términos del servicio. Así, se aumenta el poder de negociación frente a las empresas y se empodera al gobierno y sus intereses.

Este documento se enfoca en la adopción de la nube por autoridades de la UE por lo que sugiere que los servidores de los proveedores se encuentren en la región. Especialmente para asegurar el cumplimiento de las reglas de inmunidad y privilegios de las instituciones europeas[61].

[61] En el Protocolo No 7 de los Privilegios e Inmunidades de Unión Europea, se especifican los privilegios e inmunidades que gozan las instituciones de la UE en el territorio de los países miembro para cumplir con sus responsabilidades.

Dos años después, la Comisión Europea dio a conocer la *Estrategia Europea de datos*[62]. Esta estrategia reconoce que "*las tecnologías digitales han transformado nuestra economía y nuestra sociedad*" y "*que los datos están en el centro de esta transformación*"[63]. Sin embargo, enfatiza que las tecnologías -y su evolución- deben tener como eje rector el respeto de los derechos fundamentales[64].

A través de esta estrategia, se buscó crear un mercado europeo de datos sólido, confiable, competitivo y soberano que permitiera consolidar a la UE como potencia en la adopción y, sobre todo, oferta de estos servicios[65].

Los Estados miembro han establecido acuerdos para impulsar acciones coordinadas que permitan el desarrollo de servicios e infraestructura de nube competitivo y seguro en toda Europa. Incluso se prevé la inversión de dos billones de euros en este proyecto[66].

Existe un área de oportunidad que la Unión Europea quiere aprovechar para asegurar su soberanía en tecnologías de la información. El uso de la nube permitirá mejorar los procesos de tratamiento de datos, favoreciendo la descentralización, disminuyendo los costos e impacto ambiental. Con este proyecto la UE dejará de ser únicamente usuario para convertirse en proveedor de servicios de la nube. La soberanía digital se convierte en un objetivo.

A partir de esta estrategia se han impulsado proyectos y grupos de trabajo para reunir a expertos de todos los sectores y adoptar las mejores prácticas a nivel mundial.

---

62 https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0066&from=EN

63 Comunicación de la Comisión al Parlamento Europea, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Una Estrategia Europea de Datos, página 1.

64 https://digital-strategy.ec.europa.eu/en/policies/strategy-data

65 ISBN 978-92-76-15991-9 doi:10.2775/987881 NA-01-20-096-EN-N

66 https://digital-strategy.ec.europa.eu/en/policies/cloud-computing

La coordinación entre el sector privado y público es fundamental para el desarrollo de una nube europea que aumente la competitividad de la región y asegure su soberanía frente a proveedores de otras regiones. Por esta razón se unieron para emitir la *Declaration Building the next generation cloud for businesses and the public sector in the EU*[67]*.* Este proyecto permitirá a los gobiernos ofrecer servicios públicos más eficientes y mayor seguridad jurídica a los proveedores de los servicios respecto de sus obligaciones[68].

Los países firmantes de esta declaración se comprometieron a:

- Coordinar inversiones públicas y privadas para desarrollar sistemas e infraestructura de la nube competitivos, seguros y responsables con el medio ambiente.
- Impulsar una alianza *European Alliance on Industrial Data, Edge and Cloud*.
- Definir un enfoque y reglas comunes de los servicios de la nube para encontrar soluciones tecnológicas conjuntas e interoperables.
- Impulsar la adopción de servicios de la nube y servidores más eficientes, seguros e interoperables en el sector privado y el sector público.

Como consecuencia de esta declaración se fundó, a principios de 2021, la *Alianza Europea de la Nube y Datos industriales (European Alliance for Industrial Data, Edge and Cloud)*[69] que buscará detallar el plan de trabajo e inversiones necesarias para cumplir con los objetivos de la Declaración. Es un esfuerzo de colaboración a largo plazo en el que participarán representantes de la sociedad civil, expertos, proveedores de servicios y autoridades.

La nube es un elemento habilitador para el desarrollo de otras tecnologías como la inteligencia artificial y la red 5G. De ahí la importancia de consolidar a la UE como un referente en la industria.

---

67 https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-europe

68 Stolton, Samuel. *What's behind the EU's new Cloud Codeo f Conduct?* (2021)

69 https://digital-strategy.ec.europa.eu/en/policies/cloud-alliance

Cada día se generan más datos. El acceso a nuevas tecnologías favorece una descentralización del procesamiento de datos que modificará, en los siguientes años, el mundo digital. Las autoridades europeas consideran que este proyecto puede mejorar el procesamiento de datos sensibles de una forma segura y respetando los derechos fundamentales de sus titulares.

Un elemento muy importante de esta alianza es el trabajo conjunto entre el sector privado y público para lograr un bien común: el desarrollo de una nueva generación de la nube interoperable, segura y responsable con el medio ambiente.

La tecnología sin la confianza del usuario nunca podrá alcanzar su potencial. No es suficiente con emitir normas regulatorias comunes que exijan mecanismos para la protección de datos; es necesario implementar mecanismos de comunicación entre proveedores y usuarios para establecer un vínculo de confianza.

Después de cuatro años de colaboración[70] entre autoridades europeas y empresas proveedoras del servicio de la nube, y con el visto bueno del Comité Europeo de Protección de Datos[71], se publicó el Código de Conducta para los proveedores de servicios de la nube que realicen tratamientos trasnacionales de datos personales (*EU Cloud Codeo of Conduct*) [72].

Este Código desarrolla el artículo 28 del RGPD y es el primer documento reconocido por autoridades nacionales[73] como herramienta para comprobar el cumplimiento de la legislación europea sobre protección de datos personales. Incluye requerimientos específicos que deben adoptar los proveedores del servicio

[70] El primer proyecto del Código se realizó en 2014 pero las mesas de trabajo iniciaron desde la

[71] https://edpb.europa.eu/system/files/2021-05/edpb_opinion_202116_eucloudcode_en.pdf

[72] https://eucoc.cloud/en/home.html

[73] La Autoridad Belga para la protección de datos personales aprobó el Código en mayo de 2021.

para cumplir con los estándares del RGPD y estándares internacionales como ISO27001 y 27018[74].

El Código es aplicable para proveedores de los tres servicios de la nube -IaaS, PaaS y SaaS- y la declaratoria de cumplimiento la emite una organización independiente encargada del monitoreo constante del cumplimiento del Código[75].

De acuerdo con los documentos y pruebas que remitan los proveedores, el Código reconoce tres niveles de cumplimiento:

1. Primer nivel, el solicitante realiza una revisión interna de sus procesos y envía la información necesaria para acreditar su cumplimiento.
2. Segundo nivel, el solicitante realiza una revisión interna de sus procesos y además realiza auditorías externas parciales a sus procesos.
3. Tercer nivel, el solicitante somete todos sus procesos a una auditoría externa y remite los resultados.

