Recomendaciones para el tratamiento de datos personales mediante servicios de computación en la nube

Abril de 2021

RED IBEROAMERICANA DE PROTECCION DE DATOS

RED IBEROAMERICANA DE PROTECCION DE DATOS

Tabla de contenido

RED IBEROAMERICANA DE PROTECCION DE DATOS

/ 01. Introducción

/01. Introducción

La computación en la nube o "cloud computing" es una alternativa mediante la cual las organizaciones pueden obtener a través de Internet diversos recursos y servicios informáticos. El uso de dichos servicios implica que se realicen tratamientos de datos personales porque, según el caso, podría efectuarse, entre otras, almacenamiento, circulación (nacional o transfronteriza) o uso de esa información.

El Instituto Nacional de Estándares y Tecnología (NIST-National Institute of Standards and Technology. U.S. Department of Commerce) ha establecido que la computación en la nube es un *"modelo que permite, cuando sea solicitado, el acceso ubicuo y conveniente a la red, a un grupo compartido de recursos informáticos configurables (Ej. redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar y liberar rápidamente con un mínimo esfuerzo de administración o interacción por parte del proveedor de servicios. "*[1] Dentro de los servicios de cloud computing se destacan , entre otras, las siguientes categorías: (1) software como servicio (software as a service - SaaS); (2) plataforma como servicio (platform as a service –PaaS-), y (3) Infraestructura como servicio (infraestructure as a service –IaaS-). Estos los podemos obtener en un escenario de nube pública, privada, híbrida o comunitaria.

En el año 2012, durante la 34a Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (hoy Global Privacy Assembly -GPA-[2]), se recomendó lo siguiente en la resolución sobre computación en la nube[3]:

- La computación en la nube no debe generar una reducción de la privacidad ni de la protección de datos en relación con otras formas de Tratamiento de esa información.

- Los Responsables del Tratamiento deben efectuar análisis de riesgos y evaluaciones de impacto sobre protección de datos necesarias antes de contratar servicios o realizar proyectos de computación en la nube.

- Los proveedores de servicios en la nube deben garantizar transparencia adecuada, seguridad, responsabilidad y confianza en las soluciones de computación en la nube, en particular con respecto a la información sobre violaciones de seguridad de los datos y cláusulas contractuales que promuevan, en su caso, portabilidad de datos y control de datos por parte de los usuarios de los servicios de computación en la nube.

- Para generar más confianza y garantizar un adecuado tratamiento de datos a través de los servicios de computación en la nube se deben adoptar medidas desde el diseño de la arquitectura tecnológica de dichos servicios (privacidad desde el diseño).

- Todas las partes interesadas o involucradas (proveedores y clientes de servicios de computación en la nube y los reguladores) deberían cooperar para garantizar un alto nivel de privacidad, protección de datos y seguridad.

---

1 Cfr. NIST Cloud Computing Program (NCCP). En: https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp . The NIST Definition of Cloud Computing (2011). En: https://csrc.nist.gov/publications/detail/sp/800-145/final

2 https://globalprivacyassembly.org/

3 Cfr. AUTORIDADES DE PROTECCIÓN DE DATOS Y PRIVACIDAD. 2012. Resolution on cloud computing. 34a Conferencia internacional de Autoridades de Protección de Datos y Privacidad. Punta del Este, Uruguay. En: https://edps.europa.eu/sites/edp/files/publication/12-10-26_uruguay_resolutionon_cloud_computing_en.pdf

/01. Introducción

Esta guía pretende establecer los principales aspectos que deben tenerse presente cuando se utilizan servicios de computación en la nube desde la perspectiva de la regulación sobre tratamiento de datos personales. Como tal, presenta algunas orientaciones para que sean tenidas en cuenta por quienes contratan los servicios de computación en la nube y por quienes prestan este tipo de servicios.

RED IBEROAMERICANA DE PROTECCION DE DATOS

/02. Precisiones y limitaciones

/02. Precisiones y limitaciones

Esta guía es complementaria de las recomendaciones y documentos que han emitido algunas autoridades de protección de datos y otras organizaciones[4]. Se centrará en los aspectos jurídicos que involucra el tratamiento de datos a través de servicios de computación en la nube y no en elementos o conceptos tecnológicos.

Para la elaboración[5] de este documento se adoptaron los *Estándares de protección de datos personales para los Estados Iberoamericanos* de la RIPD[6] como el referente para establecer los principios, términos, definiciones, etc. No obstante, no se transcriben todos los aspectos de los mismos sino que se hace alusión a algunos de ellos. Por lo tanto, este documento debe leerse de manera conjunta e integral con los citados estándares.

Este texto no es un concepto legal, ni un artículo académico, ni constituye asesoría jurídica. Tampoco pretende ser un listado exhaustivo de recomendaciones específicas porque ello es un asunto interno que corresponde decidir a cada organización a la luz de los objetivos y la magnitud de cada proyecto que implique el uso de servicios de computación en la nube.

