Consideraciones Legales Relativas a la Privacidad en Proyectos de Cloud Computing en el Exterior de Argentina

Juan Cruz González Allonca[1,2] y Darío Piccirilli[2]
1. Dirección Nacional de Protección de Datos Personales. Ministerio de Justicia y Derechos Humanos. Argentina
2. Programa de Magister en Ingeniería de Sistemas de Información. Universidad Tecnológica Nacional (FRBA). Argentina
jgonzalez@jus.gov.ar, juanallonca@gmail.com, dpiccirilli@unlp.edu.ar, dariopiccirilli@gmail.com

***Abstract* — El modelo de prestación de servicios de cómputo en la nube (cloud computing) ofrece múltiples ventajas tanto técnicas como económicas para las empresas y organismos que deciden implementarla. Este modelo, sin embargo, requiere tener consideraciones de carácter legal y de cumplimiento normativo desde el inicio del proyecto. Este estudio se propone recorrer la normativa argentina relativa a la protección de datos personales bajo esta plataforma, brindándole al lector un panorama sobre el cuerpo normativo vigente que debe ser aplicado a servicios de cloud computing en el exterior del país. A su vez identifica los riesgos asociados a estos servicios que deben ser contemplados con el fin de evitar responsabilidades.**

***Palabras Clave* — Cloud Computing, Privacidad, Datos Personales, Legislación**

I. 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. Flexibilidad, accesibilidad, autoservicio bajo demanda, escalabilidad, gestión de grandes volúmenes de datos, son algunos de los beneficios que ofrece este esquema de cómputo. Sin embargo, estas ventajas, muchas veces no contemplan cuestiones críticas como la seguridad de la información y la privacidad de los datos almacenados o la intelectualidad de los datos y sistemas.

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. 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 cómputo en la nube.

Como se señala [Etro 2010] en un informe realizado por el Foro Económico Mundial en 2010 en el que se consultaba al sector industrial, gobiernos y académicos, los principales obstáculos para la adopción de servicios cloud se concentran en tres cuestiones de 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 cloud computing, 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. Existe legislación aplicable que determina la extensión de responsabilidad de usuario y proveedor. El realizar un análisis previo en este sentido, permite al usuario conocer la extensión de la reparación ante un evento que le provoque un daño. De este modo, el mismo podrá valorar qué delega en este modelo y qué cuestiones prefiere reservarse, pudiendo tomar una decisión responsable, basada en criterios técnicos y legales.

Uno de los grandes interrogantes que se presentan en torno a los soluciones de cómputo en la nube es como nos aseguramos que se están aplicando los procedimientos y disponiendo los medios necesarios para la protección de la información que se aloja y se procesa en esos ambientes. Este trabajo también pretende presentar alternativas para confirmar la aplicación de los procedimientos de seguridad utilizados.

En virtud de lo expuesto, la instancia metodológica comprende en primer lugar una descripción del modelo de servicios de cloud computing. Se explicarán sus características, tipos y modelos de despliegue.

En una segunda etapa se presentarán las distintas regulaciones aplicables en la Argentina relacionadas con servicios de cómputo en la nube en el exterior del país, como la transferencia internacional de datos personales y la prestación por cuenta de terceros de servicios de tratamiento de datos personales.

En tercer lugar se abordarán los principales riesgos asociados al modelo de cómputo en la nube, principalmente relacionados con la falta de control, disponibilidad y la confidencialidad de los datos alojados en ambientes cloud.

Luego se hará una breve descripción de distintos estándares de auditoría y control asociados a arquitecturas de cómputo en la nube.

Por último se expondrán las conclusiones obtenidas del trabajo y se trazarán las futuras líneas de investigación relacionadas con el tema.

II. El modelo de Cloud Computing

Hablar de cloud computing es presentar un concepto de servicios de cómputo por demanda. Se trata de un nuevo esquema en el uso de los recursos de tecnológicos y de los modelos de consumo y distribución de esos recursos.

El Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos y su laboratorio de tecnología de información, definió este nuevo concepto de la siguiente manera:

Cloud Computing es un modelo para habilitar acceso conveniente por demanda a un conjunto compartido de recursos computacionales configurables, por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios, que pueden ser rápidamente aprovisionados y liberados con un esfuerzo mínimo de administración o de interacción con el proveedor de servicios. Este modelo de nube promueve la disponibilidad y está compuesto por cinco características esenciales, tres modelos de servicio y cuatro modelos de despliegue[1].

Este modelo presenta un cambio importante en el paradigma computacional actual, la transformación de la infraestructura y las aplicaciones de un mundo claramente dominado y administrado por las organizaciones, a otro donde un tercero, en principio confiable y conocido, brinda capacidad de infraestructura para almacenamiento y uso de servicios o aplicaciones.

La Cloud Security Alliance (CSA) es la Guía para la Seguridad en áreas críticas de atención en Cloud Computing y describe cinco características esenciales en las que se evidencian similitudes y diferencias con las estrategias de computación tradicionales:

- Autoservicio por demanda. Un consumidor puede abastecerse unilateralmente de tiempo de servidor y almacenamiento en red, según sus necesidades, de forma automática sin requerir la interacción humana con cada proveedor de servicios.
- Amplio acceso a la red. Las capacidades están disponibles en la red y se accede a ellas a través de dispositivos estándar (p.ej., PC, teléfonos móviles y tablets).
- Reservas de recursos en común. Los recursos como por ejemplo el almacenamiento, el procesamiento o la memoria del proveedor son compartidos y pueden ser utilizados por múltiples clientes. Estos recursos son asignados dinámicamente y reasignados en función de la demanda de los consumidores. El cliente por lo general no tiene control o conocimiento exacto sobre la ubicación los recursos. Usualmente el proveedor no revela el lugar, aunque se puede especificar una ubicación genérica, como región o país.
- Rapidez y elasticidad. Las capacidades pueden suministrarse de manera rápida y elástica, en algunos casos de manera automática, para poder realizar el redimensionado correspondiente rápidamente. Para el consumidor, las capacidades disponibles para abastecerse a menudo aparecen como ilimitadas y pueden adquirirse en cualquier cantidad y en cualquier momento.
- Servicio supervisado. Los sistemas de nube controlan y optimizan el uso de los recursos de manera automática utilizando una capacidad de evaluación en algún nivel de abstracción adecuado para el tipo de servicio (p.ej., almacenamiento, procesamiento, ancho de banda, y cuentas de usuario activas).

[1] Mell P., Grance T., (2011) "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, U.S. Department of Commerce, NIST Special Publication 800-145

Existen tres modelos distintos de prestación de los servicios en la nube y se definen del siguiente modo:

Infrastructure as a Service (IaaS)

En este modelo de infraestructura como servicio, el Cloud Service Provider (CSP) brinda al usuario una infraestructura de recursos IT como procesamiento, energía, almacenamiento, redes y otros recursos básicos para que el consumidor pueda implementar y ejecutar cualquier tipo de aplicación. También suele llamárselo Hardware as a Service. Aquí, el usuario tiene control sobre los sistemas operativos, almacenamiento, aplicaciones desplegadas. Este esquema puede escalarse automáticamente, según las necesidades del cliente.

Un ejemplo de proveedor del modelo IaaS es Amazon y con su Elastic Compute Cloud (Amazon EC2). En este servicio el usuario tiene la capacidad de desplegar entorno informático virtual, que le permite utilizar interfaces de servicio web e iniciar instancias con distintos sistemas operativos, cargarlas con su entorno de aplicaciones personalizadas, gestionar sus permisos de acceso a la red y ejecutar su imagen utilizando los sistemas que desee[2].

Cabe señalar que Amazon no comenzó con la visión de crear un negocio de cloud computing. Esta compañía construyó una infraestructura masiva en apoyo de su propio negocio de venta y descubrió que sus recursos fueron infrautilizados. Por ello, en lugar de permitir que este activo quedara fuera de uso, Amazon decidió aprovechar esa capacidad y ofrecerla al mercado como IaaS[3].

Platform as a Service (PaaS)

En la plataforma como servicio, en cambio, la capacidad proporcionada al consumidor es el despliegue de todo lo necesario para la construcción y puesta en marcha de aplicaciones y servicios web completamente accesibles en Internet.

El consumidor no controla la capa de infraestructura de la nube pero gestiona las aplicaciones allí alojadas junto con la posibilidad de controlar su entorno y configuración.

