# MODELO DE ANÁLISIS RELATIVO A LA PROTECCIÓN DE DATOS PERSONALES PARA PROYECTOS DE CÓMPUTO EN LA NUBE

Juan Cruz González Allonca, Darío Piccirilli & Ma. Florencia Pollo-Cattaneo
Grupo de Estudio en Metodologías de Ingeniería de Software (GEMIS), Programa de Maestría en Ingeniería en Sistemas de Información. Universidad Tecnológica Nacional. Facultad Regional Buenos Aires
Medrano 951 (C1179AAQ) Ciudad Autónoma de Argentina. Buenos Aires Tel +54 11 4867-7511
{ juanallonca, dariopiccirilli, flo.pollo}@gmail.com

## Resumen

La información es el activo más importante de las organizaciones. Es por ello que asegurar la protección de los datos personales y la privacidad de la información durante su ciclo de vida es crucial a la hora de utilizar servicios de cómputo en la nube (Cloud Computing).

El esquema de cómputo en la nube ofrece beneficios como: flexibilidad, accesibilidad, autoservicio bajo demanda, escalabilidad, gestión de grandes volúmenes de datos. Sin embargo, estas ventajas, muchas veces no contemplan cuestiones críticas como la seguridad de la información y la privacidad de los datos almacenados.

Teniendo en cuenta estas falencias, es deseable definir un proceso de análisis que permita describir y evaluar la reglamentación vigente en el país referida a la protección de datos personales en proyectos de cómputo en la nube en el exterior del país. El proceso de análisis propuesto permitirá identificar y valorar el grado de cumplimiento con la normativa local, lo que facilitará la toma de decisiones informadas, basadas no solo en criterios técnicos o económicos, sino también regulatorios.

**Palabras clave:**

Cómputo en la nube, Privacidad, Cloud Computing, Protección de Datos Personales.

## Contexto

La presente investigación se desarrolla dentro de una línea de trabajo incipiente del Grupo de Estudio de Metodologías para Ingeniería en Software y Sistemas de Información (GEMIS), conformado por un conjunto de docentes y alumnos de la Facultad Buenos Aires de la Universidad Tecnológica Nacional (UTN-FRBA). El grupo GEMIS, se halla abocado a la búsqueda de la sistematización de cuerpos de conocimientos y promoción sobre el campo de la Ingeniería en Sistemas de Información y la Ingeniería en Software, sus aplicaciones y abordajes metodológicos en todo tipo de escenarios (convencionales y no convencionales).

En el marco de la UTN-FRBA, el equipo de investigadores ha trabajado desde las carreras de grado y posgrado de Ingeniería en Sistemas de Información, integrando entre sus miembros a docentes de grado y de posgrado, articulando los resultados de investigaciones con el desarrollo de Trabajos Finales de Carrera, Trabajos Finales de Especialidad y Tesis de Maestría.

## Introducción

En los últimos años gran cantidad de empresas se ven atraídas por las ventajas técnicas y los bajos costos de mantenimiento que ofrece el esquema de cómputo en la nube (CN). Flexibilidad, accesibilidad, autoservicio bajo demanda, escalabilidad, gestión de grandes volúmenes de datos, son algunos de los beneficios que ofrece este esquema de CN. Sin embargo, estas ventajas, muchas veces no contemplan cuestiones críticas como la seguridad de la información y la privacidad de los datos almacenados [1].

Actualmente, la información es el activo más importante de las organizaciones. Es por ello que asegurar la privacidad de la información

durante su ciclo de vida es crucial a la hora de utilizar este tipo de servicios.

El desconocimiento o la no aplicación de la normativa vigente pueden transformase tanto en pérdida de confianza o daño en la imagen de una empresa o perjuicio económico y hasta en responsabilidades jurídicas [2-4]. Las preocupaciones por estos inconvenientes por lo general son lo suficientemente importantes para algunas empresas y organizaciones, tanto que les llevan a evitar implementar sus sistemas en arquitecturas de CN.