---

4 - Por ejemplo, ver las mencionadas en la sección de documentos consultados. En caso de contradicción manifiesta entre este documento y alguna recomendación o guía de la autoridad local, se sugiere seguir la recomendación de dicha autoridad en el entendido que corresponde a la entidad pública encargada de velar por la protección de datos en determinada jurisdicción. En cualquier caso, la aplicación de estas recomendaciones deberá hacerse en armonía con las recomendaciones de las autoridades de protección de datos y, sobre todo, la legislación local aplicable.

5 - La Red Iberoamericana de Protección de Datos (RIPD) publicó la versión previa del presente documento para comentarios de la opinión pública. Se recibieron y analizaron las observaciones y sugerencias de las siguientes personas y organizaciones cuya participación agradecemos: (1) Rafael Pérez Colón (HISKEN VENTURES SL); (2) La Asociación Latinoamericana de Internet (ALAI) y (3) la Cámara de Industria Digital y Servicios de la Asociación Nacional de Empresarios de Colombia (ANDI).

6 - Cfr. Red Iberoamericana de Protección de Datos -RIPD- (2017). Estándares de protección de datos personales para los Estados Iberoamericanos. Disponibles en: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

RED IBEROAMERICANA DE PROTECCION DE DATOS

/ 03. Neutralidad tecnológica en el tratamiento de datos personales

/ 03. Neutralidad tecnológica en el tratamiento de datos personales

La regulación sobre tratamiento de datos personales es neutral tecnológica y temáticamente. Ello significa que aplica a cualquier tratamiento de datos, con independencia de las técnicas, procesos o tecnologías –*actuales o futuras*- que se utilicen para dicho efecto. En este sentido, el artículo 4.1. de los Estándares dice que los mismos son *"aplicables al tratamiento de datos personales que obren en soportes físicos, automatizados total o parcialmente, o en ambos soportes,* ***con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización"*** (Destacamos)

Los Estándares definen Tratamiento como *"cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados realizadas sobre datos personales, relacionadas, de manera enunciativa más no limitativa, con la obtención, acceso, registro, organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, elaboración, transferencia, difusión, posesión, aprovechamiento y en general cualquier uso o disposición de datos personales".*[7] Este término es de enorme importancia porque cualquier actividad que se realice con datos personales, a través de medios manuales o automatizados, con o sin intervención humana, debe observar las reglas establecidas en las normas sobre protección de datos personales.

Dato Personal, por su parte, es *"cualquier información concerniente a una persona física identificada o identificable, expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo".*[8] En este orden de ideas, cualquier tratamiento de esa información debe ser respetuoso de los derechos de las personas y de las regulaciones pertinentes con independencia de las técnicas, tecnologías, o herramientas que se utilicen.

En suma, la regulación sobre Tratamiento de Datos Personales debe aplicarse al margen de los procedimientos, metodologías o mecanismos que se utilicen para recolectar, usar o tratar ese tipo de información. Por ende, debe ser cumplida por quien realice Tratamiento de datos mediante el uso de técnicas, herramientas como, entre otros, en internet de las cosas, las App, la inteligencia artificial, la robótica y la computación en la nube. El uso de esas innovaciones tecnológicas no desaparece la protección de datos ni debe convertirse en un instrumento para disminuir el nivel de protección de los derechos de las personas que es exigido por la regulación en comento.

---

7 - Cfr. Literal i) del artículo 2.1 de los Estándares de protección de datos personales para los Estados Iberoamericanos (2017).

8 - Cfr. Literal c) del artículo 2.1 de los Estándares de protección de datos personales para los Estados Iberoamericanos (2017).

RED IBEROAMERICANA DE PROTECCION DE DATOS

/ 04. Principales actores en el tratamiento de datos personales a través de servicios de computación en la nube (CEN)

/ 04. Principales actores en el tratamiento de datos personales a través de servicios de computación en la nube (CEN)

A continuación, se presentan los principales actores involucrados no sólo en el tratamiento de datos personales a través de servicios de computación en la nube sino en la supervisición o control para que dicha actividad se realice respetando las regulaciones pertinentes y garantizando los derechos de las personas:

- **Proveedor de servicios de computación en la nube (PSCEN)**

Desde la perspectiva de la regulación sobre tratamiento de datos, las empresas Proveedoras de servicios de computación en la nube (PSCEN) usualmente obran como Encargados del Tratamiento definidos por los Estándares como *"prestador de servicios, que con el carácter de persona física o jurídica o autoridad pública, ajena a la organización del responsable, trata datos personales a nombre y por cuenta de éste"*[9]

De conformidad con el artículo 34 de los Estándares la prestación de los servicios entre el responsable y el encargado -*como la prestación de servicios de computación en la nube*- debe formalizarse mediante un contrato o instrumento jurídico que contenga, por lo menos, lo que se indica en los artículos 34.2 y 34.3. a que nos referiremos posteriormente.

Adicionalmente, el artículo 35 establece unos requisitos que debe cumplir el encargado (por ejemplo, un PSCEN) cuando subcontrata servicios que implican tratamiento de datos personales.