Las diferencias en los niveles de cumplimiento únicamente se basan en los documentos que utilizaron como fundamento para la certificación ya que en los tres casos se exige que cumplan con todas las disposiciones del Código. Los proveedores pueden adherirse con uno o la totalidad de los servicios que ofrecen.

A través de la implementación de este Código, se busca aumentar la transparencia y rendición de cuentas de los proveedores de servicios de la nube.

Al igual que en el caso estadounidense, la actividad jurisdiccional en la UE ha sido determinante para interpretar y adecuar la legislación a las nuevas tecnologías.

[74] https://eucoc.cloud/en/about/about-eu-cloud-coc/
[75] Scope Europe es una organización sin fines de lucro establecida en Bélgica, que fue designada como autoridad responsable de certificar el cumplimiento de los proveedores con el Código.

La sentencia del Tribunal de Justicia de la Unión Europea C-311/18, *Facebook Ireland v Shrems* (*Sentencia Schrems II*)[76]es de gran relevancia porque establece límites a las injerencias de autoridades extranjeras en la confidencialidad de datos por temas de seguridad nacional, defensa y seguridad del Estado.

En este caso, un ciudadano de la UE alegó que se estaban transfiriendo datos personales a un tercer país -EUA- que no cumplía con los principios y estándares del RGPD y, por lo tanto, solicitaba la prohibición de futuras transferencias.

Las cláusulas tipo han sido utilizadas como mecanismos para transferir datos personales a países fuera de la UE. Especialmente a países que se ha reconocido cuentan con un nivel de protección adecuado de acuerdo con los estándares del RGPD. En el caso, una vez realizadas las transferencias -a través de estas cláusulas- a servidores estadounidenses, las autoridades nacionales podían acceder a datos confidenciales, afectando el derecho a la privacidad de ciudadanos no estadounidenses, bajo el argumento de seguridad nacional.

El TJUE resolvió que los programas de vigilancia de las autoridades estadounidenses y la violación de la confidencialidad de la información bajo el argumento de seguridad nacional, no cumplía con el principio de proporcionalidad ni garantizaba una protección judicial efectiva de los derechos de los titulares frente a este tratamiento de datos.

A pesar de las consecuencias políticas de esta decisión, sus implicaciones jurídicas son fundamentales para el empoderamiento de las personas, frente a empresas y autoridades, respecto al uso y tratamiento de su información.

Proyectos nacionales

[76] Sentencia aprobada en julio de 2020 https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62018CJ0311&from=es

En este contexto político y normativo, varios países han implementado estrategias digitales y políticas públicas para la adopción de la nube en el sector público. A continuación, se mencionan algunos casos.

Italia

Con base en la Estrategia de Crecimiento Digital y el Plan de Tecnologías de la Información para la Administración Pública 2017-2019, el gobierno italiano emitió una estrategia de la nube que establece los lineamientos y procesos que deben cumplir los actores públicos y privados para proveer de servicios de la nube a la administración pública[77].

El objetivo es establecer reglas claras que permitan a las instituciones que integran la administración pública adoptar esta tecnología a través de servicios homogéneos que puedan ser interoperables.

Polonia

Desarrolló un programa denominado "*Common State IT Infraestructure" (WIIP)*[78] que busca difundir los beneficios de estas nuevas tecnologías, las implicaciones y retos. Además, contempla programas para la inversión en el suministro de infraestructura de tecnologías de la información.

Este programa prevé la construcción, desarrollo y mantenimiento de la nube de computación gubernamental (*RChO*)[79] como una nube comunitaria de la administración pública. También permite a las entidades de la administración pública adquirir servicios de procesamiento en nubes de computación pública (*PCHO*). Esta nube es pública con servicios de proveedores comerciales que cumplen con los requisitos de confidencialidad, integridad y disponibilidad

[77] https://www.agid.gov.it/en/infrastructures/pa-cloud
[78] https://chmura.gov.pl/informacje/projekt-wspolna-infrastruktura-informatyczna-panstwa
[79] https://chmura.gov.pl/informacje/rzadowa-chmura-obliczeniowa

necesarios para garantizar la seguridad de la información de la administración pública[80].

Bélgica

Como resultado de la colaboración entre distintas instituciones públicas que podrían beneficiarse de esta transición tecnológica, se implementó el programa "*G-Cloud*".

Es una nube híbrida que ofrece servicios de empresas privadas y servicios alojados en centros de datos estatales. La adopción de la nube es voluntaria para todas las instituciones gubernamentales.

La nube inició operaciones en 2015 y ha estado sujeta a constantes procesos de revisión y mejora[81].

Estonia

Es el país más avanzado en la implementación de tecnologías de la información a las actividades y servicios gubernamentales. Actualmente, el 99% de los servicios públicos están disponibles en línea[82].

El gobierno apostó a la transparencia como el mecanismo idóneo para construir una relación de confianza con la ciudadanía y la consolidación del Estado de derecho.

La adopción de la nube gubernamental ha permitido la implementación de servicios electrónicos y soluciones digitales que disminuyen los costos y tiempos burocráticos.

Además, permite el uso y aprovechamiento de herramientas que facilitan la toma de decisiones informadas. La protección de los datos personales ha sido una de sus principales preocupaciones al desarrollar esta solución tecnológica por lo

[80] https://chmura.gov.pl/informacje/publiczna-chmura-obliczeniowa
[81] https://www.gcloud.belgium.be/fr/home
[82] https://e-estonia.com/solutions/e-governance/government-cloud/

que todos sus sistemas y procesos de tratamiento de datos fueron creados de acuerdo con los parámetros de la legislación europea.

La descentralización de la tecnología disminuye los riesgos de interrupción del servicio y pérdida de la información e impulsa el desarrollo de otras regiones en el país, por esta razón se prevé que uno de los dos centros informáticos se encuentre fuera de la capital. A largo plazo, se pretende establecer embajadas electrónicas en países con regulaciones similares y buenas relaciones internacionales con Estonia.

Esta nube fue posible gracias a la colaboración entre el gobierno y compañías privadas que alinearon sus objetivos para mejorar el desempeño de las oficinas gubernamentales y, más importante, mejorar la calidad de vida de los ciudadanos.

Francia

En 2021, el gobierno francés anunció su Estrategia Nacional de la Nube cuyo objetivo será la transformación del Estado y sus actividades al mundo digital[83].

