UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

agesic

Análisis de la Norma ISO/IEC 27.018 desde la perspectiva de la Protección de Datos Personales

(Mayo 2015)

Esc. María Cecilia Montaña
Dr. Gonzalo Sosa Barreto

www.datospersonales.gub.uy / Tel: (+598) 29010065 opción 3 / Andes 1365 piso 7 (C.P. 11100 / Montevideo, Uruguay)

1.- Introducción.

La Norma ISO/IEC Nº 27.018, de 01 de agosto de 2014, perteneciente a la familia de la Serie 27.000 relativas a la seguridad de la información, fue creada para estandarizar el procesamiento de datos personales para las empresas que prestan servicios en la nube. La misma complementa y se apoya en gran medida en otras normas ISO/IEC como la 27.001 y en particular la 27.002 y su Anexo, que establece los estándares para la implementación de sistemas de gestión de seguridad de la información en la nube.

En particular, AGESIC elaboró un conjunto de directrices para la aplicación de la Ley Nº 18.331 de 11 de agosto de 2008 según la familia de normas ISO/IEC 27.000, con el objetivo de constituirse en recomendaciones vinculadas a la seguridad de la información que pudieran adoptar las organizaciones, a fin de dar cumplimiento a la Ley citada y su reglamentación[1].

Para comenzar el análisis de la norma que nos ocupa, interesa definir que se entiende por norma. La definición de "Norma" puede encontrarse en la Directiva Europea 98/34/EC "Sobre reglas técnicas referidas a los servicios de la sociedad de la información" (Artículo 1 (6)), que la define cómo: ***"una especificación técnica aprobada por un organismo reconocido de actividad normativa para aplicación repetida o continua, cuya observancia no es obligatoria, y que está incluida en una de las categorías siguientes: - norma internacional: norma adoptada por una organización internacional de normalización y puesta a disposición del público, - norma europea: norma adoptada por un organismo europeo de normalización y puesta a disposición del público, - norma nacional: norma adoptada por un organismo nacional de normalización y puesta a disposición del público."*** [2]

Las normas ISO/IEC por su parte representan **"*(...) un consenso global en una solución para un tema particular. Proveen requerimientos, especificaciones, lineamientos, o características que pueden ser usadas consistentemente para asegurar que los materiales, productos, procesos y servicios son seguros para usarse y adecuados para el propósito*[3]"**.

---

[1] Disp. http://www.agesic.gub.uy/innovaportal/file/1065/1/Ley_18311_Normas_de_Seguridad_CERTificate.pdf. Acc. 27/2/2015.

[2] Disp. http://ec.europa.eu/enterprise/policies/single-market-goods/files/directive98-34/index_es.pdf. Acc. 26/02/2015.

[3] Ver documento "Using and referencing ISO and IEC standards to support public policy " disponible en http://www.iso.org/sites/policy/documents/Using%20and%20referencing%20ISO%20and%20IEC%20standards%20to%20support%20public%20policy%20-%20EN.pdf. Acc. 26/02/2015. Traducción por los informantes.

La norma objeto del presente se estructura en 18 capítulos y cuenta con un anexo muy relevante a los efectos de la protección de datos personales al proponer un conjunto de controles para los Proveedores de Servicios de Nube.

La norma aporta a los mencionados Proveedores, -que además procesan información de identificación personal (personally identifiable information o PII)-, buenas prácticas que permiten que tanto cliente como proveedor cumplan con un conjunto de requisitos mínimos vinculados a la Protección de Datos Personales.

Los estándares de la ISO/IEC Nº 27.018 se alinean al modelo europeo de Protección de Datos Personales, recogiendo los contenidos del Dictamen sobre computación en la nube, publicado por el Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995. Esta Directiva refiere a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Desde hace ya varios años Uruguay es un país adecuado respecto al estándar de la normativa de la Unión Europea, por lo cual resulta altamente recomendable realizar el estudio de la ISO/IEC Nº 27.018.