- **Empresa o entidad pública que contrata los servicios de computación en la nube**

Estas empresas y organizaciones pueden ser, según el caso, Responsables o Encargados del Tratamiento. Como tales, deben cumplir las obligaciones jurídicas establecidas en la regulación que les sea aplicables. El Responsable, según los Estándares, es la *"persona física o jurídica de carácter privado, autoridad pública, servicios u organismo que, solo o en conjunto con otros, determina los fines, medios, alcance y demás*

Gráfica 1. *Principales actores en el tratamiento de datos personales a través de servicios de computación en la nube*

9 - Cfr. Literal e) del artículo 2.1 de los Estándares de protección de datos personales para los Estados Iberoamericanos (2017) .

/ 04. Principales actores en el tratamiento de datos personales a través de servicios de computación en la nube (CEN)

cuestiones relacionadas con un tratamiento de datos personales" [10]

El Responsable y el Encargado deben adoptar medidas para cumplir la regulación de protección de datos cuando realice el tratamiento a través de los servicios de CEN. Al mismo tiempo, deben estar en capacidad de responder por sus acciones u omisiones ante el Titular del dato y la Autoridad de protección de datos.[11]

- **Titular del dato personal**

El Titular es la *"persona física a quien le conciernen los datos personales"* [12] cuya información debe ser tratada debidamente. Todos los derechos del Titular deben garantizarse cuando el tratamiento se efectúe mediante servicios de computación en la nube. En el caso de los Estándares Iberoamericanos los derechos se encuentran mencionados en los artículos 24 a 32.

- **Autoridad de protección de datos (APD)**

La Autoridad de protección de datos (APD) o la Autoridad de Control[13] debe vigilar que los Responsables y Encargados que utilizan servicios de computación en la nube realicen dicha actividad observando lo que dispone la regulación sobre dicho tema.

---

10 - Cfr. Literal g) del artículo 2.1 de los Estándares de protección de datos personales para los Estados Iberoamericanos (2017)

11 - Señala lo siguiente el numeral 34.4 de los Estandares: "Cuando el encargado incumpla las instrucciones del responsable y decida por si mismos sobre el alcance, contenido, medios y demás cuestiones del tratamiento de los datos personales asumirá la calidad de responsable (...)"

12 - Cfr. Literal h) del artículo 2.1 de los Estándares de protección de datos personales para los Estados Iberoamericanos (2017)

13 - En el capítulo VII de los Estándares se establecen los principales aspectos sobre las autoridades de control y supervisión en materia de protección de datos

RED IBEROAMERICANA DE PROTECCION DE DATOS

/ 05.Recomendaciones

/ 05. Recomendaciones

En virtud de lo anterior, la Red Iberoamericana de Protección de Datos recomienda lo siguiente:

- **Respetar las normas locales sobre Tratamiento de Datos Personales (TDP)**

Los PSCEN deben cumplir las normas nacionales de tratamiento de datos en aquellos países que presten servicios. Los Responsables o Encargados que contraten lo servicios de CEN (contratantes de servicios de CEN) deben tener presente que están obligados a cumplir las normas nacionales sobre tratamiento de datos personales. Por ende, los contratos de CEN deben ser consistentes con lo que ordenan dichas regulaciones y no deben desconocer los mandatos legales.

Usualmente, los PSCEN utilizan proformas estandarizadas de los términos y condiciones de la prestación de sus servicios. Dichos textos son redactados teniendo en cuenta las características de los servicios y los intereses de los PSCEN y la regulación de su país de origen que con frecuencia es un país distinto al de los contratantes de servicios de CEN. Por eso, para que el tratamiento de datos mediante servicios de CEN no sea objetado o cuestionado jurídicamente es muy relevante que antes de suscribir los contratos, dichos contratantes realicen un estudio de riesgos legales que puede implicar la suscripción de dichos contratos.

Lo anterior le permitirá a los contratantes de servicios de CEN definir una estrategia para, entre otros: (i) mitigar dichos riesgos; (ii) ganar y mantener la confianza de los Titulares de los datos; (iii) no afectar la buena reputación de su organización y (iv) evitar reclamaciones por parte de los interesados que puedan derivar en investigaciones y posibles sanciones por parte de las autoridades de protección de datos o de otras entidades.

Los PSCEN, por su parte, deberían establecer términos y condiciones de sus contratos teniendo en cuenta las regulaciones locales sobre tratamiento de datos de manera que sus clientes (contratantes de servicios de CEN) no asuman riesgos legales por eventuales infracciones a las leyes que deben cumplir.

- **Formalizar un acuerdo con el PSCEN que contenga aspectos mínimos sobre tratamiento de datos personales.**

Como se mencionó, el PSCEN obra como un Encargado del tratamiento que presta servicios de computación en la nube a una empresa o entidad pública. Los Estándares señalan que el encargado debe realizar el *"tratamiento de los datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido del mismo, así como limitará sus actuaciones a los términos fijados por el responsable"* [14].