La adopción de esta tecnología por parte del sector público inició desde 2018 cuando se publicaron los tres servicios de la nube que utilizaría el gobierno. El primero, sería un círculo interno con datos sensibles y regulado por estándares altos de confidencialidad. El segundo, sería una nube desarrollada por un socio comercial adaptada a las necesidades gubernamentales y con datos menos riesgosos. El tercero, sería una nube externa de uso genérico. Esta visión apoyaba el uso de la nube en el sector público y la reconocía como un eje esencial para la transformación del Estado.

El objetivo a largo plazo de la Estrategia es posicionar a Francia como un proveedor de tecnología a nivel mundial, especialmente de servicios de la nube, en concordancia con los niveles más altos de protección de datos personales.

83 https://observatoire-fic.com/en/national-cloud-strategy-is-france-ready-to-enter-the-era-of-liquid-computing/

Portugal

En 2020 se publicó el *Plan de Acción de la Transición Digital de Portugal*[84]. Su finalidad es empoderar a los ciudadanos en la era digital, impulsar la transformación de las empresas y promover la digitalización del Estado.

Algunos de los programas que implementará el gobierno son:

- Crear una identificación digital que permita a los ciudadanos no residentes en el país a utilizar servicios públicos.
- Simplificar y digitalizar los 25 servicios más utilizados por la población.
- Crear una Estrategia de la nube para la administración pública.
- Simplificar, digitalizar y transparentar los procesos de adquisición de bienes y servicios.

Austria

El gobierno austriaco fue uno de los primeros en adoptar el gobierno electrónico para disminuir la burocracia y lograr una administración más eficiente y cercana a la sociedad.

Con la iniciativa *ö-Cloud*[85], se permitió el tratamiento de datos a través de procesos seguros que cumplan con los estándares de la UE. El objetivo es fortalecer al país como un lugar seguro para la ubicación de centros de datos.

Reino Unido

La adopción ordenada y gradual de la nube es una prioridad para el Reino Unido. Para su gobierno, los beneficios de esta tecnología[86] únicamente se lograrán si se garantizan los estándares de protección de datos y las necesidades de cada

---

84 https://eportugal.gov.pt/en/noticias/governo-lanca-plano-de-acao-para-a-transicao-digital

85 https://www.digitalaustria.gv.at/initiativen/verwaltung/verwaltungs-projekte/OECloud.html

86 El gobierno del Reino Unido incluso reconoce que se puede garantizar una mayor seguridad de los datos a través de esta tecnología.

institución. Tomando en cuenta la opinión de expertos de diversos sectores gubernamentales[87], el gobierno del Reino Unido emitió "*The One Government Cloud Strategy*[88]". Esta guía analiza los principales retos en la implementación de la nube en el sector público y posibles soluciones. La gradualidad es un elemento muy importante para implementar esta tecnología de forma exitosa. De acuerdo con la guía, la transición debe ser considerada como un objetivo de largo plazo para garantizar que se cubra cualquier contratiempo y se garantice la máxima protección de datos personales.

En la estrategia se aclara que la información oficial puede ser almacenada y procesada en servidores fuera del territorio, pero impone limitaciones para la información clasificada como secreta o ultrasecreta.

Para acelerar la adopción de la nube, el gobierno británico implementó, en 2019, la política "*Cloud First Policy*"[89] que significa privilegiar el uso de la nube frente a otras tecnologías.

Un ejemplo de éxito ha sido la implementación de una nube híbrida en el sistema de trenes. Esta nube tiene varios proveedores para evitar una dependencia con efectos nocivos para el servicio público. Otra de las prioridades fue la capacitación del personal para potencializar sus beneficios[90]. La transparencia en la transición también fue fundamental para convencer a actores relevantes de los beneficios de la decisión y desmitificar los riesgos de seguridad de la nube.

El uso de la nube no sólo es el futuro de las telecomunicaciones sino un área de oportunidad para los gobiernos. Los países de Europa han identificado esta oportunidad y buscarán consolidar a la región en este nuevo sector que ofrecerá

---

[87] https://technology.blog.gov.uk/2020/03/31/introducing-the-gov-uk-cloud-guide/

[88] https://www.gov.uk/government/publications/cloud-guide-for-the-public-sector/cloud-guide-for-the-public-sector

[89] Esta política significa que ante un problema o nuevo servicio siempre se debe considerar a la nube como la primera herramienta para solucionarlo u ofrecerlo.

[90] https://www.gov.uk/government/case-studies/how-network-rail-implemented-its-hybrid-cloud-strategy

sus servicios de forma transversal a todas las industrias y servicios. Además, reconocen que el uso de esta tecnología no excluye los máximos niveles de protección de datos e, incluso, incentiva una mayor transparencia respecto al tratamiento de los datos y sus fines.

Asia

Asia es una región en la que en términos generales el uso de la nube se encuentra en contínuo incremento.

En el continente asiático, paises como Australia, Filipinas y Singapur han adoptado la política *Cloud first* en el sector público, que alienta y en algunos casos mandata el uso de la nube en los ámbitos gubernamentales.[91]

De acuerdo con el Índice 2020 de la *Asia Cloud Computing Association*, en el continente asiático las regulaciones relativas a la nube abordan tres aspectos fundamentales: a) privacidad, b) entorno de regulación gubernamental y c) protección de la propiedad intelectual.[92]

El primer aspecto, es decir el relativo a la privacidad, implica que los servicios en la nube requieren de la libre circulación de los datos en un entorno legal de protección y privacidad.

El entorno de regulación gubernamental, por otra parte, supone que los gobiernos nacionales cuenten con modelos regulatorios que permitan y promuevan el uso de tecnologías de la nube en el sector público.

---

[91] Asia Cloud Computing Association. *From vision to procurement: principles for adopting cloud computing in the public sector*. 2019.
[92] Asia Cloud Computing Association. *Cloud Readiness Index 2020*. 2020. Página 19.

Finalmente, la protección de la propiedad intelectual conlleva la existencia de normas que refrenden esta clase de derechos como un pre requisito para la implementación de la innovación tecnológica a través de la nube.

En este rubro, la puntuación que la *Asia Cloud Computing Association* asignó en 2020 a los países de la región, en el rubro de regulación de la nube (*Cloud Regulation*) colocó en los primeros lugares a Singapur, Japón, Australia, Nueva Zelanda y Hong Kong, en ese orden.

En el aspecto específico del desarrollo de normas nacionales para el uso de la nube en el sector público, el índice asiático mencionado reporta que Corea del Sur ocupa el primer lugar, seguido de Australia, Singapur, Taiwan y Hong Kong, en ese orden.