Los principales obstáculos para la adopción de servicios CN [5] se concentran en tres cuestiones vinculadas a la localización de los datos: privacidad, confidencialidad y las relacionadas con la propiedad y los derechos de los datos en la nube. Por lo tanto, al momento de iniciar un proyecto de estas características, es determinante adecuarse a la normativa local y a su vez, analizar las cláusulas relativas a la seguridad de la información, especialmente a la protección de los datos personales. Si bien existe legislación aplicable que determina la extensión de responsabilidad, tanto del cliente, como del proveedor de servicios de CN, pocas organizaciones realizan un análisis previo en este sentido, donde se le permita al usuario conocer su nivel de riesgo y de cumplimiento normativo [6].

Por consiguiente, a partir del presente estudio se definirá un proceso de análisis que permita a las empresas u organismos locales, describir y evaluar la reglamentación vigente referida a la protección de datos personales en proyectos de cómputo en la nube con proveedores alojados en el exterior del país. Este proceso de análisis permitirá verificar el grado de cumplimiento con la normativa vigente, sumando el aspecto regulatorio a los análisis de viabilidad de un proyecto de CN.

A su vez, se promueve la implementación del estándar ISO/IEC 27018 [7], que puede contribuir a proporcionar confianza a los clientes de estos servicios respecto de la capacidad de cumplimiento normativo de los proveedores.

## Líneas de Investigación, Desarrollo e Innovación

Para llevar a cabo el presente trabajo, se debe identificar el modelo de CN (nuevo paradigma en la forma de brindar servicios de cómputo por demanda [8]). Este modelo presenta un cambio importante en el paradigma computacional actual, la transformación de la infraestructura y las aplicaciones, desde un mundo claramente dominado y administrado por las organizaciones, a otro donde un tercero confiable y conocido le brinda servicios de infraestructura y uso de aplicaciones.

La Cloud Security Alliance (CSA) [9] describe cinco características esenciales en las que se evidencian similitudes y diferencias con las estrategias de computación tradicionales [10]:

1. Autoservicio por demanda.
2. Amplio acceso a la red
3. Reservas de recursos en común.
4. Rapidez y elasticidad.
5. Servicio supervisado.

Por otro lado, existen tres modelos distintos de prestación de los servicios en la nube [11]: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) y Software as a Service (SaaS)

Independientemente del modelo de servicio utilizado, existen cuatro formas de despliegue de los servicios de CN [12]: Nube Privada, Nube Pública, Nube Híbrida y Nube Comunitaria.

Estos modelos y formas de despliegue de los servicios de CN implican el tratamiento de datos de carácter personal [13], y su regulación que se encuentra determinada en el cuerpo jurídico local.

La protección de datos es un derecho a la intimidad personal que tienen las personas contra un tratamiento incorrecto, no autorizado o contrario a las normativas vigentes de sus datos personales por tratadores de datos. Al proteger los datos personales frente al riesgo de la recopilación y el mal uso, se ampara por ende, la privacidad de las personas.

La presente investigación, se centra en la Ley 25.326 [14], que establece las pautas para

la transferencia internacional de datos y la prestación de servicios informatizados de información en proyectos de CN. Es una norma de orden público que regula la actividad de las bases de datos que registran información de carácter personal y garantiza al titular de los datos la posibilidad de controlar el uso de sus datos.

La contratación de servicios de cómputo en la nube (que para la legislación argentina es una prestación de servicios informatizados) implica necesariamente un tratamiento de datos personales por terceros y las obligaciones de este tratamiento se encuentran determinadas su artículo 25 de la Ley 25.326 [14] y en el mismo artículo del Decreto 1558/01 [15], que reglamenta dicha ley.

Poner en marcha una estrategia de CN en el exterior del país implica necesariamente la transferencia internacional de datos de carácter personal. Esto genera que el control de la información deja de estar bajo el dominio del usuario y entra en la órbita de un tercero. La ley argentina pone particular atención en este tipo de tratamiento regulándolo específicamente, ya que los principios y derechos incluidos en la misma corren riesgos si no se establece un control que constituya límites de garantía y seguridad en la transferencia de los datos hacia otros países.