2.- Análisis de la Norma Técnica y su Anexo.

2.1.- Presentación de la norma.

Todas las organizaciones que prevean seleccionar un proveedor para contratar servicios en la nube podrán tomar esta norma como referencia al momento de un mejor tratamiento de los datos personales.

La Norma pretende brindar un marco común a todas las organizaciones que procesen datos personales en la nube, independientemente de si se encuentran en un país adecuado o no. Se lograría con la adopción de este estándar, mayor confianza en los proveedores de servicios en la nube que lo implementen.

Sí es importante destacar que como toda norma técnica, la misma establece un conjunto de medidas a adoptar, pero no necesariamente el cumplimiento in totum de las mismas importa el cumplimiento de la normativa nacional en materia de protección de datos, por lo cual quien contrate los servicios del proveedor deberá analizar no sólo si éste se adecua a la norma sino además, si por el carácter o tipo de información que se maneja, o por las operaciones que se prevén con la misma, no requiere de medidas adicionales atento a la legislación uruguaya -en el caso-. En consecuencia, debe analizarse en primer lugar la normativa de protección de datos personales.

2.2.- Alcance.

Comienza describiendo el alcance de la norma, indicando que abarca a las organizaciones de cualquier tipo y tamaño, ya sean públicas o privadas, organismos gubernamentales y organizaciones sin fines de lucro que contractualmente provean servicios de procesamiento de información como encargados de tratamiento de PII a otras organizaciones a través de la nube.

El estándar propuesto puede también ser relevante para otras organizaciones responsables de PII, si bien éstas pueden estar sujetas a otros controles legales no aplicables a los encargados de tratamiento.

Vemos así que desde el punto de vista subjetivo, en principio la norma abarca a todo tipo de Proveedor de Servicios de Nube que opere como encargado de tratamiento de la información, por cuenta de un cliente.

Además, también resulta destacable que **la aplicación de los estándares se encuentra prevista para hipótesis de nube "pública".** Recordemos que según las definiciones del National Institute of Standards and Technology (NIST), la "nube pública" consiste en aquella infraestructura que se provee para uso abierto por el público en general, que puede ser propiedad, u operada o gestionada por una organización empresarial, académica, o gubernamental, o por una combinación de ellas, y existe bajo la premisa de que hay un proveedor de nube[4][5].

La ISO/IEC describe además el marco normativo de referencia, que incluye normas de Cloud Computing y normas técnicas de seguridad.

---

[4]Ver al respecto http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. Acc. 24/02/2015. El documento refiere a los distintos tipos de cloud, de servicios prestados a través de la misma, y otras definiciones de interés en la temática.

[5]En el caso uruguayo, se cuenta por parte de los organismos del inciso Presidencia con una nube que "*(...) se diseñó con la finalidad de optimizar la gestión, mejorando la calidad de los servicios en base a la aplicación de estándares muy exigentes de la industria, alojándose en el nuevo Datacenter de la Torre Ejecutiva, diseñado específicamente para brindar estos servicios y respaldado en normas de organismos internacionales como ISO, TIA, BICSI, ICREA entre otros. Este respaldo implica la obtención de buenos niveles de seguridad, disponibilidad y confiabilidad, al cumplir con determinados requerimientos para con la electricidad, el aire acondicionado, la seguridad, la obra civil y las comunicaciones entre otros*." Conf. http://www.agesic.gub.uy/innovaportal/v/3028/16/agesic/que_es.html. Acc. 24/02/2015. Independientemente de ello, debe tenerse presente que estas nube no es "pública" en el sentido arriba mencionado sino "privada", por lo que no se aplican directamente los estándares previstos en esta norma.

Esos niveles deben ser acordes a los establecidos en el decreto 92/014 de 24 de abril de 2014 en el Anexo III "Lineamientos para la implementación y uso de centros de datos seguros", aplicables a toda la Administración Central (Art. 3º).