Un claro ejemplo de PaaS es Google App Engine (GAE). Se trata de una plataforma gratuita que ofrece Google desde el año 2008 que permite a los usuarios desarrollar, ejecutar y alojar sus aplicaciones web en la infraestructura de Google[4]. El modelo de desarrollo de aplicaciones que ofrece dentro de GAE permite el crear aplicaciones en leguaje Pyton y Java, administrarlas vía una interfaz web y publicar la aplicación en los servidores de Google.

Software as a Service (SaaS)

En Software como servicio, la capacidad que se le promociona al consumidor consiste en utilizar las aplicaciones del proveedor que se ejecutan en una infraestructura de nube, las cuales pueden accederse desde distintos dispositivos e interfaces del cliente (p.ej., correo, web, VPN). En este nivel, el consumidor no gestiona ni controla la infraestructura de nube subyacente que incluye la red, servidores, tampoco sistemas operativos, almacenamiento con la posible excepción de unos parámetros de configuración de la aplicación específicos del usuario.

[2] Amazon Inc., *Funcionalidad de Amazon EC2*. http://aws.amazon.com/es/ec2/ Página vigente al 12 de septiembre de 2013.
[3] Bengamin Black (2009). *EC2 Origins.* http://blog.b3k.us/2009/01/25/ec2-origins.html Página vigente al 17 de septiembre de 2013.
[4] Zahariev A. (2009). *Google App Engine.* Helsinki University of Technology Seminar on Internetworking

Exponente del modelo SaaS es Google Drive. Se trata de un producto de Google que reemplaza a Google Docs que permite almacenar, crear, modificar, compartir y acceder a documentos, archivos y carpetas de todo tipo en un único lugar[5]. Una de las ventajas de esta aplicación es que no están ligada a una PC específica; no es necesario descargar ni instalar ninguna aplicación en una computadora en particular, y cualquier dispositivo con acceso a internet puede acceder también a las aplicaciones que brinda Google Drive. Debido a que cada usuario guarda la información en la nube, puede acceder a dicha información desde cualquier punto.

También permite la concurrencia de usuarios para editar los mismos archivos al mismo tiempo, lo que permite encarar procesos de colaboración online.

En este servicio, el usuario accede a aplicaciones que se ejecutan directamente sobre la infraestructura y la plataforma del proveedor.

Independientemente del modelo de servicio utilizado (SaaS, PaaS, IaaS) existen cuatro formas de despliegue de los servicios de cloud computing:

- Nube Privada: La característica principal de este modelo de despliegue es que el usuario no comparte infraestructura física con ningún otro cliente, agrupando los servicios y la infraestructura en una red privada, lo que ofrece un mayor nivel de seguridad y control. Se basa en la reserva de recursos hardware y software en exclusiva para un usuario.
- Nube Pública: En este despliegue los clientes contratan los recursos que necesiten para sus proyectos, siendo el proveedor del servicio el responsable del mantenimiento y de la gestión de la infraestructura, lo que reduce significativamente los costos iniciales de desarrollo de estructura y acceso inmediato a sus servicios en contratación.
- Nube Hibrida: El cliente gestiona exclusivamente su infraestructura, pero dispone de acceso a los recursos de la nube pública que controla el CSP en sus instalaciones, pudiendo ampliar sus recursos en cualquier momento, obteniéndolos de la nube pública.
- Nube comunitaria: Aquí, la infraestructura es compartida por diversas organizaciones y soporta una comunidad específica que tiene intereses similares (p.ej., misión, requisitos de seguridad, políticas y consideraciones sobre cumplimiento normativo).

Por lo tanto, basándonos en dichos conceptos, observamos que el proveedor de los servicios tiene una alta responsabilidad para mantener la continuidad, seguridad y control de la infraestructura tecnológica, de tal forma que el cliente, confíe, ejecute y utilice los servicios contratados con el tercero:

- En el modelo SaaS, en caso de ocurrir alguna falla en el uso de esta aplicación, el cliente no tendrá control para avanzar en el análisis de la misma, la cual estará supeditada a la reacción del proveedor del servicio.
- Por otro lado en el modelo PaaS, ante la existencia de errores o fallas del de sistema operativo, redes o almacenamiento, el cliente no tendrá margen de maniobra, pues estará limitado por la oportunidad del proveedor para soportar dicha falla.
- Finalmente en el modelo IaaS, el proveedor se encargará de lo referido a los temas de continuidad, acceso a los servidores y demás componentes tecnológicos.

En este escenario, los referentes de seguridad y control propios de tecnologías de información, adquieren una relevancia marcada, dado que se está entregando en un tercero la información de la empresa.

III. Marco Legal Aplicable

¿Cuál es la importancia de la privacidad y por qué la legislación argentina la protege? Es decir, ¿de dónde surge la necesidad de tomar medidas técnicas para su protección? La privacidad es un derecho humano fundamental y se encuentra receptado en tratados internacionales, leyes, disposiciones y jurisprudencia[6]. Es el derecho que protege la libertad individual, la libertad de expresión, la intimidad y la dignidad personal e incluye el derecho la protección de datos personales y la figura del Habeas Data.

Ahora bien, ¿cuál es la relación que existe entre privacidad, protección de datos y habeas data? De manera general, se puede decir que la protección a la privacidad es el género y la protección de datos la especie. Y todavía en un sentido más estricto queda la figura de habeas data, la cual se opera como un derecho de acceso a la información personal dentro del régimen de datos personales[7].

El derecho a la privacidad se sustenta en principios fundamentales como el honor y la dignidad personal. Como lo afirma la Secretaría de Asuntos Jurídicos, Organización de los Estados Americanos, "el derecho a la privacidad va más allá de la protección de datos, abarca el respeto de la vida familiar, preferencias religiosas, políticas y sexuales, fuera de la intervención de las comunicaciones, y fuera del uso de cámaras ocultas o de los análisis genéticos, etc. La protección de la vida privada y la protección de la intimidad son necesarias para el orden jurídico y como garantía de respeto a la dignidad personal"[8].

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 de sus datos personales, se ampara por ende, la privacidad de las personas.

[5] *Google Inc. Descripción general de Google Drive* https://support.google.com/a/answer/2490026?hl=es Página vigente al 10 de octubre de 2013.

[6] En el ámbito internacional, la Declaración Universal de Derechos Humanos de 1948, protege específicamente la privacidad territorial y de las comunicaciones. En su Artículo 12 establece que: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques". A su vez, se encuentra reconocido de forma expresa en el en tratados regionales. El artículo 11 de la Convención Americana sobre Derechos Humanos estipula el derecho a la privacidad en términos similares a los de la Declaración Universal. En 1965, la Organización de Estados Americanos proclamó la Declaración Americana de los Derechos y Deberes del Hombre, la cual estableció la protección de varios derechos humanos, entre ellos el de privacidad. Así también, la Corte Interamericana de Derechos Humanos ha empezado a ocuparse de problemas de privacidad en sus casos.

[7] Secretaría de Asuntos Jurídicos, Organización de los Estados Americanos (2012). Interrelación entre protección a la privacidad, protección de datos y habeas data. http://www.oas.org/dil/esp/proteccion_de_datos_privacidad_habeas_data.htm.

[8] Opt. Cit.