Adicionalmente, los Estándares establecen la necesidad de suscribir un contrato mediante el cual se acuerden los términos concretos de la prestación de los servicios –en este caso de computación en la nube- entre el PSCEN y quien lo contrata. Según el artículo 34.2. ese contrato o instrumento jurídico *"establecerá, al menos, el objeto, alcance, contenido, duración, naturaleza y finalidad del tratamiento; el tipo de datos personales; las categorías de titulares, así como las obligaciones y responsabilidades del responsable y encargado"*.

Particularmente y sin perjuicio de lo que establezcan las regulaciones locales, el artículo 34.3. ordena que ese acuerdo debe establecer, entre otras, cláusulas generales que establezcan las siguientes obligaciones al encargado (en este caso el PSCEN):

14 - Cfr. Artículo 33.1 de los Estándares de protección de datos personales para los Estados Iberoamericanos (2017)

/ 05. Recomendaciones

a. *"Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable.*
b. *Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable.*
c. *Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables.*
d. *Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones.*
e. *Guardar confidencialidad respecto de los datos personales tratados.*
f. *Suprimir, devolver o comunicar a un nuevo encargado designado por el responsable los datos personales objeto de tratamiento, una vez cumplida la relación jurídica con el responsable o por instrucciones de éste, excepto que una disposición legal exija la conservación de los datos personales, o bien, que el responsable autorice la comunicación de éstos a otro encargado.*
g. *Abstenerse de transferir los datos personales, salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad de control.*
h. *Permitir al responsable o autoridad de control inspecciones y verificaciones en sitio.*
i. *Generar, actualizar y conservar la documentación que sea necesaria y que le permita acreditar sus obligaciones.*
j. *Colaborar con el responsable en todo lo relativo al cumplimiento de la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia."*

Todo lo anterior y otros aspectos se deben incorporar en los Acuerdos de Nivel de Servicio (Service Level Agreement – SLA).

Adicionalmente, los Estándares permiten que el PSCEN *"pueda subcontratar servicios que impliquen el tratamiento de datos personales, siempre y cuando exista una autorización previa por escrito, específica o general del responsable, o bien, se estipule expresamente en el contrato o instrumento jurídico suscrito entre este último y el encargado"* [15]. Para el efecto, el PSCEN deberá suscribir un acuerdo con el subcontratado sobre el alcance de la prestación de sus servicios.
El prestador del servicio debe ser diligente y transparente en orden a facilitar información sobre los servicios subcontratados

- **Respetar las reglas sobre transferencias internacionales de datos**

Si los "data center" o los equipos de almacenamiento de los PSCEN están ubicados fuera del país en donde se encuentra el contratante de los servicios de CEN, los datos personales serán remitidos o exportados desde un país a empresas y organizaciones PSCEN ubicadas en un territorio diferente al del país de envío. Se trata de un proceso de exportación de datos personales.
En este caso, la empresa contratante de los servicios de CEN será el exportador y el PSCEN obrará como el destinatario de dicha exportación de datos. Los Estándares definen al exportador como la *"persona física o jurídica de carácter privado, autoridad pública, servicios, organismo o prestador de servicios situado en territorio de un Estado que efectúe transferencias internacionales de datos personales, conforme a lo dispuesto en los presentes Estándares"* [16]. Así las cosas, el contratante de los servicios de CEN debe observar las reglas locales de la transferencia internacional de datos.

15 - Cfr. Artículo 35.1 de los Estándares de protección de datos personales para los Estados Iberoamericanos (2017)

16 - Cfr. Literal f) del artículo 2.1 de los Estándares de protección de datos personales para los Estados Iberoamericanos (2017)

/ 05. Recomendaciones

Es importante que el contratante de los servicios de CEN sea plenamente consciente y en su caso, pueda aceptar o limitar, los países en los que van a estar alojados los servidores, además de estar informado de las garantías adecuadas que se adopten.

Las regulaciones sobre transferencia internacional de datos o "flujo transfronterizo de datos" procuran garantizar que el nivel de protección de los datos personales de los ciudadanos de un país no disminuya o desaparezca cuando estos deben ser exportados o transferidos a otro u otros países. Esta regla se conoce como el principio de continuidad de la protección de datos, el cual se fundamenta en que la transferencia internacional de datos no debe afectar la protección de los interesados por lo que respecta al tratamiento de sus datos personales.

La exportación de información personal no puede convertirse en un escenario reductor del nivel de protección que se le confiere al titular del dato en el país desde donde se exportan datos personales. Dichas actividades no deben facilitar, permitir ni tolerar la vulneración de los derechos de las personas ni la disminución de las garantías con que cuentan en el país exportador.

En ese sentido, se deben cumplir las reglas de transferencias internacionales que rigen en el país del contratante de los servicios de CEN. En el caso de los Estándares, en el artículo 36 se prevén las alternativas permitidas para exportar los datos.