No hay que perder de vista que una nota distintiva del uso de la nube en el continente asiático es que en términos generales no existen leyes específicas e integrales sobre la nube, sino que predominan los ordenamientos sobre privacidad y datos personales, así como regulaciones administrativas o de *soft law* que se refieren a sectores económicos, industriales o gubernamentales; y que tangencialmente abordan cuestiones como la contratación y la seguridad de la información en la nube.

El siguiente cuadro indica cuáles son ámbitos en que se han desarrollado esta clase de regulaciones sectorizadas:[93]

Japón	Sector médico, sector financiero, sector público, seguridad cibernética para agencias gubernamentales, protección de datos.
Singapur	Sector financiero, sector de los medios de información y comunicación, protección de datos.

[93] https://cloud.google.com/security/compliance/offerings#/regions=Asia_Pacific

Australia	Sector financiero, sector público, ley de privacidad, banca, seguros, jubilaciones.
Malasia	Sector financiero, sector público.
Filipinas	Sector financiero.
Korea	Sector financiero, internet y seguridad de la información.
Taiwán	Sector financiero.
Indonesia	Comercio electrónico, servicios públicos, sector financiero.
Hong Kong	Servicios financieros, protección de datos.
Indonesia	Operaciones comerciales, sector público.
India	Sector financiero, sector público.

No hay que perder de vista, sin embargo, que en Asia también se han desarrollado políticas que dificultan el libre tránsito de datos a través de la imposición de medidas de localización de datos dentro de las fronteras nacionales de China, Hong Kong, India, Malasia, Tailandia y Vietnam.[94] Es decir, que algunos gobiernos nacionales han implementado medidas restrictivas del flujos transfronterizo de datos.

Asia es una región de movimiento dinámico en la implementación y regulación de la nube, pero también es una zona de alta tensión entre las posturas de franca apertura *versus* las medidas restrictivas basadas en la localización de datos y en el acotamiento del flujo transfronterizo.

[94] Asia Cloud Computing Association. *Cloud Readiness Index 2020*. 2020. Página 8.

Australia.

En Australia se promulgó el 2018 una estrategia para la adopción de la nube por parte de las entidades del sector público. Se trata de la *Australia´s Secure Cloud Strategy,* cuya premisa fundamental está en el reconocimiento de que la implementación de la nube en el sector público será generadora de una mejora contínua en la prestación de los servicios del gobierno.

La estrategia australiana se sustenta en nueve puntos clave:[95]

a) Las agencias gubernamentales desarrollarán sus propias estrategias de cómputo en la nube, de acuerdo a sus necesidades.
b) Siete principios sirven como guía de las agencias gubernamentales en el desarrollo de sus estrategias de cómputo en la nube:[96]
    i. Tomar decisiones basadas en riesgos en lo que se refiere a las necesidades de seguridad en la nube.
    ii. Diseñar servicios de la nube por parte de las agencias gubernamentales.
    iii. Utilizar los servicios de nube pública por *default,* es decir adoptar por regla general soluciones basadas en servicios de nube .
    iv. Utilizar la nube tanto como sea posible.
    v. Utilizar los servicios "*tal como vienen*".
    vi. Aprovechar al máximo las prácticas de automatización de la nube.
    vii. Monitorear el estado y el uso de los servicios de nube en tiempo real.
c) La estrategia se desarrollará con base en un modelo de certificación.
d) Se alineará la adquisición de servicios en la nube con las recomendaciones de adquisición de tecnologías de la información y comunicaciones.
e) Un marco de evaluación común hará pondrá en claro los requerimientos del sistema en la nube.

[95] https://www.dta.gov.au/our-projects/secure-cloud-strategy
[96] Commonwealth of Australia (Digital Transformation Agency). *Secure Cloud Strategy*. 2021.

f) Un nuevo modelo de contratos aclarará las responsabilidades de los proveedores de la nube.
g) La *Digital Transformation Agency* desarrollará una plataforma para compartir conocimientos y experiencia sobre productos y servicios en la nube.
h) Se incrementarán las habilidades y la experiencia en la nube en el servicio público.
i) Se desarrollarán plataformas compartidas que pueden usar diferentes servicios, reduciendo la duplicación.

El modelo australiano se distingue por la adopción de la política pública conocida como *Cloud first*[97], la cual constituye una estrategia desarrollada desde 2014 para migrar hacia la nube aquella información genérica y de bajo riesgo en posesión de los entes gubernamentales.[98]

La principal autoridad rectora es la *Digital Transformation Agency*, que define su misión en facilitar la adopción de la nube en el sector gobierno, con el fin de aumentar la productividad y brindar mejores servicios.

Además, en la transición hacia la nube por parte de las agencias gubernamentales australianas, destaca un caso de orden local: Nueva Gales del Sur.[99]

En 2021, la entidad denominada *Information and Privacy Comission de New South Wales* relató su experiencia en esa transformación hacia el uso de la nube en el sector público.[100]

---

[97] Asia Cloud Computing Association. *Cloud Readiness Index 2020*. 2020.
[98] https://www.digitalrealty.com/blog/why-adopting-a-cloud-first-policy-is-the-right-move-for-the-australian-government
[99] New South Wales Information and Privacy Comission, *Guide – Transition to the cloud: Managing your agency's privacy risks*, May 2021
[100] https://iapp.org/media/pdf/resource_center/new_south_wales_transition_to_cloud_managine_agency_privacy_risks.pdf

Como misión hacia 2023, el gobierno local se fijó el objetivo de que todas las agencias gubernamentales de Nueva Gales del Sur utilicen la nube pública para un mínimo del 25% de sus servicios de tecnologías de la información comunicaciones.

La estrategia dio inicio una década atrás, con una estrategia de almacenamiento de datos en una nube privada, que ahora se se está expandiendo hacia la nube para el sector público.

La vision del gobierno se expresa así: "*Permitir la adopción en todo el gobierno de los servicios de nube pública de una manera alineada y segura, para acelerar la innovación, modernizar la prestación de servicios e impulsar mejores resultados para los ciudadanos de Nueva Gales del Sur*".

El estado de Nueva Gales del Sur en Australia, ejemplifica con claridad el caso de una transición hacia la nube por parte de las agencias gubernamentales.

En síntesis, la transición hacia la nube forma parte de la agenda de transformación digital de las agencias gubernamentales australianas, bajo la condición fundamental de que ello tendrá un efecto positivo en los servicios públicos.

Esto incluye asegurar procesos de adquisición transparentes y justos, inclusiones de contratos adecuadas, gestión de contratos eficaz, gestión de riesgos durante la vida del trabajo y procedimientos de terminación adecuados. También implica que cuando el proveedor de servicios de la nube acceda, mantenga, use o divulgue información personal para brindar los servicios, la privacidad debe convertirse en una consideración clave en todos los aspectos de la contratación.