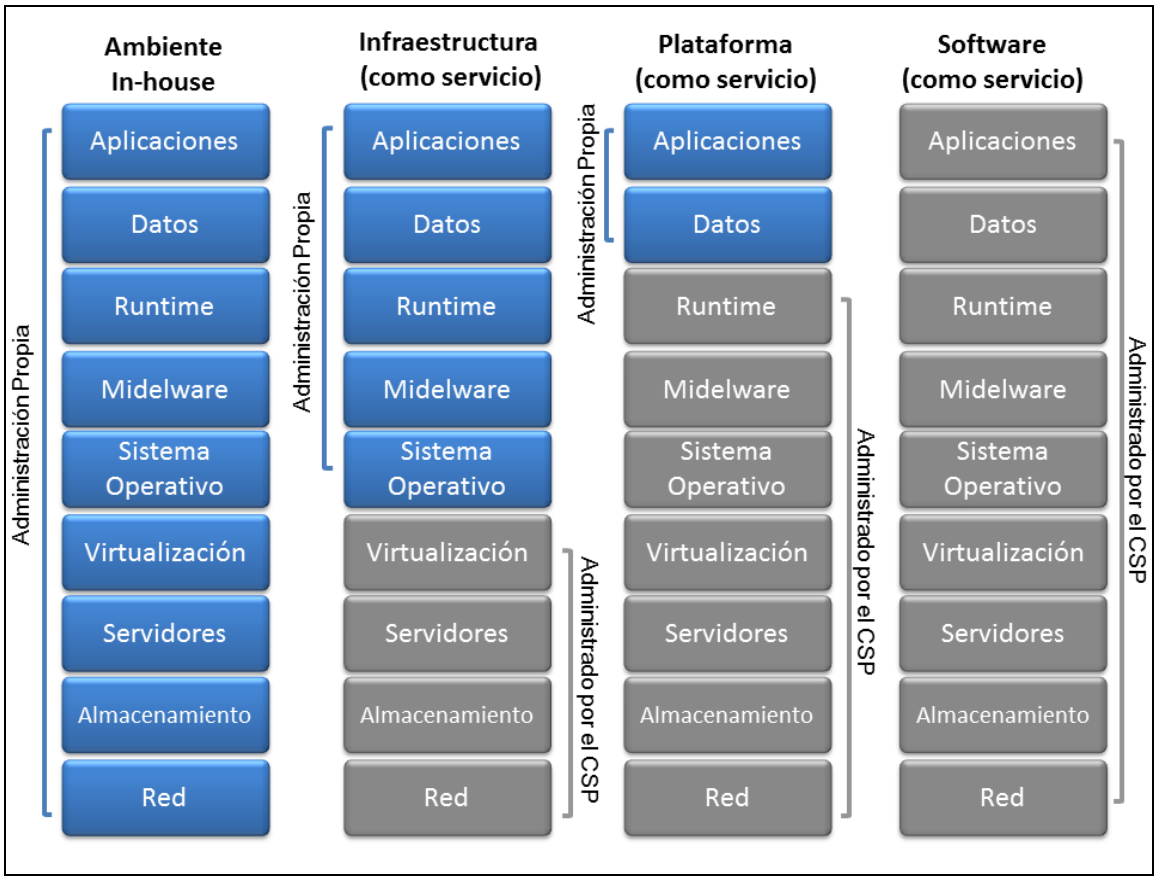

Fig. 1. Modelos de servicios de cloud computing [Ludwig 2011]

Dentro del derecho de protección de datos personales se encuentra la figura de Habeas Data. Se trata de una acción legal mediante la cual las personas agraviadas pueden informarse sobre datos referidos a ellos y el propósito de su recolección. A su vez permite exigir, dependiendo el caso, su rectificación, actualización o supresión de información personal alojada en bancos o registros de datos, públicos o privados[9].

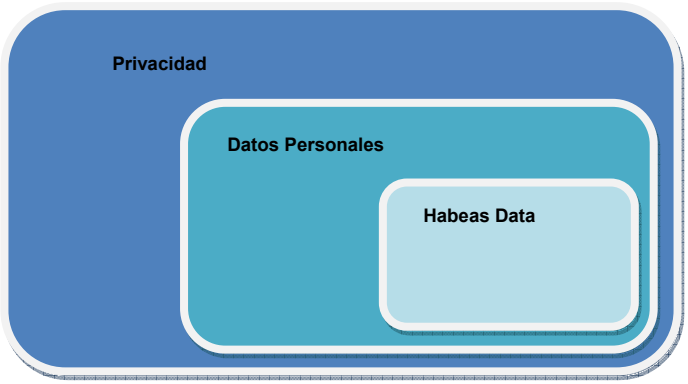

Figura 2.. Relación entre Privacidad, Protección de Datos y Habeas Data

Nuestro país cuenta con una amplia tradición en materia de protección de datos personales que se manifiesta en tres niveles distintos.

En el primer nivel se encuentra la Constitución Nacional, que luego de su reforma en el año 1994 incluyó el artículo 43 que en su párrafo tres contempla el llamado habeas data, de la siguiente forma:

Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística.

Como se advierte, esta reforma de la Constitución Nacional ha establecido una institución que carecía de antecedentes en el derecho federal aunque ya se encontraba en las constituciones provinciales: la acción de habeas data.

Se trata de un procedimiento especialmente necesario a partir del aumento del uso de las computadoras que pueden compilar la información y datos personales afectando el honor y la privacidad de las personas. La acción también está establecida para tomar conocimiento de estos datos y en su caso exigir la supresión, rectificación, confidencialidad o actualización.

El segundo nivel está representado por la ley 25.326 sancionada en el año 2000, que tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre.

A su vez, el Poder Ejecutivo reglamentó dicha ley por medio del decreto N° 1558 del año 2001 en el que se crea la Dirección Nacional de Protección de Datos Personales, que es el órgano de control de la ley, primero en América Latina y el tercero del hemisferio sur.

[9] Esta acción se encuentra regulada en la legislación argentina en los artículos 14 y 16 de la ley 25.326 de Protección de Datos Personales.

En un tercer nivel encontramos la interpretación y la aplicación que hacen los jueces de estas normas.

A partir de este desarrollo legislativo, Argentina fue declarada país adecuado por la Unión Europea en materia de Protección de Datos Personales, de conformidad con la "Directiva 95/46/CE". Esta directiva reconoce a la Argentina como país en condiciones de cumplir con los controles que exige la Unión Europea y garantiza la debida salvaguarda o tutela de los datos personales. Cabe destacar que la Argentina fue uno de los cinco primeros países, por fuera de la Unión Europea, en obtener este reconocimiento en el año 2003[10].

Esta adecuación constituye un beneficio significativo por diversas razones. En primer lugar, permite el libre flujo de datos y también elimina requisitos, autorizaciones y garantías adicionales para la transferencia internacional de datos personales. Esto a su vez impacta en mayor grado sobre la inversión en el país, ya que empresas de diversos rubros -tales como call centers, de informática, financieras, etc.- contemplarán a la Argentina con mayores ventajas comparativas respecto al resto de los países de la región[11].

En la presente investigación, se hará énfasis en la ley de protección de datos personales, ya que nos ayudará a analizar la transferencia internacional de datos y la prestación de servicios informatizados de información en proyectos de cómputo en la nube.

La Ley de Protección de Datos Personales

La Ley 25.326 es una norma de orden público, es decir fundamental para regular el orden social del país y por lo tanto no pude ser dejada de lado por un acuerdo entre particulares. 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 personales.

Esta ley define su objeto en su artículo 1º como la protección integral de los datos personales asentados en bancos de datos, sean éstos públicos o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre.

En su artículo 2°, y con la intención de fijar criterios unificados aplicables a todo el articulado, la ley establece una serie de definiciones:

Datos personales: información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

Datos sensibles: datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

Archivo, registro, base o banco de datos: conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

Tratamiento de datos: operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

Responsable de archivo, registro, base o banco de datos: persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.

Datos informatizados: datos personales sometidos a tratamiento o procesamiento electrónico o automatizado.

Titular de los datos: toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.

Usuario de datos: toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.

Disociación de datos: todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

Requisitos de licitud del tratamiento de datos personales

Al hablar de los datos personales, es importante saber que principios rigen su tratamiento. Como se remarcó en el apartado anterior, el tratamiento de datos implica una multiplicidad de acciones, que van desde la recolección pasando por su procesamiento hasta la destrucción de los mismos, es decir todo el ciclo de vida de la información. Para que estas acciones sean licitas, la ley impone determinados requisitos que deben cumplirse por el responsable de un registro o base de datos.

Inscripción en el Registro:

El artículo 3° establece que la formación de archivos de datos será lícita cuando se encuentren debidamente inscriptos y la información allí alojada no puede tener finalidades contrarias a las leyes o a la moral pública.

Es importante destacar que la inscripción, por si sola, no implica la licitud del Banco de Datos, sino que debe cumplir asimismo con el resto del ordenamiento de la Ley Nº 25.326. Dicha inscripción debe realizarse en el Registro Nacional de Bases de Datos, lo que no implica ceder los datos, sino que se trata de una mera descripción del banco de datos.