2.3.- Definiciones.

La ISO/IEC establece una serie de definiciones que en líneas generales se encuentran emparentadas con las manejadas por la Unión Europea y nuestro país, con algunas aclaraciones que se verán luego.

En definitiva, el estándar hace aplicables todas las definiciones contendidas en las normas ISO/IEC 17.788 y la familia de las ISO/IEC 27.000, con algunas referencias particulares a algunos conceptos que se verán a continuación.

A los efectos de determinar la adecuación o no de los mencionados conceptos a la normativa uruguaya, parece conveniente establecer un paralelismo entre las definiciones de la ISO/IEC y aquellas provistas por la legislación nacional (en particular la Ley Nº 18.331 y el decreto Nº 414/009 de 31 de agosto de 2009), lo que se detallará en el Anexo I.

Resulta relevante realizar además, las siguientes distinciones entre las definiciones que determinan el alcance de la ISO/IEC 27.018 y la legislación nacional:

a) Respecto del concepto de "data breach". Sólo existe en la legislación de protección de datos una referencia indirecta a "vulneración de seguridad", así como una referencia más genérica a "incidente de seguridad" en el decreto Nº 451/009 de 28 de setiembre de 2009. No obstante ello, de la definición provista por el decreto, la referencia del decreto Nº 414/009 y la aplicación práctica del artículo 10 de la Ley Nº 18.331 (Principio de seguridad de los datos), puede alcanzarse una definición aproximada a la referida en la ISO/IEC.

b) Respecto del alcance de los titulares de la PII. Se distingue el "personally identifiable information (PII) principal" del "titular de dato personal" como está establecido en la normativa nacional, en que la ISO/IEC restringe su alcance a las "personas físicas", a diferencia de la norma uruguaya, que también es aplicable a las personas jurídicas.

c) Respecto al "public cloud service provider" o "proveedor de servicios de nube pública". En la legislación nacional no existe una norma específica asociada a este concepto, salvo referencias indirectas como la realizada en el Anexo III del decreto Nº 92/014 ya referido, que en su último punto indica que "*Se deben definir acuerdos de niveles de servicio con los proveedores que den soporte a los componentes críticos del centro de datos y deben ofrecer cobertura en un régimen de 7 días/24 horas/365 días/año*".

Sí es importante señalar que la norma refiere a proveedores de servicios de nube pública que operen exclusivamente como encargados de tratamiento en los términos del artículo 4 literal H de la Ley Nº 18.331, siendo aplicable

además al caso, como se verá luego, entre otros, el artículo 30 del mismo cuerpo normativo ("*Prestación de servicios informatizados de datos personales.- 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.*

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").

2.4.- El **capítulo 4** presenta una visión general de la norma, incluyendo un cuadro en el que se especifican, conjuntamente con las categorías ya definidas en la ISO/IEC 27.002, los casos en que se imponen controles adicionales referidos a la temática de la ISO/IEC 27.018.

Las categorías de control de la ISO son las siguientes:

a) Objetivo del control estableciendo qué es lo que se procura obtener; y

b) uno o más controles que pueden aplicarse para alcanzar el objetivo de control.

Finalmente, los restantes numerales en los que se divide la norma tienen un paralelismo como se mencionó, con la ISO/IEC 27.002, en las que mayormente se entienden aplicables los estándares previstos en la citada norma, con algunas guías específicas vinculadas al tratamiento de la PII.

Veremos algunas cuestiones jurídicas planteadas en algunos de los puntos mencionados en la ISO/IEC 27.018:

a) Políticas de seguridad de la información (cláusula 5).

En este punto, y como guías específicas, se hace hincapié en la necesidad de que las políticas de seguridad de la información tengan en cuenta el apoyo y compromiso para alcanzar la adecuación a la normativa en materia de protección de datos y a los contratos entre los proveedores de servicios de cloud que además realizan tratamiento de datos y sus clientes. Estos contratos deberían determinar además las responsabilidades de unos y otros dependiendo del tipo de servicio prestado.