La cesión de datos personales dentro del país no sufre restricciones[1]. Sin embargo, el panorama cambia al momento de transferir datos al exterior del país. En este último caso la ley contempla ciertos requisitos para que estas cuenten con garantías necesarias de respeto a la protección de la vida privada de los afectados y a sus derechos.

Para la ley 25.326, una transferencia internacional es un tipo de tratamiento de datos que consiste en la transmisión de datos, fuera de un Estado, realizado por el responsable del tratamiento a una persona física o jurídica, que los recibirá en un tercer país, para aplicarles un nuevo tratamiento, bien sea por cuenta propia o por cuenta del transmitente de los datos.

El principio general en materia de transferencia internacional se encuentra establecido en el artículo 12 de la Ley 25.326 [14] y dispone que la misma será lícita únicamente cuando el país importador de los datos tenga una legislación adecuada o equiparable a la del país exportador. Debido a la poca flexibilidad que otorga, se introdujo una excepción fundamental, a través del Decreto 1558/01, que establece que la prohibición de transferir datos personales hacia países u organismos que no proporcionen niveles de protección adecuados, no rige cuando el titular de los datos hubiera consentido expresamente o exista un contrato adecuado que garantice el nivel de protección de los datos personales.

El uso de servicios de computación en la nube, como se ha señalado, ofrece un gran número de ventajas. Pero a su vez presenta, por sus características específicas, una serie de riesgos que deben afrontarse con una adecuada gestión. En este aspecto las organizaciones deben estar atentas para revisar entre otros aspectos las obligaciones de cumplimiento regulatorio propias de la organización (como normas y procedimientos de seguridad corporativos) cómo a su vez la regulación local y de los países donde se procesarán los datos.

## Resultados y Objetivos

Teniendo en cuenta las falencias presentes, se concluye que es deseable, definir un proceso de análisis que permita describir y evaluar la reglamentación vigente en el país referida a la protección de datos personales en proyectos de cómputo en la nube en el exterior del país. El proceso de análisis propuesto permitirá identificar y valorar el grado de cumplimiento con la normativa local, lo que facilitará la toma de decisiones informadas, basadas no solo en criterios técnicos o económicos, sino también regulatorios.

Se buscará la validación del proceso de análisis mediante el estudio de casos empíricos

[1] La transferencia internacional de datos personales está específicamente regulada por el art. 12 de la Ley Nº 25.326, en el que se dispone la prohibición de transferir datos personales de cualquier tipo con países u organismos internacionales que no proporcionen niveles de protección adecuados. En la mencionada ley, no se imponen restricciones para la transferencia de datos dentro del país.

de implementación de servicios de CN a través de proveedores en el exterior del país.

Para ello, se proponen los siguientes objetivos específicos:

• Promover el uso buenas prácticas de seguridad y privacidad en CN establecidas en el estándar ISO/IEC 27018 [7].

• Individualizar y analizar la legislación Argentina relativa a la transferencia internacional de datos y a la prestación de servicios informatizados de datos personales.

• Identificar los principales riesgos asociados a la los datos personales en el modelo de negocios de CN.

• Desarrollar una propuesta inicial de metodología de evaluación de riesgos en materia de protección de datos personales en servicios de CN.

## Metodología de Trabajo

Las tareas a realizar para conseguir los objetivos antes mencionados serán las siguientes:

Para construir el conocimiento se seguirá un enfoque de investigación clásico [16-17] con énfasis en la producción de tecnologías [18], identificando métodos y materiales necesarios para desarrollar el proyecto.

Dentro de los métodos a utilizar se prevé: revisiones sistemáticas [19] y entrevistas con expertos [20]. Los expertos a entrevistar son: Dr. Pablo Palazzi [21], Dr. Horacio Azzolin [22], Iván Arce [23] y Dr. Daniel Altmark [24]

A continuación se detallan los materiales a utilizar:

• Ley N° 25.326 [14] y Decreto N° 1558/01 [15].