Es importante destacar que el cumplimiento de la ley y la licitud de la base de datos protege a los responsables de bases de datos frente a eventuales denuncias por ejercicio de los derechos de acceso, rectificación, supresión o bloqueo (arts. 14, 16 y 27 Ley 25.326) o problemas en el tratamiento de datos personales. Una base de datos no inscripta en el Registro carece de otra condición de licitud, lo que acarreará responsabilidades y sanciones más severas, al contrario que una base de datos debidamente inscripta.

La inscripción en el Registro Nacional de Bases de Datos debe comprender como mínimo la siguiente información:

a) Nombre y domicilio del responsable;
b) Características y finalidad del archivo;
c) Naturaleza de los datos personales contenidos en cada archivo;
d) Forma de recolección y actualización de datos;
e) Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos;
f) Modo de interrelacionar la información registrada;

[10] Decisión de la Comisión de las Comunidades Europeas con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina (2003). http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:168:0019:0022:ES:PDF. Página vigente al 10 de septiembre de 2013.

[11] Comisión Europea, Comunicado de prensa (2012). http://europa.eu/rapid/press-release_IP-12-1403_es.htm. Página vigente al 10 de septiembre de 2013.

g) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información;
h) Tiempo de conservación de los datos;
i) Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos.

A su vez aclara que ningún usuario de datos podrá poseer datos personales de naturaleza distinta a los declarados en el registro y que el incumplimiento de estos requisitos puede generar sanciones administrativas previstas en la ley.

Calidad de los datos:

a) Características de los datos: Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.
b) La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la ley.
c) Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.
d) Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario.
e) Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados.
f) Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso.
g) Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.

Consentimiento libre, expreso e informado:

El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias.

Interés legítimo:

La información personal podrá circular entre distintas personas sólo si existe un interés legítimo que lo justifique. Sin interés legítimo la información no podrá circular en el mundo informativo.

Información del Banco de Datos:

El artículo 13 de la Ley Nº 25.326 establece que toda persona puede solicitar al organismo de control información relativa a la existencia de bancos de datos personales, sus finalidades y la identidad de sus responsables. La consulta del Registro es pública y gratuita.

Seguridad:

El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad y confidencialidad de los datos personales. Es en el artículo 9 de la ley 25.326 donde se impone a los tratadores de datos que implementen medidas de seguridad de la información con el fin de evitar la adulteración, pérdida, consulta o tratamiento no autorizado de los datos, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

En tal sentido, la autoridad de control de la ley, ejerciendo su atribución de dictar normas y procedimientos técnicos relativos al tratamiento y condiciones de seguridad de las bases de datos, creó dos disposiciones:

La primera es la Disposición 11/2006 en la que se fijan las medidas de seguridad para el tratamiento y conservación de los datos personales contenidos en archivos, registros, bancos y bases de datos públicos no estatales y privados. En ella se establecen tres niveles de seguridad: Básico, Medio y Critico, conforme la naturaleza de la información tratada, pautas aplicables también a los archivos no informatizados (registro manual).

Para cada uno de los niveles antes mencionados prevén distintas medidas de seguridad, establecidas teniendo en cuenta la mayor o menor necesidad de garantizar la confidencialidad e integridad de la información contenida en el banco de datos respectivo; la naturaleza de los datos y la correcta administración de los riesgos a que están expuestos, así corno también el mayor o menor impacto que tendría en las personas el hecho de que la información registrada en los archivos no reúna las condiciones de integridad y confiabilidad debidas.

La segunda disposición es la 09/2008 donde se aprueba un modelo de documento de seguridad de datos personales.

Es importante remarcar que estas regulaciones de seguridad implican un piso o estándar básico, lo que no obsta a que los organismos y empresas escalen las mismas otorgando mayores medidas de seguridad a sus bases de datos.

Confidencialidad:

El deber de secreto respecto de los datos personales tratados, es una obligación que corresponde al responsable de la base de datos y a toda persona que efectúe tratamiento de datos personales, obligación que se mantiene aún finalizada la relación que permitió el acceso al banco de datos.

Respeto de los derechos del titular del dato:

La ley le otorga al titular del dato determinados derechos como los de información, acceso, rectificación, actualización y supresión (arts. 14, 15 y 16 Ley Nº 25.326), todos de raigambre constitucional (art. 43 CN).

El ciudadano tiene derecho a estar informado por completo acerca de los usos que se darán a sus datos personales, razón por la cual el responsable o usuario de la base de datos deberá informarle en forma expresa y clara acerca de la existencia del archivo, nombre del responsable y su domicilio; la finalidad de la base de datos y sus destinatarios; el carácter obligatorio u optativo de responder al cuestionario que se le proponga; las consecuencias de brindar datos, su negativa a darlos o la inexactitud de los mismos; la posibilidad de ejercer los derechos de acceso, rectificación o supresión y, en caso de preverse cesiones de los datos, a quién y con qué fin se cederán los mismos.

Tratamientos especialmente regulados por la ley

Como se expuso más arriba, la ley de protección de datos personales en su artículo 2° entiende por tratamiento las operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias. Pero a su vez, por considerarlas relevantes para la integridad de

los datos, regula de forma específica algunos tipos de tratamiento de datos, entre ellos la prestación de servicios informatizados, la cesión y la transferencia internacional.

Cesión:

La cesión de datos implica necesariamente la transferencia de información. Sin embargo, debe tenerse en cuenta que ésta no constituye la delegación de la titularidad del dato, que siempre es de la persona a la que se refiere.

Existen una serie de requisitos impuestos por el artículo 11 de la ley de protección de datos personales para que la cesión se constituya como válida y son los siguientes:

A. Interés legítimo de cedente y cesionario: El interés es la medida de todas las acciones y el interés legítimo es aquel que justifica para su titular el ejercicio de las acciones correspondientes[12].

La cesión debe ser realizada para el cumplimiento de los fines que justificó la recolección de los datos y esta finalidad no puede ser distinta o incompatible a la que motivó la recolección del dato, ya que de lo contrario se estaría vulnerando el principio de finalidad establecido por el artículo 4º.

Cabe remarcar que en las Bases públicas (por ejemplo el Padrón Electoral) destinadas a la difusión, el interés legítimo está implícito en el interés general.

B. Condiciones para la cesión: Los datos personales, objeto de tratamiento, sólo pueden ser cedidos con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan individualizarlo.

Se considera a la cesión como una de las operaciones más riesgosas, que justifica la exigencia de un consentimiento específico, ya que el titular del dato pierde el control de su propia información personal, debido a que la misma sale del ámbito de quien la recabó.

No se exige el consentimiento para la cesión en los siguientes casos:

- Cuando así lo disponga una ley (es necesaria una ley formal del Poder Legislativo).
- En los supuestos previstos en el artículo 5° inciso 213.
- Cuando se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias;
- Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados;
- Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables.

La prestación de servicios informatizados de datos personales

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 en el artículo 25 de la Ley 25.326 y en el mismo artículo del decreto que reglamenta dicha ley:

Artículo 25.- Ley 25.326

1. Cuando por cuenta de terceros se presten servicios de tratamiento de datos personales, éstos no podrán aplicarse o utilizarse con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni aun para su conservación.

2. Una vez cumplida la prestación contractual los datos personales tratados deberán ser destruidos, salvo que medie autorización expresa de aquel por cuenta de quien se prestan tales servicios cuando razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrá almacenar con las debidas condiciones de seguridad por un período de hasta dos años.

A su vez, en el artículo 25 del Decreto 1558 del año 2001, formula que:

Los contratos de prestación de servicios de tratamiento de datos personales deberán contener los niveles de seguridad previstos en la Ley Nº 25.326, esta reglamentación y las normas complementarias que dicte la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, como así también las obligaciones que surgen para los locatarios en orden a la confidencialidad y reserva que deben mantener sobre la información obtenida.

La realización de tratamientos por encargo deberá estar regulada por un contrato que vincule al encargado del tratamiento con el responsable o usuario del tratamiento y que disponga, en particular:

a) que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento;

b) que las obligaciones del artículo 9º de la Ley Nº 25.326 incumben también al encargado del tratamiento.

Por lo tanto, a partir de este último artículo, se suman otros requisitos a considerar al momento de la realización de un contrato escrito de prestación de servicios de tratamiento de datos personales.