Se afirma en la ISO/IEC que algunas legislaciones sólo son aplicables al responsable de los datos pero no a los encargados de tratamiento, por lo que la

responsabilidad del segundo debería estar estipulada en el contrato, que podría además ser auditado conforme los estándares previstos en la ISO/IEC Nº 27.002.

En el caso uruguayo ya se ha hecho mención a la distinción entre responsable de los datos y encargado de tratamiento, debiendo aclararse además que la Ley Nº 18.331 establece en su artículo 12 específicamente la consagración del principio de responsabilidad, por el cual el responsable de la base de datos es responsable de la violación de las disposiciones de la presente ley. Independientemente de ello, la responsabilidad del encargado de tratamiento también es clara en la Ley Nº 18.331 en su artículo 35 que prevé la posibilidad de que el encargado de tratamiento sea sancionado al igual que el responsable por el organismo de control, y en el decreto Nº 414/009 en su artículo 7º que establece la responsabilidad del encargado de tratamiento de proteger los datos personales sometidos a tratamiento mediante las "*(...) medidas técnicas y organizativas que resulten idóneas para garantizar su integridad, confidencialidad y disponibilidad*". Finalmente, el artículo 17 inciso final de la Ley Nº 18.331 reafirma lo antedicho al establecer: "*El destinatario quedará sujeto a las mismas obligaciones legales y reglamentarias del emisor y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate*".

En conclusión, a los efectos de la normativa uruguaya debe tenerse presente que existe responsabilidad tanto del responsable como del encargado de tratamiento, preste éste o no sus servicios en la nube.

b) Organización de Seguridad de la Información (cláusula 6).

La mayoría de los numerales referidos en este punto hacen referencia a normas técnicas establecidas en la ISO/IEC 27.002, con excepción del caso del numeral 6.1.1 en materia de roles y responsabilidades de seguridad de la información. En este punto se indica que el PII processor debería de designar un punto de contacto para ser empleado por el cliente del servicio de cloud vinculado al tratamiento contractual de la PII. Más allá de la razonabilidad de la medida, la misma no merece comentarios del punto de vista jurídico.

c) Seguridad de los recursos humanos (cláusula 7).

Al igual que en el resto de los casos, son aplicables los conceptos de la ISO/IEC 27.002 haciéndose una especial referencia para el caso del numeral 7.2.2 vinculado al conocimiento, educación y entrenamiento en seguridad de la información. Se propone que se adopten medidas para dar a conocer al personal en las posibles consecuencias de las vulneraciones de seguridad en el tratamiento de datos para el encargado de tratamiento, su personal y el

titular. La ISO/IEC señala que en algunas jurisdicciones el encargado de tratamiento en la nube pública puede estar sujeto a sanciones que pueden ser económicas por parte de la autoridad de control. En otras, se supone que el uso de estos estándares en los contratos entre el proveedor y el cliente podrá establecer las bases para sanciones contractuales en caso de incumplimientos.

El cumplimiento del principio de reserva impone también la necesidad de que los involucrados en el tratamiento de la información tengan conocimiento de las consecuencias de un accionar ilegítimo. En particular el artículo 11 de la Ley Nº 18.331 indica: "*Aquellas personas físicas o jurídicas que obtuvieren legítimamente información proveniente de una base de datos que les brinde tratamiento, están obligadas a utilizarla en forma reservada y exclusivamente para las operaciones habituales de su giro o actividad, estando prohibida toda difusión de la misma a terceros.*

Las personas que, por su situación laboral u otra forma de relación con el responsable de una base de datos, tuvieren acceso o intervengan en cualquier fase del tratamiento de datos personales, están obligadas a guardar estricto secreto profesional sobre los mismos (artículo 302 del Código Penal), cuando hayan sido recogidos de fuentes no accesibles al público. Lo previsto no será de aplicación en los casos de orden de la Justicia competente, de acuerdo con las normas vigentes en esta materia o si mediare consentimiento del titular.