- **Efectuar estudios de impacto a la protección de datos personales**

Los Estándares disponen que *"cuando el responsable pretenda llevar a cabo un tipo de tratamiento de datos personales que, por su naturaleza, alcance, contexto o finalidades, sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares, realizará, de manera previa, a la implementación del mismo una evaluación del impacto a la protección de los datos personales."*[17]. Por ende, según el caso y siempre y cuando se cumplan los anteriores requerimientos, se debe efectuar una evaluación de impacto a la protección de datos (Data Protection Impact Assessment - DPIA por sus siglas en inglés), con el fin de poner en funcionamiento un sistema efectivo de manejo de riesgos y controles internos, para garantizar que los datos se tratarán debidamente y conforme a la a la regulación existente.

Dicha evaluación debería incluir, como mínimo, lo siguiente:

- Una descripción detallada de las operaciones de tratamiento de datos personales que involucra la CEN;
- Una evaluación de los riesgos específicos para los derechos y libertades de los titulares de los datos personales, así como los riesgos asociados a los pedidos o requerimientos de autoridades públicas de el/los países donde se alojaría la información en ocasión de la aplicación de normas de derecho público.
- Una evaluación de los riesgos de afectación de derechos de los titulares derivados de la regulación aplicable en el país donde se estén almacenando los datos personales
- Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad, diseño de software, tecnologías y mecanismos que garanticen la protección de datos personales, teniendo en cuenta los derechos e intereses legítimos de los titulares de los datos y de otras personas eventualmente afectadas.

17 - Red Iberoamericana de Protección de Datos (2017), Artículo 41.1

/ 05. Recomendaciones

Los resultados de este estudio, junto con las medidas para mitigar los riesgos, hacen parte de la aplicación de la medida proactiva de privacidad desde el diseño y por defecto.[18]

- **Incorporar la privacidad, la ética y la seguridad desde el diseño y por defecto**

La privacidad desde el diseño y por defecto *(Privacy by Design and by Default)* es considerada una medida proactiva para cumplir con el Principio de *Accountability,*[19] como se observa en los numerales 1 y 2 del artículo 38 de los Estándares de la RIPD. Al incrustar la privacidad desde el diseño, se está buscando garantizar el correcto tratamiento de los datos a través de los servicios de CEN, incluso antes de la materialización de los riesgos.

La Privacidad por Diseño *"promueve la visión de que el futuro de la privacidad no puede ser garantizada sólo por cumplir con los marcos regulatorios; más bien, idealmente el aseguramiento de la privacidad debe convertirse en el modo de operación predeterminado de una organización".*[20] Por eso, desde antes que se recolecte información y durante todo el ciclo de vida de la misma, se deberían adoptar medidas preventivas de diversa naturaleza (tecnológica, organizacional, humana, procedimental, entre otras) con el objeto de garantizar el debido tratamiento de los datos personales.

La ética desde el diseño y por defecto debe irradiar el esquema, desarrollo y uso de los productos o procesos de computación en la nube, debiendo ser parte del ADN de cualquier aspecto relacionado con la prestación de dichos servicios.

Lo anterior también debe predicarse en la seguridad del tratamiento de datos mediante la CEN. Sin seguridad no habrá debido tratamiento de los datos personales. Es fundamental adoptar medidas tecnológicas, humanas, administrativas, físicas, contractuales y de cualquier otra índole para garantizar la confidencialidad, integridad y disponibilidad de los datos personales y que, entre otras, cumplan los siguientes objetivos:

- Evitar accesos indebidos o no autorizados a la información
- Evitar la manipulación accidental o no autorizada de la información
- Evitar la destrucción accidental o no autorizada de la información
- Evitar usos indebidos o no autorización de la información
- Evitar circular o suministrar la información a personas no autorizadas

Las medidas de seguridad deben ser apropiadas considerando varios factores como entre otros, los siguientes: (i) los niveles de riesgos del tratamiento; (ii) la naturaleza o sensibilidad de los datos; (iii) la magnitud del daño que se puede causar a los titulares y al responsable; (iv) la cantidad de información; (v) el tamaño de la organización; (vi) los recursos disponibles y (vii) el monitoreo y seguimiento a la confiabilidad los servicios de CEN; (vii) el origen de los datos personales, las operaciones de tratamiento que se ejecutarán, y las categorías de datos que serán objeto del tratamiento. Todas estas, deben ser objeto de revisión, evaluación y mejoras permanentes.

Adicionalmente debe garantizarse la obligación por

---

18 - "Privacidad por diseño y privacida por defecto" es considerada en los Estándares como una medida proactiva en el tratamiento de datos personales (Artículo 38)

19 - Cavoukian (2011).

20 - Cfr. Cavoukia, Ann. Privacidad por Diseño: Los 7 principios fundamentales. Disponible en: https://www.mediascope.es/wp-content/uploads/2016/10/privacidad-por-disen%CC%83o-1.pdf

/ 05. Recomendaciones

parte del prestador de servicios CEN de comunicar al responsable que lo contrató las brechas de seguridad que puedan producirse y las medidas adoptadas para resolverlas
Con el fin de poder disponer de información actualizada sobre las medidas de seguridad el contratante de servicios de cloud podrá requerir la realización de auditorías de seguridad por parte de un tercero independiente.