Japón.

En términos generales, Japón cuenta con un robusto sistema de regulación que facilita la implementación de la nube.

En primer lugar, Japón ha tomado medidas activas para facilitar el libre flujo de datos. Es decir, que el marco normativo y de políticas públicas japonesas apoya y promueve en general el libre flujo de información más allá de las fronteras. [101]

Además, no existen requisitos de localización de datos para toda la economía, ni específicos por sector.

Cuatro notas distintivas son la que tiene el caso japonés:

- La Ley de Protección de la Información Personal facilita las transferencias de datos transfronterizas. Para ello en 2017 se aprobaron enmiendas a la Ley de Protección de Información Personal, que prescriben que para las transferencias de información personal a un tercero en un país extranjero se debe considerar que el país de destino tenga un nivel aceptable de protección de datos, que se garantice el mismo nivel de protección de datos que en Japón o que la persona interesada ha dado su consentimiento para la transferencia.
- Los flujos de datos transfronterizos se consideran cruciales para el logro de los objetivos socioeconómicos de Japón y revitalizar la economía.[102]
- El gobierno japonés ha adoptado el sistema de Reglas de Privacidad Transfronterizas de la APEC, que postula el compromiso voluntario de establecer estándares de regulación de privacidad con el objetivo de facilitar los flujos de datos y el comercio entre las economías de la APEC.
- En 2015 Japón formuló su declaración para convertirse en la nación de tecnologías de la información más avanzada del mundo.

[101] Asia Cloud Computing Association. *Cross-Border data Flows: A review of the regulatory enablers, blockers, and key sectoral opportunities in five asian economies: India, Indonesia, Japan, the Philiphines, and Vietnam.* 2018. Página 38.

[102] Asia Cloud Computing Association. *Cross-Border data Flows: A review of the regulatory enablers, blockers, and key sectoral opportunities in five asian economies: India, Indonesia, Japan, the Philiphines, and Vietnam.* 2018. Página 35.

En la puesta en marcha de lo anterior, la autoridad relevante es el *Ministry of Internal Affairs and Communications*, que dentro de sus funciones principales tiene la de promover la digitalización del país.

Así, en junio de 2021 dicha autoridad reportó que, conforme a un estudio realizado en 2020, la tasa de introducción de servicios de computo en la nube en las empresas en Japón aumentó a casi el 70%; y que aquellos que usan la nube reconocieron los méritos de ésta, incluido que no está sujeta a ubicaciones o tipos de equipos específicos y la facilidad de subcontratar activos y servicios de mantenimiento. El 87.1% de las empresas que introdujeron la computación en la nube reconocieron que era efectiva o algo efectiva.[103]

Japón impulsa la adopción de la nube en el sector público. Para ello, en junio de 2018 se aprobó la Política de adopción de la nube para los sistemas de información gubernamentales, que en consonancia con el principio *Cloud first* plantea el uso de la nube como política básica.

Por ejemplo, la digitalización de la industria de la salud de Japón se considera fundamental para la sostenibilidad de su plan de seguro médico público. En este ámbito, en 2015, el Ministerio de Salud de Japón anunció la eliminación de las barreras regulatorias a la telemedicina en un movimiento para estimular a nuevas empresas; y en 2017 se publicó la Ley de Infraestructura Médica de Próxima Generación, para promover activamente el uso seguro de datos de atención médica anonimizados y así desarrollar el sector.

Por otro lado, en el terreno educativo desde 2016 se creó un Consejo de la Educación en la Nube, con la finalidad de promover la cooperación y coordinación de proveedores de servicios educativos en la nube y difundir los servicios de educación en la nube en todo Japón.

---

103 https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pressrelease/2021/6/18_07.html

Además, existe una visión de futuro hacia 2030 enfocada en la realización de todos los beneficios económicos de las tecnologías digitales.

Hong Kong.

Hong Kong representa un modelo de regulación de protección de datos altamente desarrollado en la región Asia Pacífico.

La *Personal Data (Privacy) Ordinance* es la regulación vigente en Hong Kong, expedida en 1995 y reformada en 2012 y 2021. Se trata de una regulación aplicable tanto al sector público como al privado, que postula la neutralidad tecnológica y la preeminencia de seis principios rectores en la materia de protección de datos:

1. Propósito y forma de recolección de datos.
2. Precisión y duración de la retención de datos.
3. Uso de datos.
4. Seguridad de datos.
5. Apertura y transparencia.
6. Acceso y corrección.

Por cuanto al uso de la nube, tanto las reglas como los principios establecidos en la *Personal Data (Privacy) Ordinance* constituyen un marco de referencia obligado para la implementación de esta clase de servicios.

De tales principios y reglas se derivan las siguientes directrices para el uso de la nube:[104]

a) Principios:

- En lo que se refiere a la precisión y duración de la retención de datos.- cuando un usuario contrata a un procesador de datos, ya sea dentro o fuera de Hong Kong, debe adoptar medidas contractuales para evitar que los datos

104

https://www.pcpd.org.hk//english/resources_centre/publications/files/IL_cloud_e.pdf

personales transferidos se mantengan más tiempo del necesario en el procesamiento.

- Por cuanto al uso de datos.- éstos no deben usarse para un nuevo propósito a menos que se obtenga el consentimiento expreso y voluntario del interesado.
- En materia de seguridad de los datos.- se requiere que el usuario adopte todas las medidas razonablemente prácticas para garantizar que los datos personales que posee estén protegidos contra el acceso, procesamiento, borrado, pérdida o uso no autorizado o accidental.
- En cuanto a la contratación.- si se contrata a un procesador de datos dentro o fuera de Hong Kong para procesar datos personales, se deben adoptar medidas contractuales para evitar el acceso, procesamiento, borrado, pérdida o uso no autorizado o accidental.

b) Reglas de la *Personal Data (Privacy) Ordinance:*

- Cualquier violación de datos o uso indebido de éstos por parte del contratista (proveedor de nube) será tratado como realizado por el usuario de datos así como por su contratista. En otras palabras, un usuario de datos será responsable de los actos realizados por su proveedor de servicios de nube.
- Los usuarios de datos deben proteger y prevenir el uso indebido de los datos personales que les confían los interesados, independientemente de si dichos datos personales se almacenan dentro de las propias instalaciones de los usuarios o se subcontrata a proveedores en la nube.
- Para los proveedores de nube que tienen centros de datos distribuidos en múltiples jurisdicciones, los datos personales que se les confían pueden fluir de una jurisdicción a otra. No obstante, se debe precisar que está próxima a entrar en vigor en una ordenanza para restringir la transferencia de datos personales a lugares fuera del territorio de Hong Kong.
- Si los usuarios de datos ubicados en Hong Kong permiten que los datos personales recopilados por ellos se transfieran a lugares fuera de Hong Kong, deben asegurarse de que dichos datos se traten con un nivel de protección similar, como si residieran en Hong Kong.