Esta obligación subsistirá aun después de finalizada la relación con el responsable de la base de datos".

Son aplicables a estas consideraciones las analizadas en el literal a) (cláusula 5), vinculado a la posibilidad por parte de la URCDP de imponer sanciones tanto al responsable como al encargado de tratamiento de los datos.

d) Gestión de activos (cláusula 8).

No existen nuevos lineamientos además de los previstos en la ISO/IEC 27.002.

e) Control de acceso (cláusula 9).

Existen guías específicas en los numerales vinculados a gestión de acceso de usuarios (numeral 9.2), registro y eliminación de usuarios (numeral 9.2.1) y procedimientos de registro seguro (numeral 9.4.2). Estos refieren a medidas de seguridad para el acceso, registro, etc. de usuarios a los sistemas, lo que se encuentra en línea con las normas indicadas precedentemente (art. 10 de la Ley Nº 18.331 y art. 7 del decreto Nº 414/009).

f) Criptografía (cláusula 10).

Las guías específicas refieren a la política en el uso de registros criptográficos (numeral 10.1.1), con especial énfasis en los datos protegidos. Merece idénticos comentarios que el numeral anterior.

g) Seguridad física y de medio ambiente (cláusula 11).

Es interesante la referencia realizada en el numeral 11.2.7 vinculado al descarte o reutilización segura de equipos, en tanto señala que si existe la posibilidad de que el equipo contenga PII, el mismo debe ser tratado como si efectivamente la contuviera. Si bien no existe una norma específica en este sentido, se entienden aplicables los conceptos mencionados en el numeral anterior.

h) Seguridad de operaciones (cláusula 12).

Se establecen guías específicas en los puntos de Respaldo de información (numeral 12.3.1), de Registro de accesos (numeral 12.4.1) y de protección de información de accesos (numeral 12.4.2). Merece especial atención el numeral 12.3.1 por cuando indica que debería crearse múltiples copias en distintas ubicaciones para propósito de recuperación o respaldo, aclarando que la responsabilidad es del consumidor de los servicios de nube, por lo que es importante brindarle información clara. No existe en nuestro país una norma que imponga una frecuencia o procedimiento específico para el respaldo de la información.

Son aplicables a las empresas subcontratadas que respalden información las mismas normas que para los proveedores de servicios de cloud referidos.

i) Seguridad de las comunicaciones (cláusula 13).

El punto 13.2.1 establece guías particulares para políticas y procedimientos de transferencia de información. Ya se ha hecho referencia a las normas vinculadas a la seguridad de los datos, aplicables en el caso.

j) Adquisición, desarrollo y mantenimiento de sistemas (cláusula 14).

Se aplican las disposiciones de la ISO/IEC 27.002.

k) Relaciones con proveedores (cláusula 15).

Se aplican las disposiciones de la ISO/IEC 27.002.

l) Gestión de incidentes de seguridad de la información (cláusula 16).

En el punto vinculado a la gestión de los incidentes de seguridad de la información y mejoras (16.1) se establece la conveniencia de una tarea de cooperación entre el proveedor del servicio de nube y el consumidor para la implementación de los controles previstos.

En lo que respecta al punto de responsabilidades y procedimientos (punto 16.1.1) se indica especialmente que los incidentes de seguridad debería de generar una revisión por el encargado de tratamiento de la PII, a diferencia de la ocurrencia de un evento de seguridad. Podemos trazar en este punto un paralelismo con las disposiciones del decreto Nº 451/009 precitado, que distingue un caso del otro e impone a los organismos públicos la obligación de denunciar ante el Centro Nacional de Respuesta a Incidentes de Seguridad Informática (Cert-uy) la ocurrencia de los primeros (Art. 8º lit a).

m) Aspectos de seguridad de la información de gestión continuada de negocios (cláusula 17).