• Disposiciones y Dictámenes publicados por la Dirección Nacional de Protección de Datos Personales [25].

• Hemeroteca de la Universidad Tecnológica Nacional, Regional Buenos Aires [26].

• ISO/IEC 27018:2014 [6].

• Acceso a la biblioteca digital de IEEE [27].

• Acceso a la biblioteca digital de Springer [28].

• Acceso a la biblioteca digital de European Union Agency for Network and Information Security (ENISA) [29].

• Guía para la Evaluación de Impacto en la Protección de Datos Personales (Agencia Española de Protección de Datos) [30].

La presente investigación adopta una perspectiva descriptiva, empleando principalmente elementos cualitativos para identificar y describir las normas relativas a la protección de los datos personales que deben cumplirse en la implementación de proyectos de cómputo en la nube utilizando proveedores del exterior del país.

Para alcanzar los objetivos trazados se propone: (i) individualizar y analizar la legislación argentina relativa a la transferencia internacional de datos y a la prestación de servicios informatizados de datos personales, (ii) identificar casos de estudio, (iii) identificar los principales riesgos relativos a la seguridad de la información y a la privacidad de los datos en ambientes de CN, (iv) analizar los marcos regulatorios de otros países en cuanto a la transferencia internacional de datos personales, (v) realizar entrevistas semi estructuradas con expertos para validar la información recolectada en los puntos i, iii y iv, (vi) desarrollar una propuesta inicial de metodología de evaluación de riesgos en materia de protección de datos personales en servicios de CN, y (vii) validar los casos empíricos de implementación de servicios de CN en el exterior del país.

## Formación de Recursos Humanos

El proyecto busca tanto la obtención de nuevos conocimientos como la motivación de los implicados para que asciendan dentro de la carrera de investigadores.

Los recursos humanos deben poseer una firme convicción que la protección de los datos personales y el resguardo de la privacidad y la intimidad son centrales para el desarrollo de las personas y las organizaciones. De esta manera, se logra un doble beneficio, el proyecto obtiene e incorpora el conocimiento regulatorio y técnico de los recursos humanos en el área de la especialidad, a la vez que plantea un esquema de formación de especialistas de punta en el proceso de gestión.

Finalmente, en el marco de este proyecto de investigación se encuentra radicada una Tesis de Magister en Ingeniería en Sistemas de Información y un Trabajo Final de Especialidad. Asimismo, se prevé incorporar alumnos avanzados en la carrera de Ingeniería en Sistemas de Información con posibilidades de articular sus Trabajos Finales de Carrera de Grado. De esta manera se espera generar un verdadero espacio integrado de investigación en los niveles de carreras de grado y posgrado.

## Referencias


[1]. European Union: European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Unleashing the Potential of Cloud Computing in Europe, 27 September 2012, COM(2012) 529 final, disponible en: http://goo.gl/hBJKi7 disponible online en Marzo 2016.

[2]. Blodget, H. (2011), Amazon's Cloud Crash Disaster Permanently Destroyed Many Customers' Data http://goo.gl/CsDRKz disponible online en Marzo 2016.

[3]. Wittow, M. H. (2011) Cloud Computing: Recent Cases and Anticipating New Types of Claims http://goo.gl/PXEGKr disponible online en Marzo 2016.

[4]. Sherman, M. (2014) Supreme Court Justices concerned over impact on cloud computing in Aereo case http://goo.gl/TSVh4J. Disponible online en Marzo 2016

[5]. Etro, F. (2010) "The Economic Consequences of the Diffusion of Cloud Computing" en Dutta, Soumitra; Mia, Irene. The Global Information Technology Report 2009 – 2010 ICT for Sustainability. Londres, Foro Económico Mundial - INSEAD.

[6]. González Allonca J. C., Ruiz Martínez E. (2015) Cloud Computing: la regulación de la transferencia internacional de datos personales y la prestación de servicios por parte de terceros, Ed. Infojus DACF150527. http://goo.gl/efNsq6 disponible online en Marzo 2016.