En relación a lo analizado sobre estos dos artículos, deberá tenerse en cuenta:

1. Contar con un contrato de prestación de servicios de tratamiento de datos personales, en el que se determine la relación entre las partes
2. Fijar en el mismo contrato que la empresa prestadora de servicios informatizados se compromete a:
   a. Cumplir con los niveles de seguridad previstos en la ley

[12] Pueden advertirse los alcances específicos del interés legítimo en dictamen 98/2005 de la Dirección Nacional de Protección de Datos Personales: "El "interés legítimo" requerido por la citada norma, es el que determina la licitud del tratamiento de datos personales. De modo que, no sólo la finalidad de la base de datos debe ser legítima sino que la cesión de datos sólo puede hacerse "para el cumplimiento de los fines relacionados con los intereses legítimos del cedente y del cesionario". Es una manera de hacer respetar el principio de finalidad para que los datos que fueron recogidos con un fin no sean destinados a otro. Ambos - cedente y cesionario - serán responsables solidariamente, por la observancia de la Ley Nº 25.326 (artículo 11, inciso 4), ya que las restricciones que rigen la operatoria del cedente se extienden al cesionario respecto de la utilización de los datos".

[13] No será necesario el consentimiento cuando: a) Los datos se obtengan de fuentes de acceso público irrestricto; b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento; e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526.

b. Con la reglamentación y las normas complementarias que dicte la Dirección Nacional de Protección de Datos Personales (DNPDP),

c. Como así también las obligaciones que surgen en orden a la confidencialidad y reserva que deben mantener sobre la información obtenida.

Es fundamental hacer énfasis en que la empresa u organización que adquiera servicios de cómputo en la nube, deberá asegurarse que la prestadora asuma y garantice estas obligaciones, ya que en caso de incumplimiento (por ejemplo, pérdida o fuga de información) será la empresa que contrata estos servicios quien debe responder ante los titulares de los datos personales.

Otro punto importante sobre este tema es la prohibición de realizar algún tipo de cesión. Es decir, que la empresa contratada para el tratamiento informatizado de datos, no podrá realizar otra cesión de información a un tercero, ni siquiera para fines de almacenamiento.

Transferencia internacional

Poner en marcha una estrategia de cloud computing 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 transferencia de datos personales dentro del país no sufre restricciones. 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.

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.

En este tipo de tratamiento se pueden identificar la intervención de dos tipos de sujetos: un exportador de los datos y un importador de los mismos.

El exportador de datos es el responsable del tratamiento que transfiere los datos personales fuera del país. El importador de datos es quien recibe los datos del exportador para su posterior tratamiento, o el encargado del tratamiento que convenga en recibir del exportador datos personales para su posterior tratamiento en nombre de éste, conforme a las instrucciones que aquél le entrega.

El principio general en materia de transferencia internacional se encuentra establecido en el artículo 12 de la ley 25.326 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[14]. Por ejemplo, si fuera necesario realizar la transferencia de datos personales a Francia, no sería necesaria una autorización específica, ya que ese país cuenta con un adecuado nivel de protección según el órgano de control argentino, la Dirección Nacional de Protección de Datos Personales.

Cabe destacar que es responsabilidad del transmisor argentino verificar las condiciones del país receptor.

Debido a la poca flexibilidad que otorga, se introdujo una excepción fundamental en la reglamentación de dicho artículo. La misma establece que la prohibición de transferir datos personales hacia países u organismos internacionales o supranacionales que no proporcionen niveles de protección adecuados, no rige cuando el titular de los datos hubiera consentido expresamente.

Para los en que el consentimiento del titular del datos sea de difícil cumplimiento (por ejemplo grandes bases de datos). La Dirección Nacional de Protección de Datos Personales permite suplir dicho consentimiento si se confecciona un contrato adecuado que garantice el nivel de protección de los datos personales. De esta forma, y a partir de un marco contractual confeccionado entre las partes, será finalmente posible la transferencia internacional de los datos.

Para el caso de EEUU, principal proveedor de servicios de cloud computing y por ende, país destino de las transferencias internacionales, quien no posee una legislación adecuada para la protección de datos personales en los términos de la Ley Nº 25.326, la licitud de la transferencia internacional dependerá del amparo que establezcan las cláusulas contractuales entre el exportador y el importador.

De esta forma y para recapitular, cuando una transferencia internacional de datos personales tenga por objeto la prestación de servicios de tratamiento de datos personales por parte de terceros (art. 25 Ley Nº 25.326) y como destino un país u organismo internacional que no proporcionen niveles de protección adecuados, según lo define la ley 25.326 en su art. 12 y el Decreto reglamentario 1558/01, y la transferencia no esté contenida entre las excepciones del art. 12 inc. 2 de la ley 25.326 o no cuente con el consentimiento previsto por el art. 12 del Anexo I del Decreto 1558/01, se deberá celebrar un contrato -además o junto con el previsto en el art. 25 de la ley 25.326- de transferencia internacional de datos entre el exportador y el importador que contenga razonablemente, y en lo que resulte pertinente, las siguientes condiciones:

a) Identificar al exportador y al/los importador/es de los datos, o sea a las partes del contrato de transferencia, indicando nombre, número de identificación (en caso de existir), dirección, teléfono, fax y correo electrónico.

b) Indicar la ubicación de las bases de datos y ante quien, donde y como podrá ejercer sus derechos el titular del dato, describiendo nombres, números de identificación (en caso de existir), la dirección, teléfono, fax y correo electrónico.

c) Definir como ley aplicable del contrato, derechos y obligaciones aplicables al mismo, a la ley argentina Nro. 25.326. En tal sentido, las definiciones de los términos contractuales deberán seguir las de la ley 25.326. Las partes deben asumir la totalidad de las disposiciones de la ley

[14] En el mismo artículo contempla casos puntuales donde se aplica esta prohibición. Estos son: a) Colaboración judicial internacional; b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto se realice en los términos del inciso e) del artículo anterior (se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables); c) Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable; d) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte; e) Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

25.326 como norma básica y condición de existencia del contrato.

d) Determinar de manera precisa las categorías y sub-categorías de datos personales a transferir.

e) La declaración jurada del exportador manifestando que el tratamiento de los datos que va a transferir se realiza en un total de acuerdo con la ley 25.326, indicando expresamente que el archivo se encuentra inscripto ante la Dirección Nacional de Protección de Datos (DNPDP) y que en el formulario de registro ha denunciado como destino de transferencia al país u organismo internacional receptor.

f) Indicar la finalidad a la que serán destinados dichos datos, verificando que cumpla con los requisitos del art. 4 de la ley 25.326.

g) En caso que la transferencia implique una cesión de datos deberá desprenderse del mismo el cumplimiento de los requisitos de los arts. 4, 5 y 11 de la ley 25.326.

h) Precisar las medidas de seguridad a las que se sujetará la transferencia y el tratamiento de datos personales, verificando que la misma cumpla con las pautas habituales del sector y con la normativa vigente.

i) El compromiso del importador que los datos recibidos serán tratados en un todo y sin excepciones según lo dispone ley 25.326, y de que se obliga frente a la DNPDP y los titulares de los datos, a respetar y dar cumplimiento a la totalidad de los derechos y facultades que la ley 25.326 les otorga, y que no cederá los datos a quienes no resulten firmantes del contrato y se sometan a iguales obligaciones.

j) El exportador y el importador responderán solidariamente frente a los titulares de los datos y a la DNPDP por todo eventual incumplimiento del contrato y la ley aplicable.

k) El exportador y el importador se obligarán a responder de manera solidaria y conforme a la ley argentina frente a los titulares de los datos cuando estos resulten perjudicados como consecuencia de la transferencia y el tratamiento de sus datos personales.

l) La garantía de que el titular de los datos podrá ejercitar los derechos de acceso, rectificación, supresión y demás derechos contenidos en el Capítulo III, arts. 13 a 20 de la ley 25.326, tanto ante el exportador como el importador de los datos.

m) El compromiso del importador de cumplir las disposiciones de la DNPDP, en especial sus facultades de inspección y sanciones, permitiendo a la DNPDP en el ejercicio de sus funciones, o a quien esta delegue, el acceso a la documentación y equipos que se utilicen en el tratamiento de datos personales objetos del contrato de transferencia internacional.

n) La declaración del importador de que no tiene motivos para creer que la legislación local aplicable le impida cumplir con sus obligaciones convenidas en el contrato de transferencia.