Además, en Hong Kong se reconoce que la implementación de estándares ISO proporciona una referencia para ayudar a los usuarios de datos a seleccionar a los proveedores de servicios de nube.

La autoridad relevante es la *Office of the Privacy Commissioner for Personal Data*, que es una instancia independiente en materia de protección de datos personales, que tiene facultades para interpretar la legislación y emitir directrices relativas al uso de la nube.

Nueva Zelanda.

Nueva Zelanda, al igual que otras naciones de la región Asia – Pacífico, es un postulante de la política pública *Cloud first*, en aras de la innovación digital.

En Nueva Zelanda, una de las premisas regulatorias consiste en reconocer que los servicios de nube de proveedores globales son más seguros que los tradicionales sistemas de tecnología de la información. Esto en razón de su especialización, economía de escala, capacidad de infraestructura y prácticas para el manejo de riesgos, entre otros factores.[105]

La base regulatoria a partir de la cual emanan directrices para la implementación de la nube es la *Privacy Act,* que se aplica a personas, empresas y organizaciones de Nueva Zelanda. La Ley, emitida en 2020, incluye principios de privacidad acerca de cómo se puede recopilar, usar, almacenar y divulgar la información personal.

La autoridad relevante es el *Privacy Commissioner*, cuya función principal es desarrollar y promover una cultura en la que la información personal sea protegida y respetada. Adicionalmente, el *New Zealand Media Council* es una instancia independiente que puede conocer de quejas en materia de privacidad en contra de

[105] Asia Cloud Computing Association. *From vision to procurement: principles for adopting cloud computing in the public sector.* 2019. Página 10.

la prensa y las plataformas de medios digitales que no están cubiertas por la Ley de Privacidad.

Por su parte, los tribunales han desarrollado precedentes en materia de privacidad, conforme a los cuales existe el derecho de una persona a demandar a otra por la violación de su privacidad (*Hosking v Runting*).

Dentro de las medidas que ha adoptado Nueva Zelanda en su proceso de conversión hacia la preeminencia de la nube, se encuentran:

- El establecimiento, del deber de revelar las transferencias de datos hacia otras jurisdicciones, así como satisfacer requisitos de *due diligence* o auditoría (2020).
- La obligación de realizar una evaluación de impacto de privacidad.
- El deber de asegurarse de que la información personal enviada al extranjero, a través del flujo transfronterizo de datos, esté sujeta a salvaguardas de privacidad similares a los de Nueva Zelanda. En este aspecto, una empresa u organización puede divulgar información personal a otra organización fuera de Nueva Zelanda si la entidad receptora: a) está sujeta a la *Privacy Act* por ser una agencia de Nueva Zelanda o agencia extranjera que opera en Nueva Zelanda; b) se compromete contractualmente a proteger la información o está sujeta a leyes de privacidad con garantías comparables a las de la *Privacy Act*.

Corea del Sur.

En Corea del Sur se postula como objetivo regulatorio el éxito de la cuarta revolución industrial y de la innovación digital. Se persigue la construcción de infraestructura y de servicios innovadores, basados en nuevas tecnologías.

En 2015, la Asamblea Nacional de Corea del Sur promulgó el *Cloud Computing Act*, que entre otras cosas, impulsó el uso de la nube en las instituciones públicas, con el propósito de eficientar sus costos y mejorar su operación.

También en 2015 se promulgó la *Act on the Development of Cloud Computing & Protection of Its Users* y se anunció un Plan de Activación de la Computación en la Nube.

En términos generales dicho marco legal tiene el propósito de promover el desarrollo de la industria de la computación en la nube y proporcionar un entorno de uso seguro.

De acuerdo con el *Korea 2018 Internet White Paper*,[106] Corea del Sur representa el 0.6% del mercado mundial de la computación en la nube; pero se prevé que el mercado nacional de la computación en la nube registre una tasa de crecimiento promedio anual del 14.8%, para 2021 (IDC, Junio de 2017).

El mismo reporte indica que el mercado de la computación en la nube en el mundo se está centrando en SaaS (*Software as a Service*), pero que el mercado nacional hasta 2017 se había concentrado en IaaS (Infraestructure as a Service). Incluso el informe reconoce que la velocidad de expansión de la computación en nube en el mercado nacional sigue siendo lenta.

En términos regulatorios, las autoridades relevantes en Corea del Sur son: a) *Korea Internet & Security Agency, b)* P*ersonal Information Protection Comission; y c)Korea Communications Commis*sion.

La nota distintiva del caso coreano para el uso de la nube es que la *Korea Internet & Security Agency* actualmente hace necesaria una certificación que incluye la separación física de la red, la localización de datos y el uso de algoritmos locales.

[106] Korea Internet and Security Agency. *Korea 2018 Internet White Paper.* 2019.

Conclusiones y recomendaciones para el caso mexicano.

De acuerdo con la experiencia internacional, la adopción del uso de la nube genera ahorros económicos, disminuye el impacto ambiental del mundo digital y, en muchos casos, garantiza una mayor seguridad de la información. La adopción de esta tecnología ha demostrado mejorar el desempeño de las funciones gubernamentales a través de procesos más eficientes y menos costosos. Para implementar esta tecnología en el sector público mexicano es importante considerar las coincidencias en las estrategias públicas de los países analizados y adoptar los procesos exitosos.

A continuación, se presenta un listado de conclusiones y recomendaciones de índole regulatorio para la implementación de la nube en el sector público mexicano:

1. Se debe recalcar que no todos los sistemas de información cuentan con datos personales. Existen sistemas con grandes volúmenes de datos no personales que pueden ser de gran utilidad para las autoridades y sus procesos de decisión que se beneficiarían del procesamiento a través de los servicios de la nube.
2. Las autoridades deben analizar la información en sus sistemas para determinar su clasificación de acuerdo con las leyes mexicanas. Es decir, distinguir entre sistemas con información pública, personal, reservada o relacionada con temas de seguridad nacional.
3. El uso de la nube debe ser impulsado como una política pública basada en el principio *Cloud first*.
4. Es indispensable establecer canales de comunicación y coordinación entre las instancias legislativas, los órganos reguladores, los entes públicos ejecutivos y los agentes económicos, para instaurar reglas generales, estándares sectorizados y generar confianza en la nube.