[7]. ISO/IEC 27018:2014. (2014) Information technology – Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, International Organization for Standardization ISO.

[8]. Ravindran, A. (2013) Eemerging cloud computing paradigm and its impact on enterprises. Business Review: Advanced Applications, Cambridge Scholars Publishing http://goo.gl/JAPTjR disponible online en Marzo 2016.

[9]. Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing. Versión 3.0 (2011) https://goo.gl/cvCDgm disponible online en Marzo 2016

[10]. Ludwig S.,'Cloud 101: What the heck do IaaS, PaaS and SaaS companies do?', http://goo.gl/kn91F5 disponible online en Marzo 2016.

[11]. Voorsluys, W.; Broberg, J.; Buyya, R. (2011) Introduction to Cloud Computing. En R. Buyya, J. Broberg, A.Goscinski. Cloud Computing: Principles and Paradigms . EEUU: Wiley pp. 1–44. ISBN 978-0-470-88799-8.

[12]. McFedries, P. (2008) The Cloud Is The Computer. IEEE Spectrum Magazine http://goo.gl/GgQhHY disponible online en Marzo 2016.

[13]. Becerra, M., Navarro, M. (2012) Retos actuales para la protección de datos personales en las organizaciones. Universidad Nacional de San Juan, FFCEF y N , Proyecto Código Nº21/E/871. "Convergencia de Tecnologías informáticas y Metodologías para la implementación de sistemas de Información". (178-192).

[14]. Ley N° 25.326 (2000) Ley de Protección de Datos Personales. Boletín Oficial de la República Argentina.

[15]. Decreto 1558 (2001) Reglamentación de la Ley N° 25.326. Boletín Oficial de la República Argentina.

[16]. Riveros, H. y Rosas, L. (1985) El Método Científico Aplicado a las Ciencias Experimentales. México: Editorial Trillas. ISBN 96-8243-893-4.

[17]. Creswell, J. (2002) Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research. Prentice Hall. ISBN 10: 01-3613-550-1.

[18]. Sabato J, Mackenzie M. (1982). La Producción de Tecnología: Autónoma o Transnacional. Instituto Latinoamericano de Estudios Transnacionales - Technology & Engineering. ISBN 9789684293489.

[19]. Argimón J. (2004). Métodos de Investigación Clínica y Epidemiológica. Elsevier España, S.A. ISBN 9788481747096.

[20]. Martínez, M. (2006) La Investigación Cualitativa (Síntesis conceptual). Revista de investigación en psicología, ISSN-e 1560-909X, Vol. 9, Nº. 1, 2006 , pp. 123-146

[21]. Dr. Pablo Palazzi, Curriculum Vitae disponible en: http://goo.gl/VNe0nM

[22]. Dr. Horacio Azzolin, Curriculum Vitae disponible en: https://goo.gl/gvhMpw

[23]. Iván Arce, Curriculum Vitae disponible en: https://ar.linkedin.com/in/ivanarce

[24]. Dr. Daniel Altmark, Curriculum Vitae disponible en: http://goo.gl/YQ8s8Y

[25]. Acceso a normativa publicada por la Dirección Nacional de Protección de Datos Personales http://www.jus.gob.ar/datos-personales disponible online en Marzo 2016.

[26]. Hemeroteca de la Universidad Tecnológica Nacional, Regional Buenos Aires, Escuela de Posgrado. http://goo.gl/taoMv2

[27]. Biblioteca digital de IEEE http://goo.gl/u1CeGj disponible online en Marzo 2016.

[28].Biblioteca digital de Springer http://goo.gl/svKQj4 disponible online en Marzo 2016.

[29]. Biblioteca digital de European Union Agency for Network and Information Security (ENISA) https://goo.gl/Z0UZBL disponible online en Marzo 2016.

[30]. Agencia Española de Protección de Datos (2014) Guía para la Evaluación de Impacto en la Protección de Datos Personales, Agencia Española de Protección de Datos. https://goo.gl/FZTj8v disponible online en Marzo 2016.