- **Materializar el principio de responsabilidad proactiva**

Los diseñadores y creadores de productos de CEN y las organizaciones contratantes de los servicios de CEN deben adoptar medidas útiles, apropiadas y efectivas para cumplir sus obligaciones legales. Adicionalmente, tendrán que evidenciar y demostrar el correcto cumplimiento de sus deberes. Dichas herramientas, deben ser objeto de revisión y evaluación permanente, a fin de determinar su nivel de eficacia en cuanto al cumplimiento y grado de protección de los datos personales.

Para la implementación adecuada del citado principio, los Estándares de la RIPD recomiendan los siguientes mecanismos:

a. *"Destinar recursos para la instrumentación de programas y políticas de protección de datos personales.*
b. *Implementar sistemas de administración de riesgos asociados al tratamiento de datos personales.*
c. *Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable.*
d. *Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones en materia de protección de datos personales.*
e. *Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.*
f. *Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.*
g. *Establecer procedimientos para recibir y responder dudas y quejas de los titulares."*[21]

El reto de las organizaciones frente al Principio de Responsabilidad Proactiva va mucho más allá de la mera expedición de documentos o redacción de políticas. Se trata de una actividad de supervisión continua que exige demostrar un cumplimiento real y efectivo en la práctica de sus funciones. No basta hacer meras declaraciones simbólicas de buenas intenciones, sino que es necesario evidenciar resultados concretos respecto del debido tratamiento de los datos personales.

En este aspecto es esencial realizar entrenamientos periódicos y especializados al equipo humano de la organización para proveerles la experticia, guía y herramientas que requieren para el correcto desarrollo de su actividad.

La identificación y clasificación de riesgos, así como la adopción de medidas para mitigarlos, son elementos cardinales del principio de responsabilidad. Es fundamental que las organizaciones desarrollen y pongan en marcha, entre otros, un *"sistema de administración de riesgos asociados al tratamiento de datos personales"*[22] que les permita *"identificar, medir, controlar y monitorear todos aquellos hechos o situaciones que puedan incidir en la debida*

21 - Red Iberoamericana de Protección de Datos (2017), Artículo 20.3

22 - Superintendencia de Industria y Comercio (2015) *"Guía para implementación del principio de responsabilidad demostrada (accountability)"*. Págs 16-18

/ 05. Recomendaciones

administración del riesgo a que están expuestos en desarrollo del cumplimiento de las normas de protección de datos personales".[23]

- **Adoptar medidas para garantizar los principios sobre TDP mediante los servicios de CEN**

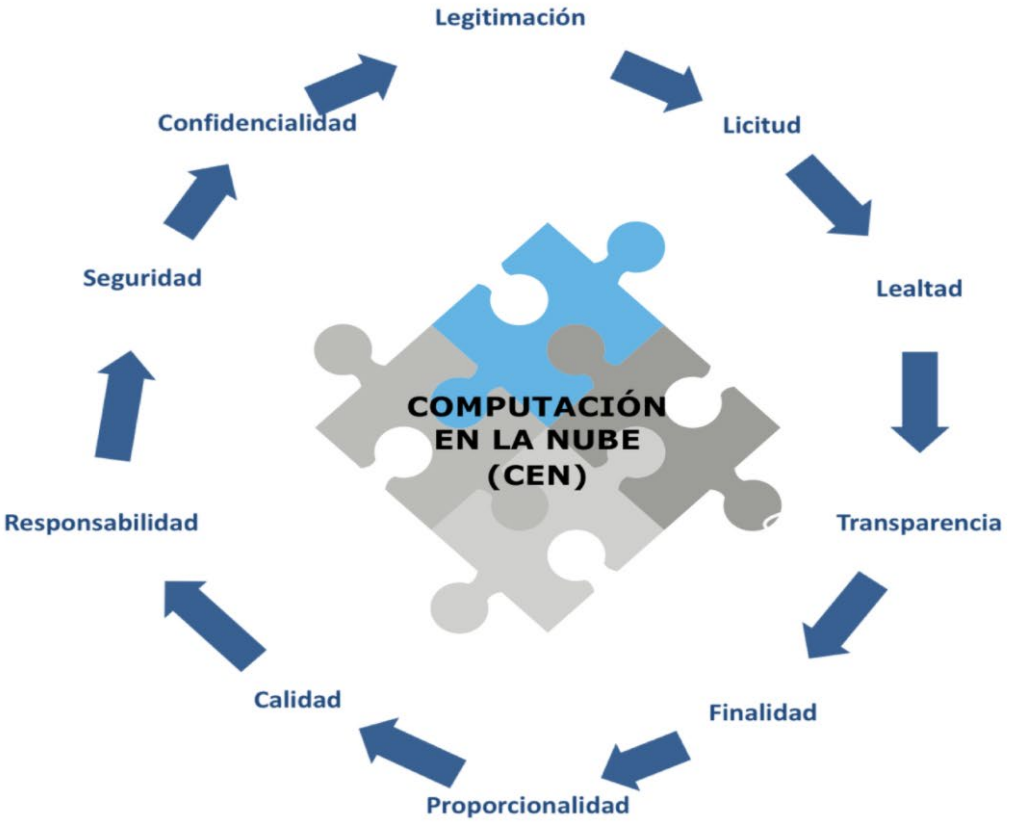
Es necesario que los Responsables o Encargados que contraten los servicios de CEN prevean estrategias pertinentes y eficientes para garantizar el cumplimiento de los principios sobre tratamiento de datos contenidos en el Capítulo II de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos emitidos por la RIPD[24].