ñ) La obligación de destruir, y en su caso también reintegrar al exportador, los datos personales objeto de la transferencia cuando se produzca alguna de las siguientes circunstancias: 1) Finalización del contrato; 2) Imposibilidad de cumplimiento de las disposiciones de la ley 25.326; 3) Extinción de la finalidad por la que se transmitieron los mismos.

o) Se pactará la jurisdicción de los Tribunales argentinos por cualquier conflicto o reclamo que surgiera con motivo de dicha transferencia internacional.

A su vez, las transferencias internacionales deben ser denunciadas ante la DNPDP mediante el Formulario de Inscripción en el Registro Nacional de Bases de Datos (art. 21 de la Ley 25.326), donde se requiere a los Responsables de Bancos de Datos privados que indiquen el destino del país al que transfieren sus datos, lo que permite a la DNPDP el control de las mismas y exigir la acreditación del cumplimiento de las garantías necesarias.

Sanciones

A la hora de garantizar el cumplimiento de la norma, la legislación argentina establece sanciones efectivas y disuasorias, tanto de naturaleza administrativa como penal. Asimismo, en caso de que el tratamiento ilícito haya causado perjuicios, se aplicarán las normas de la legislación relativas a la responsabilidad civil (tanto contractual como extracontractual).

Por lo tanto, el no cumplimiento de las exigencias establecidas en la ley, trae como consecuencia la imposición de las sanciones, las que pueden ser de dos tipos: de carácter administrativo o penal.

Sanciones Administrativas

Como se ha descrito anteriormente, la ley de protección de datos personales estipula que todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control. El incumplimiento de estos requisitos dará lugar a las sanciones administrativas.

De esta forma el artículo 31 establece la responsabilidad por daños y perjuicios derivados de la inobservancia de ley. El organismo de control podrá aplicar las sanciones de apercibimiento, suspensión, multa, clausura o cancelación del archivo, registro o banco de datos.

La aplicación y cuantía de estas sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad.

A su vez, y según la Disposición 7/2005 de la DNPDP, las infracciones se clasifican en tres tipos: leves, graves y muy graves.

Sanciones Penales

Según el Código Penal, modificado por leyes 25326 y 26388, se aplicará la pena de prisión a quienes cometan los siguientes delitos:

- Proporcionar a un tercero a sabiendas información falsa contenida en un archivo de datos personales.
- Acceder, de cualquier forma, a un banco de datos personales a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos.
- Proporcionar o revelar, en forma ilegítima, a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.
- Insertar o hiciere insertar datos, en forma ilegítima, en un archivo de datos personales.

La pena se agrava con inhabilitación si el que cometiere el delito es un funcionario público. Las penas de prisión varían de seis meses a cuatro años y medio, dependiendo del delito cometido y la gravedad del mismo.

IV. Riesgos para la Protección de los Datos Personales Asociados al Modelo de Cloud Computing

El uso de servicios de computación en la nube, como se ha señalado en puntos anteriores, ofrece un gran número de ventajas. Desde la reducción de costos hasta la flexibilidad y escalabilidad de los recursos informáticos. 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 las obligaciones de cumplimiento regulatorio propias de la organización (como normas y procedimientos de seguridad corporativos), y a su vez la regulación tanto local como de los países donde se procesarán los datos.

Las implicaciones de la localización de los datos, los elementos de protección de la privacidad de los datos de clientes, proveedores y empleados de la empresa, los usos secundarios de la información almacenada en la infraestructura del proveedor, el manejo de las amenazas de seguridad que se presenten, el aseguramiento de los planes de continuidad de negocio, la respuesta a los posibles litigios donde se solicite información corporativa disponible en la nube, los elementos del monitoreo de los servicios contratados en la nube y los elementos concretos de terminación del contrato con el proveedor son algunos de los temas que tanto en el ámbito académico como en el privado se están analizando.

Debido a que el presente trabajo hace eje en el tratamiento de los datos personales en ambientes de cloud computing, sólo se trataran los riesgos específicos relacionados con este contexto.

Para la doctrina actual en materia de protección de datos personales, existen dos grandes riesgos a gestionar por las organizaciones a la hora de embarcarse en un proyecto de cómputo en la nube[15]:

1. La falta de información sobre las condiciones en la que se presta el servicio (transparencia);
2. La falta de control del responsable sobre el uso y gestión de los datos personales por parte de los agentes implicados en el servicio.

Falta de Información

En cuanto a la falta de información, por un lado el proveedor es quien conoce de forma integral los detalles del servicio que ofrece. En virtud de ello existe la necesidad de conocer cabalmente el funcionamiento específico del servicio. Por ejemplo el qué, quién, cómo y dónde se lleva a cabo el tratamiento de los datos que se proporcionan al proveedor para la prestación del servicio. "Si este último no da una información clara, precisa y completa sobre todos los elementos inherentes a la prestación, la decisión adoptada por el responsable no podrá tener en consideración de forma adecuada requisitos básicos como la ubicación de los datos, la existencia de suben cargados, los controles de acceso a la información o las medidas de seguridad. De esta forma, se dificulta al responsable la posibilidad de evaluar los riesgos y establecer los controles adecuados[16]".

El documento antes mencionado reconoce también que la falta de información sobre las operaciones de tratamiento de datos presenta un riesgo, tanto para los responsables de los datos como para los tratadores de los mismos. Debido a que carecen en muchos casos de información sobre las amenazas y riesgos potenciales y por tanto no podrán adoptar las medidas que consideren apropiadas.

Algunas posibles amenazas pueden derivarse de que el responsable del tratamiento no sepa que:

- Se realiza un tratamiento en cadena con múltiples encargados del tratamiento y subcontratistas.
- Los datos personales se tratan en diferentes zonas geográficas. Ello incide directamente en la legislación de protección de datos aplicable a los litigios que puedan surgir entre usuario y proveedor.
- Se transmiten datos personales a terceros países no pertenecientes a la Comunidad Europea. Los terceros países pueden no proporcionar un nivel adecuado de protección de datos y las transferencias pueden no contar con las medidas de protección adecuadas (por ejemplo, cláusulas contractuales estándar o normas empresariales vinculantes) y, por tanto, esto puede ser ilegal.

Falta de control

La falta de control del responsable sobre la información alojada en estos servicios se evidencia a partir de las dificultades para conocer fehacientemente la ubicación de los datos, las problemas a la hora de disponer de los datos en poder del proveedor o de poder obtenerlos en un formato válido e interoperable, los obstáculos a una gestión efectiva del tratamiento o, en definitiva, la ausencia de control efectivo a la hora de definir los elementos principales del tratamiento en lo refiere a las garantías técnicas y organizativas.

Según el informe elaborado por la Comunidad Europea la falta de control mencionada puede manifestarse en los siguientes ámbitos:

- Falta de disponibilidad debido a la falta de interoperabilidad (dependencia respecto del proveedor): si el proveedor se basa en tecnología patentada, puede resultar difícil para un cliente mover los datos y documentos entre diferentes sistemas en la nube (portabilidad de los datos) o intercambiar información con entidades que utilicen servicios de computación en nube gestionados por distintos proveedores (interoperabilidad).
- Falta de integridad causada por la puesta en común de los recursos: una nube se compone de sistemas e infraestructuras comunes. Los proveedores tratan datos personales procedentes de una amplia gama de interesados y organizaciones, y es posible que surjan conflictos de intereses u objetivos diferentes.
- Falta de confidencialidad por lo que respecta a las solicitudes de intervención legal realizadas directamente a un proveedor: los datos personales tratados en la nube pueden ser objeto de solicitudes de intervención legal por parte de las autoridades policiales o judiciales de los Estados miembros de la UE y de terceros países. Existe el riesgo de revelación de datos personales a servicios incluso extranjeros sin una base jurídica de la UE válida y, por tanto, se daría una violación de la legislación de la UE sobre protección de datos.

[15] Grupo de Trabajo del Artículo 29 de la Comunidad Europea Dictamen 05/2012 sobre la computación en nube, disponible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_es.pdf Vigente al 24 de agosto de 2013.

[16] Dictamen 05/2012 Op. Cit.