5. También es aconsejable la definición de estándares técnicos claros y verificables para mayor seguridad de proveedores y usuarios.
6. Como lo señaló José Manuel Pliego Ramos en el Seminario "*Administración pública, derechos y uso de la nube en México*" (IIJ-UNAM), el libre flujo de datos es la tendencia internacional respecto del uso de la nube. Incluir prohibiciones a la geolocalización de centros de datos sería contrario a los compromisos internacionales adoptados por México.
7. De acuerdo con la *Asia Cloud Computing Association*, la regulación de la nube debe ser tecnológicamente neutral. Esto significa, conforme a la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales Convención sobre Comunicaciones Electrónica, que las reglas "*no dependen de la utilización de determinados tipos de tecnología ni la presuponen y podrían aplicarse a la comunicación y al archivo de cualquier tipo de información*" [107].
8. La transición debe ser gradual. Se sugiere iniciar la transición, como lo hizo Canadá, con sistemas que no tengan información clasificada. Así se podrán demostrar los beneficios del servicio, construir confianza en los actores gubernamentales y la sociedad y familiarizar a los servidores públicos con las nuevas tecnologías.
9. Es conveniente implementar una evaluación sectorizada, previa a la adopción de la nube, para así establecer los requerimientos específicos que se necesitan dependiendo del tipo de información que será alojada en ésta y los procesamientos que se quieran realizar. También se deben considerar los servicios requeridos por las distintas instancias gubernamentales, en atención a las características de sus funciones, de los servicios públicos que prestan y al marco jurídico que les aplica.
10. Es muy importante que se designe a un representante del sector público. Una dependencia que pueda negociar a nombre de toda la administración para fortalecer la postura del sector público frente a los proveedores de servicios

[107] Naciones Unidas. *Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales*. 2017. Página 29.

y garantizar que las cláusulas contractuales cumplan con el marco regulatorio nacional e internacional.

11. Especificar en las cláusulas contractuales las obligaciones y responsabilidades de cada parte, durante la vigencia del contrato y una vez terminada la relación contractual. Esta definición no es excluyente de la obligación de las partes de cumplir con el marco regulatorio.
12. La tecnología evoluciona rápidamente por lo que se sugiere regular el uso de la nube a través de principios, como en el caso estadounidense y europeo, para evitar que rápidamente sea superada por los avances tecnológicos.
13. Las directrices y códigos de conducta han sido herramientas regulatorias flexibles y eficaces para enfrentar las innovaciones tecnológicas y las diferencias sectoriales.
14. Los proveedores del servicio de la nube deben ser muy claros y transparentes respecto al flujo de información -incluido el flujo transfronterizo-, medidas de seguridad implementadas y procesamiento de la información.
15. Se enfatiza la necesidad de una constante comunicación con los proveedores de servicio que permitan a las autoridades gubernamentales monitorear y vigilar el cumplimiento de las cláusulas contractuales.
16. El sector público debe tener identificadas las jurisdicciones de escasa protección de datos; y de altos riesgos jurídicos, técnicos, políticos o criminales para exigir mayores controles de seguridad en caso de que el proveedor opere en esas regiones.
17. En ciertos ámbitos del sector público, como por ejemplo aquellos en los que se ve involucrado el tratamiento de datos personales patrimoniales o financieros, es conveniente que la regulación establezca procesos claros o un sistema de autorización para la adopción de servicios de la nube.[108]

[108] Asia Cloud Computing Association. *Asia´s Financial Services on the Cloud 2018. Regulatory landscape impacting the use of cloud by financial services institutions in Asia*. 2018. Página 7.

18. Se sugiere que las instancias generadoras de políticas públicas adopten las siguientes recomendaciones al momento de redactar las estrategias o documentos base:[109]
    a) Reconocer expresamente la mayor seguridad ofrecida por los sistemas de la nube.
    b) Establecer criterios apropiados de clasificación de datos, acordes a la legislación nacional.
    c) Establecer como requisito la realización de la debida diligencia respecto de las prácticas y políticas de privacidad de datos implementadas por los prestadores de servicios de nube.
    d) Establecer reglas para monitorear el acceso y modificación de la información alojada en la nube.
    e) Alentar la adopción de estándares internaciones.
19. Las regulaciones y políticas deben estar basadas en evidencia y deben describir claramente tanto los objetivos como los principios subyacentes, prefiriendo una regulación ligera para permitir mercados competitivos[110].
20. La adopción exitosa del servicio de la nube dependerá en gran medida de los servidores públicos que la utilicen y su capacidad para aprovechar los beneficios de la nueva tecnología. Por esto es importante establecer alianzas con las empresas para implementar capacitaciones y programas de intercambio para asegurar que los servidores públicos tengan los conocimientos técnicos necesarios[111].

---

[109] Asia Cloud Computing Association. *From vision to procurement: principles for adopting cloud computing in the public sector*. 2019. Página 11.
[110] Asia Cloud Computing Association. *Cross-Border data Flows: A review of the regulatory enablers, blockers, and key sectoral opportunities in five asian economies: India, Indonesia, Japan, the Philiphines, and Vietnam.* 2018. Página 62.
[111]https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/government-canada-cloud-adoption-strategy.html

21. Establecer mercados digitales con servicios de la nube auditados y certificados por autoridades gubernamentales para disminuir los costos de adopción de esta tecnología en todos los niveles de gobierno.
22. Siguiendo el modelo canadiense, impulsar el uso de la nube pública y únicamente contratar una nube privada para los sistemas con información confidencial.
23. La transición debe ser definida como un proceso a largo plazo, como lo hizo el gobierno del Reino Unido.