El alcance de cada principio está determinado en el texto de los "Estándares de Protección de Datos Personales para los Estados Iberoamericanos"[25] de la RIPD, razón por la cual nos remitimos al mismo para no transcribirlos en este espacio.

- **Garantizar los derechos de los titulares de los datos e implementar mecanismos efectivos para su ejercicio**

Los Responsables o Encargados que contraten los servicios de CEN deben garantizar los derechos de los titulares de los datos.

El alcance de cada derecho está delineado en el texto de los "Estándares de Protección de Datos



Gráfica 2. *Princios del tratamitneo de datos personales*

23 - Ibid. P 16

24 - Red Iberoamericana de Protección de Datos (2017)

25 - Cfr. Red Iberoamericana de Protección de Datos (2017). *Estándares de protección de datos personales para los Estados Iberoamericanos.* El texto oficial de los estándares puede consultarse en:

/ 05. Recomendaciones

Personales para los Estados Iberoamericanos"[26] de la RIPD razón por la cual se hace una remisión expresa a dicho documento.

- **Incrementar confianza y la transparencia con los titulares de los datos personales**

Desde hace algunas décadas se ha sostenido que la confianza es factor crucial para el crecimiento y consolidación de cualquier actividad que se realice a través del uso de las tecnologías[27], lo cual ha sido reiterado al establecer que "*las actividades continuas de creación de confianza deben ser una de las prioridades estratégicas más importantes para cada organización*"[28]

La confianza se entiende como la credibilidad que te ofrece un tercero por las garantías que te ofrece en los servicios que presta. Cuando existe confianza, la persona cree que la empresa es fiable, cumple su palabra, es sincera, íntegra y cumple con las acciones prometidas[29].

Gráfica 3. *Derechos del Titular del dato*

26 - Red Iberoamericana de Protección de Datos (2017).

27 - Cfr. Reichel & Shefter. Harvard Business Review. Jul-Ago, 2000

28 - Cfr. Edelman Trust Barometrer de 2019,

29 - Cfr. Barrera Duque, Ernesto (2018) *Diseño organizacional centrado en el cliente. Teoría y práctica en empresas sociales.* Universidad de la Sabana y Ecoe ediciones.

RED IBEROAMERICANA DE PROTECCION DE DATOS

/ 06. Glosario

/ 06. Glosario

- Computación en la nube: *"modelo para habilitar el acceso a un conjunto de servicios computacionales (e.g. Redes, servidores, almacenamiento, aplicaciones y servicios) de manera conveniente y por demanda, que pueden ser rápidamente aprovisionados y liberados con un esfuerzo administrativo y una interacción con el proveedor del servicio".*30

- Datos Personales: cualquier información concerniente a una persona física identificada o identificable, expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente, siempre y cuando esto no requiera plazos o actividades desproporcionadas.

- Encargado: prestador de servicios, que con el carácter de persona física o jurídica o autoridad pública, ajena a la organización del responsable, trata datos personales a nombre y por cuenta de éste.

- Exportador: persona física o jurídica de carácter privado, autoridad pública, servicios, organismo o prestador de servicios situado en territorio de un Estado que efectúe transferencias internacionales de datos personales, conforme a lo dispuesto en los presentes Estándares.

- Responsable: persona física o jurídica de carácter privado, autoridad pública, servicios u organismo que, solo o en conjunto con otros, determina los fines, medios, alcance y demás cuestiones relacionadas con un tratamiento de datos personales.

- Titular: persona física a quien le conciernen los datos personales.

- Tratamiento: cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados realizadas sobre datos personales, relacionadas, de manera enunciativa más no limitativa, con la obtención, acceso, registro, organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, elaboración, transferencia, difusión, posesión, aprovechamiento y en general cualquier uso o disposición de datos personales.

30 - Cfr. NIST Cloud Computing Program (NCCP). En: https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp . The NIST Definition of Cloud Computing (2011). En: https://csrc.nist.gov/publications/detail/sp/800-145/final

RED IBEROAMERICANA DE PROTECCION DE DATOS

/ 07. Siglas

/07. Siglas

APD
Autoridad de Protección de Datos o Autoridad de Control

Estándares
Estándares de Protección de Datos Personales para los Estados Iberoamericanos aprobados por la RIPD en 2017

CEN
Computación en la nube

Reglamento General de Protección de Datos o RGPD
REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE

RIPD o Red
Red Iberoamericana de Protección de Datos.

PSCEN
Proveedor de servicios de computación en la nube.

TDP
Tratamiento de datos personales.