- Falta de posibilidad de intervención debido a la complejidad y la dinámica de la cadena de subcontratación: el servicio de computación en nube ofrecido por un proveedor puede realizarse combinando servicios de varios proveedores distintos, que pueden añadirse o suprimirse dinámicamente a lo largo de la duración del contrato del cliente.
- Falta de posibilidad de intervención (derechos de los interesados): un proveedor no podrá aportar las medidas e instrumentos necesarios para ayudar al responsable del tratamiento a gestionar los datos en términos de, por ejemplo, acceso, supresión o corrección.
- Falta de aislamiento: un proveedor podrá ejercer su control físico sobre los datos de distintos clientes para vincular los datos personales. Si se proporciona a los administradores derechos de acceso suficientemente privilegiados (funciones de alto riesgo), podrían vincular información de distintos clientes.

En el mismo sentido, la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) realizó un estudio técnico donde se analizan los riesgos y ventajas para la seguridad que presenta el uso de la computación en nube, y ofrece orientaciones sobre protección para sus usuarios.

En dicho estudio se evaluó el nivel de riesgo de la protección de los datos donde destaca que "en algunos casos, puede ser difícil para el cliente en nube (en su función de controlador de datos) comprobar de manera eficaz el procesamiento de datos que lleva a cabo el proveedor en nube, y en consecuencia, tener la certeza de que los datos se gestionan de conformidad con la ley.

Tiene que quedar claro que el cliente en nube será el principal responsable del procesamiento de los datos personales, incluso cuando dicho procesamiento lo realice el proveedor en nube en su papel de procesador externo"[17].

Del mencionado informe se copian a continuación los cuadros 1 y 2 que reflejan variables como la probabilidad, el impacto, los activos afectados y el nivel de riesgo vinculados a los cambios de jurisdicción y la protección de los datos personales en ambientes cloud.

V. Auditoría y Control

Una pregunta recurrente al momento de pensar en soluciones como cloud computing es de qué forma una empresa radicada en la Argentina puede saber a ciencia cierta si se implementan las medidas de seguridad exigidos por la normativa local y por los acuerdos establecidos contractualmente entre el cliente y el CSP.

A partir del crecimiento en la utilización de arquitecturas de cómputo en la nube y los riesgos de seguridad asociados a ella las empresas se ven obligadas a utilizar nuevos modelos de auditoría para hacer frente a este cambio de paradigma. Como se analizó en el punto anterior existen una serie de riesgos vinculados a este modelo de servicio lo que redunda en la utilización de nuevos procesos de autoría y control para asegurar la confianza del cliente.

Es por ello que la realización de controles y auditorías específicas sobre protección de los datos personales es fundamental para establecer una relación de confianza entre los proveedores del servicio y sus clientes.

Como se afirma en el Dictamen 05/2012 del Grupo de Trabajo del Artículo 29 sobre la computación en nube de la Comunidad Europea, la verificación independiente o la certificación por terceros que gocen de reconocido prestigio puede ser un medio creíble para que los proveedores demuestren el cumplimiento de sus obligaciones según lo especificado en el presente dictamen. De esta forma una certificación dará, al menos, una presunción que se ha sido objeto de una auditoría o control en relación a una norma reconocida.

La auditoría informática consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información protege el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas[18]. Esto pone de manifiesto de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos, identificando necesidades, duplicidades, costes, valor y barreras, que obstaculizan flujos de información eficientes.

A partir de los procesos de auditoría se asegura que los sistemas y procesos son lo que dicen ser y que existe una persona para asumir la responsabilidad de ello. La auditoría puede llevarse a cabo por diversas razones, tales como el cumplimiento de una norma o resolución gubernamental o a partir del cumplimiento de una política corporativa.

Es en este punto, donde los clientes se plantean una serie de preguntas recurrentes a la hora de iniciar un proyecto de cloud computing en el exterior: ¿cómo puedo auditar los niveles de prestación de servicio del CSP? ¿con qué marcos de referencia para una evaluación o auditoría cuento? ¿Cómo puedo asegurarme de que se cumplen las medidas de seguridad? ¿Cuenta el proveedor con una certificación de procesos adecuada?¿En el caso de pactarse que un tercero independiente audite la seguridad, cuál va a ser entidad auditora y los estándares reconocidos que aplicará?

Cómo aporte para alcanzar algunas respuestas a esos interrogantes, se describirán brevemente estándares de auditoría y control y los diferentes dominios de riesgos que aparecen al utilizar cloud computing con los que cuenta el usuario para poder verificar que el CSP cumple con lo pactado.

A este nivel, los estándares de buenas prácticas más utilizados son: SSAE 16, ISO 27001 y COBIT 5.

A continuación se identificarán sus alcances y objetivos.

SSAE 16

SSAE 16 (Statement on Standards for Attestation Engagements No. 16) es una norma desarrollada por el AICPA (American Institute of Certified Public Accountants) orientada a organizaciones proveedoras de servicios. Esta norma reemplaza desde 2011 a la antigua SAS 70. Es una verificación independiente del cumplimiento con los controles de seguridad y de la eficacia de tales controles. Provee una guía para que un auditor independiente emita una opinión sobre los controles de la organización a través del Reporte de Servicio del Auditor; este reporte puede ser de dos tipos:

- El reporte de tipo I detalla la descripción de controles de la organización en un punto específico de tiempo.

[17] Catteddu D.; Hogben, G. (editores) (2009). *Cloud Computing. Benefits, risks and recommendations for information security*. Heraklion: ENISA p. 49.

[18] Cristiá, M. (2011) *Auditoría de Sistemas, Universidad Nacional de Rosario*. Página vigente al 26 Octubre 2013 http://www.fceia.unr.edu.ar/asist/intro-aa-t.pdf

Probabilidad	ALTA
Impacto	ALTO
Vulnerabilidades	Falta de información sobre jurisdicciones Almacenamiento de datos en jurisdicciones múltiples y falta de transparencia sobre este punto
Activos afectados	A1. Renombre de la compañía A2. Confianza del cliente A5. Datos personales sensibles A6. Datos personales A7. Datos personales - críticos A9. Prestación del servicio – servicios en tiempo real A10. Prestación del servicio
Riesgo	ALTO

Cuadro 1. Riesgos de la Protección de Datos [Catteddu; Hogben 2009]

Probabilidad	MUY ALTA
Impacto	ALTO
Vulnerabilidades	Falta de información sobre jurisdicciones Almacenamiento de datos en jurisdicciones múltiples y falta de transparencia sobre este punto
Activos afectados	A1. Renombre de la compañía A2. Confianza del cliente A5. Datos personales sensibles A6. Datos personales A7. Datos personales - críticos A9. Prestación del servicio – servicios en tiempo real A10. Prestación del servicio
Riesgo	ALTO

Cuadro 2. Riesgos derivados del cambio de jurisdicción [Catteddu; Hogben 2009]

El reporte de tipo II no sólo incluye la descripción de controles de la organización, sino que también incluye el detalle de los controles de la organización durante un período mínimo de seis meses.

Una vez finalizada la inspección, el auditor de servicios presenta una opinión sobre la siguiente información[19]:

1. Si la descripción que da la organización de servicios sobre los controles es adecuada.
2. Si los controles de la organización de servicios se han diseñado eficazmente.
3. Si los controles de la organización de servicios se han puesto en marcha en una fecha específica.
4. Si los controles de la organización de servicios se ejecutan con eficacia durante un periodo de tiempo especificado. (Solo para el Tipo II de SSAE 16 (SOC 1)).

Su alcance es sobre el control interno de la organización, alcanza procesos internos referentes a clientes, recursos humanos, operaciones, etc.

Empresas como Google aplican este proceso de auditoría para servicios cloud como Google App y Google App Engine[20].

[19] Microsoft Inc. *Seguridad, auditorías y certificaciones, Información sobre seguridad, privacidad y cumplimiento normativo de Office 365 y Microsoft Dynamics CRM Online* http://www.microsoft.com/online/legal/v2/es-es/MOS_PTC_Security_Audit.htm Página vigente al 31 de octubre de 2013.

[20] Google Inc. (2011); Security Whitepaper: Google Apps Messaging and Collaboration Products. También en Feigenbaum E. Security First: Google Apps and Google App Engine complete SSAE-16 audit. http://googleenterprise.blogspot.com.ar/2011/08/security-first-google-apps-and-google.html Página vigente al 15 de octubre de 2013.