Se aplican las disposiciones de la ISO/IEC 27.002.

n) Adecuación (cláusula 18).

Merece especial mención el punto relativo a revisiones independientes de seguridad de la información (numeral 18.2.1), que marca como deseable una auditoría independiente de las operaciones de tratamiento a fin de brindar transparencia, sin perjuicio de lo cual no merece puntualizaciones de orden jurídico.

2.5.- Finalmente, el **Anexo A desarrolla un conjunto de controles específicamente diseñados para la protección de la PII en el caso de tratamiento de la misma por un proveedor de servicios de nube.** Estos controles adicionales se vinculan a los 11 principios de privacidad regulados en la ISO 29100, a saber: Consentimiento y opción; Legitimidad de propósito y especificación; Limitación en la recolección; Minimización de datos; Limitación de uso, retención y revelación; Certeza y calidad; Apertura, transparencia y noticia; Participación individual y acceso; Rendición de cuentas; Seguridad de Información; Adecuación a la privacidad.

Los principios regulados en la normativa uruguaya, y que se encuentran consagrados específicamente en la Ley Nº 18.331 son: legalidad, veracidad, finalidad, previo consentimiento informado, seguridad de los datos, reserva y responsabilidad (art. 5º), desarrollados posteriormente en los artículos 6 a 12 de la citada norma.

Se analizarán los principios reseñados en la norma ISO/IEC conjuntamente con las normas nacionales en la materia.

a) Consentimiento y opción.

Conforme la ISO/IEC el encargado de tratamiento debería proveer a su cliente los medios para posibilitar el cumplimiento de la obligación de facilitar el ejercicio de los principales derechos vinculados a la protección de datos. De esta manera, las obligaciones del responsable deberían de estar definidas en la ley, regulación y contratos y pueden incluir materias en las que éste debe emplear algunos servicios del proveedor.

Los derechos señalados en la ISO/IEC se encuentran claramente establecidos en los artículos 14 y 15 de la Ley Nº 18.331 y en los artículos 10 a 14 del decreto N° 414/009. Estos artículos señalan los mecanismos para ejercer los derechos referidos, indicando además la forma en que deberá de procederse por parte de los responsables de la información.

En particular el artículo 9 del decreto Nº 414/009 indica que el ejercicio de los derechos se realizará: por el titular o su representante, en forma conjunta o independiente, exento de formalidades y en forma gratuita, mediante comunicación dirigida al responsable de la base de datos o tratamiento con identificación del titular, motivo de la solicitud, domicilio real y constituido, fecha y firma y documentación acreditante de la solicitud. Asimismo, el responsable deberá contestar en un plazo de 5 días hábiles desde la presentación y deberá proporcionar la información en forma legible e inteligible.

Vemos entonces que a fin de facilitar el ejercicio de los derechos deberá tenerse presente los parámetros brindados por la reglamentación nacional.

b) Legitimidad del propósito y especificación.

El fin del tratamiento debería de ajustarse a las instrucciones del cliente de los servicios de nube. Estas instrucciones deberían estar contenidas en el contrato entre el cliente y el proveedor.

Deberá además en este punto respetarse lo establecido en el principio de finalidad consagrado en el artículo 8 de la Ley Nº 18.331 (*Los datos objeto de tratamiento no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención. Los datos deberán ser eliminados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubieren sido recolectados. La reglamentación determinará los casos y procedimientos en los que, por excepción, y atendidos los valores históricos, estadísticos o científicos, y de acuerdo con la legislación específica, se conserven datos personales aun cuando haya perimido tal necesidad o*

pertinencia. Tampoco podrán comunicarse datos entre bases de datos, sin que medie ley o previo consentimiento informado del titular).

En este punto la ISO/IEC hace también referencia al uso de la PII por parte del proveedor del servicio de nube con fines de marketing y publicidad, el que sólo se prevé con consentimiento expreso del titular.