Bibliografía

- Amazon Web Services. *Data Residency.* 2020.
- Asia Cloud Computing Association. *Asia´s Financial Services on the Cloud 2018. Regulatory landscape impacting the use of cloud by financial services institutions in Asia*. 2018.
- Asia Cloud Computing Association. *Cloud Readiness Index 2020*. 2020.
- Asia Cloud Computing Association. *From vision to procurement: principles for adopting cloud computing in the public sector*. 2019.
- Asia Cloud Computing Association. *Regulating for a digital economy. Understanding the importance of cross-border data flows in Asia*. 2018.
- Asia Cloud Computing Association. *Cross-Border data Flows: A review of the regulatory enablers, blockers, and key sectoral opportunities in five asian economies: India, Indonesia, Japan, the Philiphines, and Vietnam.* 2018.
- AWS. *Data Classification Secure Cloud Adoption*. 2020.
- Brill, Julie y Sauer, Rich. *Digital Transformation in the Cloud. What enterprise leaders and their legal and compliance advisors need to know*. Microsoft. 2018.
- Commonwealth of Australia (Digital Transformation Agency). *Secure Cloud Strategy*. 2021.
- Directiva (UE) 2016/680
- Flexera. *2021 State of the Cloud Report*. 2021.
- Korea Internet and Security Agency. *Korea 2018 Internet White Paper.* 2019.
- K. W. Miller and J. Voas, "Ethics and the Cloud," in IT Professional, vol. 12, no. 5, Sept.-Oct. 2010.
- Manual de legislación europea en materia de protección de datos. Edición de 2018

- Mell, Peter y Grance, Timothy. *The NIST Definition of Cloud Computing.* National Institute of Standards and Technology. U.S. Department of Commerce. E.U.A. 2011.
- Millard, Christopher. *Cloud computing law*. Oxford University Press. Segunda edición. Reino Unido. 2021.
- Naciones Unidas. *Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales*. 2017.
- New South Wales Information and Privacy Comission, *Guide – Transition to the cloud: Managing your agency's privacy risks*, May 2021.
- Reglamento (UE) 2018/1807
- Theodore, Christakis. *21 Thoughts and questions about UK-US CLOUD Act Agreement (and an Explanation of How it Works – with Charts)*, European Law Blog, 2019
- Tratado entre México, Estados Unidos y Canadá T-MEX
- Tratado Fundacional de la UE
- Schmidt, Nicholas. *Coming Down from the Cloud: A Concise Explanation of Cloud Computing and Introduction to Systems Architecture*. International Association of Privacy Professionals.
- Stolton, Samuel. *What's behind the EU's new Cloud Codeo f Conduct?* (2021)
- Wayne A. Jansen, NIST. *Cloud Hooks: Security and Privacy Issues in Cloud Computing.*
- Wayne Jansen, Timothy Grance, Wayne Jansen Timothy Grance. G*uidelines on Security and Privacy in Public Cloud Computing*. US Department of Commerce, NIST, USA, 2011.

Enlaces de Internet consultados

- http://www.ift.org.mx/sites/default/files/dgci_estudio-cloud_computing.pdf
- https://chmura.gov.pl/informacje/projekt-wspolna-infrastruktura-informatyczna-panstwa
- https://chmura.gov.pl/informacje/publiczna-chmura-obliczeniowa
- https://chmura.gov.pl/informacje/rzadowa-chmura-obliczeniowa

- https://cloud.cio.gov/strategy/
- https://cloud.gov/
- https://cloud.google.com/security/compliance/offerings#/regions=Asia_Pacific
- https://cloud.gov/docs/customer-stories/fec/
- https://datacenters.cio.gov/policy/
- https://datacenters.cio.gov/policy/m-16-19/
- https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-europe
- https://digital-strategy.ec.europa.eu/en/policies/digital-privacy
- https://digital-strategy.ec.europa.eu/en/policies/strategy-data
- https://digital-strathttps://digital-strategy.ec.europa.eu/en/policies/cloud-allianceegy.ec.europa.eu/en/policies/cloud-computing
- https://e-estonia.com/solutions/e-governance/government-cloud/
- https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_es
- https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/gdpr-fabric-success-story_es
- https://ec.europa.eu/info/sites/default/files/gdpr_factsheet-09_en.pdf
- https://edpb.europa.eu/system/files/2021-05/edpb_opinion_202116_eucloudcode_en.pdf
- https://edps.europa.eu/data-protection/our-work/publications/guidelines/guidelines-use-cloud-computing-services-european_en
- https://eportugal.gov.pt/en/noticias/governo-lanca-plano-de-acao-para-a-transicao-digital
- https://eucoc.cloud/en/about/about-eu-cloud-coc/
- https://eucoc.cloud/en/home.html
- https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32018R1807&from=ES

- https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L0680&from=ES
- https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32009L0136&from=en
- https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0066&from=EN
- https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62018CJ0311&from=es
- https://iapp.org/media/pdf/resource_center/new_south_wales_transition_to_cloud_managine_agency_privacy_risks.pdf
- https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5593031
- https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust
- https://management.cio.gov/
- https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf
- https://observatoire-fic.com/en/national-cloud-strategy-is-france-ready-to-enter-the-era-of-liquid-computing/
- https://pro.bloomberglaw.com/brief/the-far-reaching-implications-of-the-california-consumer-privacy-act-ccpa/
- https://rm.coe.int/1680078b37
- https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8
- https://swipo.eu/
- https://technology.blog.gov.uk/2020/03/31/introducing-the-gov-uk-cloud-guide/
- https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906716
- https://www.agid.gov.it/en/infrastructures/pa-cloud
- https://www.boe.es/doue/2010/083/Z00047-00199.pdf

- https://www.boe.es/doue/2016/119/L00001-00088.pdf
- https://www.boe.es/doue/2016/119/L00001-00088.pdf
- https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/direction-secure-use-commercial-cloud-services-spin.html
- https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/direction-electronic-data-residency.html
- https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/government-canada-cloud-adoption-strategy.html
- https://www.canada.ca/en/shared-services/news/2018/02/cloud_computing.html
- https://www.cdc.gov/phlp/publications/topic/hipaa.html
- https://www.cio.gov/policies-and-priorities/FITARA/
- https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet
- https://www.digitalaustria.gv.at/initiativen/verwaltung/verwaltungs-projekte/OECloud.html
- https://www.digitalrealty.com/blog/why-adopting-a-cloud-first-policy-is-the-right-move-for-the-australian-government
- https://www.dta.gov.au/our-projects/secure-cloud-strategy
- https://www.dta.gov.au/our-projects/secure-cloud-strategy
- https://www.fedramp.gov/federal-agencies/
- https://www.gcloud.belgium.be/fr/home
- https://www.gov.uk/government/case-studies/how-network-rail-implemented-its-hybrid-cloud-strategy
- https://www.gov.uk/government/publications/cloud-guide-for-the-public-sector/cloud-guide-for-the-public-sector
- https://www.kisa.or.kr/eng/main.jsp

- https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/pdf/special_event/en/special_event_01.pdf
- https://www.nasa.gov/open/nebula.html
- https://www.nist.gov/news-events/news/2009/05/nist-defining-expanding-world-cloud-computing
- https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html
- https://www.oecd.org/sti/ieconomy/15590267.pdf
- https://www.pcpd.org.hk//english/resources_centre/publications/files/IL_cloud_e.pdf
- https://www.privacy.org.nz/
- https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/index.html
- https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pressrelease/2021/6/18_07.html
- https://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20_Flows_2020.pdf