ISO/IEC 27001

ISO/IEC 27000 es un conjunto de estándares elaborados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. Su objetivo es implantar una serie de procedimientos y controles para asegurar la gestión de la seguridad de la información en el alcance que se defina: activos de la organización susceptibles de implementar medidas, procedimientos y gestión para minimizar el riesgo derivado de su falta de integridad, confidencialidad y disponibilidad[21] . No sólo implica activos de tecnología de la información, sino otros como archivos en soporte papel, recursos humanos, etc.

La certificación de esta norma se logra a partir de un proceso por el cual una entidad de certificación externa, independiente y acreditada audita el sistema, determinando su conformidad con ISO/IEC 27001, su grado de implantación real y su eficacia y, en caso positivo, emite el correspondiente certificado.

La guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información (ISO/IEC 27002) establece 11 dominios de control que cubren por completo la Gestión de la Seguridad de la Información:

1) Política de seguridad.
2) Aspectos organizativos de la seguridad de la información.
3) Gestión de activos.
4) Seguridad ligada a los recursos humanos.
5) Seguridad física y ambiental.
6) Gestión de comunicaciones y operaciones.
7) Control de acceso.
8) Adquisición, desarrollo y mantenimiento de los sistemas de información.
9) Gestión de incidentes de seguridad de la información.
10) Gestión de la continuidad del negocio.
11) Cumplimiento.

COBIT 5

Control Objectives for Information and related Technology (COBIT) Nro. 5 es una guía de mejores prácticas dirigida a la gestión de tecnología de la información (TI). Este programa de auditoría y seguridad creado por ISACA (Information Systems Audit and Control Association) puede utilizarse como guía para para la realización de un proceso de auditoría de servicios de cloud computing.

COBIT 5 se utiliza como una herramienta de examen y punto de partida, puede ser adaptado por profesionales y auditores.

Los objetivos de la auditoría en servicios de la nube son:

- Proporcionar a los interesados una evaluación de la eficacia de los controles internos de los servicios y seguridad provistos por el proveedor en la nube
- Identificar las deficiencias de control interno dentro de la organización del cliente y su interrelación con el proveedor de servicios
- Proporcionar a los interesados de auditoría una evaluación de la calidad y su capacidad de confiar en las certificaciones del proveedor de servicios, en materia de controles internos.

Esta guía no está diseñada para reemplazar auditorías de aplicaciones de procesos específicos y excluye la garantía de la funcionalidad de una aplicación.

El examen se centra en:

1. El gobierno de computación en nube
2. El cumplimiento contractual entre el prestador y el cliente
3. El control de problemas específicos de computación en nube

En cada uno de estos marcos de buenas prácticas, los proveedores deben asumir retos de protección de los activos de información de los clientes, que articulen los números de eficiencia y efectividad en la entrega del servicio, con los niveles confiabilidad esperados por el cliente tanto en rendimiento de la plataforma, efectividad de los servicios invocados, así como en las condiciones de acceso y monitoreo de la plataforma en sus estrategias de administración.

VI. Conclusiones y futuras líneas de Investigación

Como conclusión del presente trabajo se desprende que al momento de iniciar un proyecto de cloud computing, no solo deben evaluarse variables relativas a la rentabilidad, capacidad tecnológica y ventaja de negocios, sino también es prioritario analizar el cumplimiento normativo y las cláusulas sobre seguridad de la información, especialmente las relativas a la protección de los datos personales. De no contar con ellas deben incorporase ya que existe legislación, que en definitiva, resulta aplicable a fin de determinar la extensión de responsabilidad de usuario y del proveedor. A su vez realizar un análisis en este sentido otorga a la previsión de antemano de estas cuestiones, lo que permite al usuario conocer la extensión de la reparación ante un evento que le provoque un daño. De este modo, el usuario podrá valorar qué delega en este modelo y qué cuestiones prefiere reservarse, pudiendo tomar una decisión basada en información concreta.

A su vez se puede concluir que la mejora de la seguridad de la información vendrá necesariamente asociada al desarrollo de un marco legal internacional más claro, unificado y acorde a los ambientes de cloud computing.

Como futuras líneas de investigación y a fin de complementar el presente trabajo de especialización se propone el estudio de diversos temas.

En primer lugar, y como se señaló en este estudio, el contexto internacional actual, la normativa y los mecanismos regulatorios no ofrecen criterios legales unificados. Lo que genera inconvenientes en estrategias como la de cloud computing, donde los datos son transferidos a jurisdicciones con normativas disimiles o no conocidas con precisión. Este vacío normativo promueve, sin embargo, que los desafíos en materia de protección de los datos personales recaigan en mecanismos de auto regulación, como la privacidad desde el diseño o privacy by design (PbD).

Por otro lado, resultará de gran utilidad abordar la cuestión de los SLA - Acuerdos de Niveles de Servicio y Modelos

[21] ISO/IEC 27001. (2005). Information security management systems – International Organization for Standardization – ISO, Ginebra, Suiza.

Contractuales vinculados a los servicios de cloud computing y establecer recomendaciones de índole legal fácilmente aplicables sobre cuestiones vinculadas con la protección de los datos personales.

VII. Bibliografía

[1] Marko, H. (2011). Cloud Computing Security and Privacy Issues. http://www.cepis.org/media/CEPIS_Cloud_Computing_Security_v17.11.pdf Página vigente al 15 de Febrero de 2013.

[2] Guilloteau, S., Venkatesen, M. (2012). Privacy in Cloud Computing - ITU-T Technology Watch Report March 2012. http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000160001PDFE.pdf Página vigente al 11 de Febrero de 2013.

[3] Peyrano, G. (2002) "Régimen legal de los datos personales y el habeas data". Editorial Depalma. ISBN: 9501418626

[4] Pérez Martínez J. Vergara Pardillo A. (2012) "El impacto de la regulación sobre los nuevos servicios" en Pérez J. y Badía E. (coords.) El debate sobre la privacidad y seguridad en la red. Regulación y mercados. Editorial Ariel ISBN: 9788408034360.

[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] Cavoukian, A. (2009), "Privacy by Design: The 7 Foundation Principles", Information and Privacy Commissioner Ontario, Canada http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf Página vigente al 22 de Julio de 2013.

[7] Mell P., Grance T., (2011) "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, U.S. Department of Commerce, NIST Special Publication 800-145

[8] Dictamen 05/2012 del Grupo de Trabajo del Artículo 29 de la Comunidad Europea sobre la computación en nube, disponible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_es.pdf Página vigente al 24 de octubre de 2013.

[9] Catteddu, D.; Hogben, G. (eds.) (2009). "Cloud Computing. Benefits, risks and recommendations for information security". ENISA

[10] Ludwig S.,'Cloud 101: What the heck do IaaS, PaaS and SaaS companies do?', VentureBeat blog, venturebeat.com/2011/11/14/cloud-iaas-paas-saas/ Página vigente al 25 de septiembre de 2013

[11] Information Systems Audit and Control Association (ISACA) (2011), IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud. ISBN 978-1-60420-185-7

Juan Cruz González Allonca. Es especialista en Ingeniería de Sistemas de Información por la Universidad Tecnológica Nacional. Es abogado por la Facultad de Derecho de la Universidad de Buenos Aires y tiene diploma de posgrado en Gestión de la Seguridad Informática por Facultad de Ingeniería de la Universidad Austral. Actualmente se desempeña como responsable del área de sistemas en la Dirección Nacional de Protección de Datos Personales, dependiente del Ministerio de Justicia de la Nación Argentina.

Darío Piccirilli. Licenciado en Sistemas de la Universidad Tecnológica Nacional (1979), con estudios de Posgrado como magister en Ingeniería de Software en el Instituto Tecnológico de Buenos Aires (Argentina) y Master en Ingeniería de Software en la Universidad Politécnica de Madrid (España). Profesor Titular en la Cátedra de Pericias Informáticas (Carrera de grado en Ingeniería en Sistemas de Información) y Profesor Titular en la Cátedra Auditoría, Seguridad y Pericias Informáticas (Carrera de Maestría en Sistemas de Información) en la Facultad Regional Buenos aires de la Universidad Tecnológica Nacional. Profesor Titular en Pericias Informáticas (Especialización de Posgrado en Redes) En la Facultad de Informática de la Universidad Nacional de La Plata (Argentina). Especialista en Pericias Informáticas en fueros Penal, Civil, Comercial y Laboral del Poder Judicial de la Nación dela República Argentina (desde 1989 a la fecha).