En el caso de la norma uruguaya, la Ley Nº 18.331 en su artículo 21 establece: *"Datos relativos a bases de datos con fines de publicidad.- En la recopilación de domicilios, reparto de documentos, publicidad, venta u otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo,* ***cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento.*** *En los supuestos contemplados en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno. El titular podrá en cualquier momento solicitar el retiro o bloqueo de sus datos de los bancos de datos a los que se refiere el presente artículo."*

En consecuencia, la norma uruguaya prevé otras hipótesis en las cuales es posible tratar datos personales con fines publicitarios que no se limitan a la obtención del consentimiento previo, atento a que se trataría de datos que fueron proporcionados directamente por los titulares o accesibles a través de documentos públicos.

c) Limitación de recolección.

Si bien la norma ISO/IEC no plantea controles adicionales de relevancia en este principio, sí es dable recordar que conforme al principio de veracidad consagrado en el artículo 7º de la Ley Nº 18.331 "*Los datos personales que se recogieren a los efectos de su tratamiento deberán ser veraces, adecuados, ecuánimes* ***y no excesivos en relación con la finalidad para la cual se hubieren obtenido***".

d) Minimización de datos.

La norma ISO/IEC indica que los archivos temporales y documentos deben eliminarse luego de un período específico y documentado de tiempo. Recomiendan para ello que los sistemas de tratamiento de la PII implementen controles periódicos para eliminar los archivos temporales que no se usen luego de un período especificado de tiempo.

En este punto cabe mencionar que la recomendación se ajusta a lo dispuesto por el artículo 8º inciso segundo de la Ley Nº 18.331 qué, consagrando el principio de finalidad, establece en concreto: "***Los datos deberán ser eliminados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubieren sido recolectados***". Si bien no se trata en el caso de datos "recolectados" sino generados por los sistemas de tratamiento de los mismos, en principio se entiende aplicable la citada recomendación de la ISO/IEC por analogía con lo dispuesto por el artículo mencionado.

e) Limitación de uso, retención y revelación.

En este punto la ISO/IEC señala que el contrato entre el proveedor de servicios y el consumidor de los mismos debería requerir que el primero notifique al segundo de cualquier solicitud legítima para revelar PII por parte de una autoridad de control, salvo que dicha revelación se encuentre prohibida. Recomienda en este caso que se brinden las garantías contractuales necesarias para rechazar cualquier solicitud de revelación que no sean legalmente obligatorias y que se consultará al consumidor del servicio de nube antes de realizar tal revelación de información.

Resulta de indudable aplicabilidad el Principio de Reserva consagrado en el artículo 11 de la Ley Nº 18.331 ya referenciado en el apartado 2.4.c, al analizar la cláusula 7 de la Norma.

Es importante señalar además, que la Ley Nº 18.331 en su artículo 17 hace referencia a la comunicación de datos en los siguientes términos: "*Los datos personales objeto de tratamiento sólo podrán ser comunicados para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo.*

El previo consentimiento para la comunicación es revocable.

El previo consentimiento no será necesario cuando:

A) Así lo disponga una ley de interés general.

B) En los supuestos del artículo 9º de la presente ley.

C) Se trate de datos personales relativos a la salud y sea necesario por razones de salud e higiene públicas, 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.

D) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos no sean identificables.

El destinatario quedará sujeto a las mismas obligaciones legales y reglamentarias del emisor y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate".

El artículo 9º del mismo cuerpo normativo a su vez establece la innecesariedad de ese previo consentimiento en los siguientes casos:

"A) Los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación.

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 en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento. En el caso de personas jurídicas, razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma.

D) Deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento.

E) Se realice por personas físicas o jurídicas, privadas o públicas, para su uso exclusivo personal o doméstico."

En consecuencia, y en todos los casos, deberá darse estricto cumplimiento a lo citado en la normativa precedente, más allá de cualquier pacto contractual que realicen las partes.