RED IBEROAMERICANA DE PROTECCION DE DATOS

/ 08. Documentos consultados

/08. Documentos consultados

A continuación se enunciarán en orden alfabético los principales documentos sobre tratamiento de datos y computación en la nube emitidos por autoridades de países miembros y la RIPD y otros elaborados por otras autoridades:

Textos emitidos por autoridades de países miembros de la RIPD

ARGENTINA

- DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES (HOY AGENCIA DE ACCESO A LA INORMACION PÚBLICA). Disposición DNPDP 60/2016, Anexo II (Contrato modelo de transferencia internacional de datos personales con motivo de prestación de servicios).

COLOMBIA

- SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO -SIC- (2015). Cartilla de protección de los datos personales en los servicios de computación en la nube.

- SUPERINTENDENCIA FINANCIERA (2019). Superintendencia Financiera de Colombia. Circular 5 del 11 de marzo de 2019. Instrucciones relacionadas con el uso de servicios de computación en la nube.

ESPAÑA

- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS -AEPD- (2019) Orientaciones para prestadores de servicios de cloud computing.

- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS -AEPD- (2019) Orientaciones para clientes que contraten servicios de cloud computing.

MÉXICO

- INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES -INAI- (2019). Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales.

PERÚ

- AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS PERSONALES (2018). Lineamientos para el uso de servicio en la nube para entidades de la administración pública del Estado Peruano.

URUGUAY

- UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES (2014). Dictamen 08/14 sobre el tratamiento de datos en la nube.

- UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES (2015). Análisis de la Norma ISO/IEC 27.018 desde la perspectiva de la Protección de Datos Personales.

- UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES (2019). Jornadas Tecnológicas de AGESIC. “La Nube en el Estado, el Estado en la Nube”.

Textos emitidos por otras autoridades u organizaciones

ALEMANIA

- THE ASSOCIATION OF GERMAN DATA PROTECTION AUTHORITIES -“DATENSCHUTZKONFERENZ” OR “DSK” (2011). Design and use of cloud computing in conformity with data protection law.

- THE ASSOCIATION OF GERMAN DATA PROTECTION AUTHORITIES -“DATENSCHUTZKONFERENZ” OR

/08. Documentos consultados

"DSK" (2014) Orientierungshilfe – Cloud Computing.

- THE INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS (BERLIN GROUP) (2012). Working Paper on Cloud Computing - Privacy and data protection issues - "Sopot Memorandum".

CANADÁ

- OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (2011). Cloud computing and privacy.
- OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (2011). Frequently asked questions about cloud computing.
- OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (2012). Cloud computing for small and medium-sized enterprises.
- THE OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER - BRITISH COLUMBIA, CANADA (2012). Cloud computing guidelines for public bodies.

ESTADOS UNIDOS DE ÁMERICA

- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE (2011). The NIST Definition of Cloud Computing.
- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE (2013) . NIST Cloud Computing Security Reference Architecture.
- THE FEDERAL TRADE COMMISSION -FTC- (2020). Six steps toward more secure cloud computing.

EUROPA

- COMITÉ EUROPEO DE PROTECCIÓN DE DATOS (2012). Dictamen 05/2012 sobre computación en nube.
- ENISA EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY (2011). Security and Resilience in Governmental Clouds.
- ENISA EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY. Cloud Security.
- SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (2012). Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe.
- SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (2018). Guidelines on the use of cloud computing services by the European institutions and bodies.
- COMITÉ EUROPEO DE PROTECCIÓN DE DATOS (2020). Draft Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

FRANCIA

- COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS -CNIL- (2012). Recommendations for companies planning to use Cloud computing services.

GRAN BRETAÑA E IRLANDA DEL NORTE

- THE INFORMATION COMMISSIONER'S OFFICE (ICO's) - GRAN BRETAÑA E IRLANDA DEL NORTE (2012). Guidance on the use of cloud computing.

/08. Documentos consultados

HONK KONG

- THE OFFICE OF THE PRIVACY COMMISSIONER FOR PERSONAL DATA (2012). Cloud Computing.

- THE OFFICE OF THE PRIVACY COMMISSIONER FOR PERSONAL DATA (2015). Cloud Computing.

IRLANDA

- DATA PROTECTION COMMISSION (DPC). (2019) Guidance for Organisations Engaging Cloud Service Providers.

- DATA PROTECTION COMMISSION (DPC) (2019) . Securing Cloud-based Environments.

ITALIA

- GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (2012) Cloud Computing - Protect your Data Without Falling from a Cloud.

NORUEGA

- DATATILSYNET -THE NORWEGIAN DATA PROTECTION- (2018). Cloud services.

NUEVA ZELANDA

- THE OFFICE OF THE PRIVACY COMMISSIONER (2013). Cloud Computing - A guide to making the right choices".

SUIZA

- THE FEDERAL DATA PROTECTION AND INFORMATION COMMISSIONER Guide to cloud computing.

THE GLOBAL PRIVACY ASSEMBLY (GPA)

- THE GLOBAL PRIVACY ASSEMBLY (GPA), FORMERLY KNOWN AS THE INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS (2012) Resolution on cloud computing.


RED
IBEROAMERICANA DE
PROTECCION
DE DATOS