La ISO/IEC también señala la importancia de mantener registros de las revelaciones de información realizadas por el proveedor de servicios de nube -incluyendo la información, el destinatario de la misma, y en qué momento se reveló-, lo que parece una buena práctica.

f) Certeza y calidad.

Tampoco en este punto la ISO/IEC se pronuncia por controles adicionales relevantes en la materia, más allá de los referidos en la ISO/IEC 27.002 y 29.100.

g) Apertura, transparencia y noticia.

La ISO/IEC refiere al caso de subcontratistas del proveedor de servicios de nube para el tratamiento de la PII, señalando que en todos los casos debería informarse tal situación al consumidor de los servicios, todo lo cual debería quedar reflejado en el contrato oportunamente suscrito entre las partes. Igualmente deberán informarse en forma previa los cambios. Debería de informarse según la recomendación no sólo el uso de subcontratistas sino su identificación, los lugares donde se están tratando los datos y los medios que se emplearán por estos para cumplir con las obligaciones del encargado de tratamiento original. Recomiendan además que la información del subcontratista se revele al consumidor mediante acuerdos de confidencialidad.

Parece oportuno recordar que conforme las normas ya vistas existe responsabilidad de todos aquellos que realicen tratamiento de datos personales, ya sea en forma directa o indirecta a través de la subcontratación.

h) Participación individual y acceso.

No se prevén por la ISO/IEC controles adicionales a la ISO/IEC 27.002 en la materia.

i) Rendición de cuentas.

El punto tratado por la ISO/IEC hace referencia expresa a la notificación de incidentes de seguridad que involucren PII, a períodos de retención por políticas y lineamientos de seguridad administrativos, y a la devolución, comunicación y eliminación de PII.

En el primero de los mencionados la ISO/IEC refiere a la importancia de notificar al consumidor cualquier acceso no autorizado a PII o a los equipos de tratamiento que puedan generar una pérdida, revelación o alteración de la PII. Para ello se sugiere que se incluyan en los contratos estas notificaciones, especificando la información que el proveedor de servicios debe brindar al consumidor para que este último, en su calidad de responsable, cumpla con la obligación legal de informar, así como otros elementos vinculados al plazo para comunicar, etc. También se sugiere mantener un registro de estos eventos.

Conforme el artículo 8º del decreto Nº 414/009 ya mencionado, existe una obligación directa del encargado de tratamiento de comunicar este tipo de incidentes a los interesados. También resulta aplicable al tema arriba mencionado en el punto 2.4. Literal l) para los organismos públicos.

En lo que respecta al período de retención para políticas y lineamientos de seguridad administrativos no existen normas específicas que prevean la conservación específicas de las políticas y lineamientos de seguridad, siendo razonable, ante la existencia de las responsabilidades atribuibles a los encargados de tratamiento antes mencionadas, que las mismas se conserven, en consonancia con lo indicado por la recomendación.

Finalmente, en lo que refiere a la devolución, comunicación o eliminación de la PII, la ISO/IEC hace referencia a la necesidad de que los proveedores de servicios de nube informen debidamente a sus consumidores los mecanismos para el borrado de los datos.

Ya se ha hecho mención al artículo 8º inciso segundo, que se entiende aplicable al caso concreto, correspondiendo además por la temática que se trata hacer referencia al artículo 30 de la misma norma, que impone la necesidad de destruir los datos tratados, una vez cumplida la prestación contractual -salvo 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.

j) Seguridad de la información.

En este punto existen varias sugerencias en varios ámbitos, tales como: acuerdos de confidencialidad y no revelación; restricción a la creación de material impreso; control y acceso a restauración de datos; protección de datos en contenedores que dejan las premisas; uso de contenedores y dispositivos no encriptados; encriptación de PII transmitida en redes públicas; eliminación segura de materiales impresos; uso único de contraseñas de usuarios; registro de usuarios autorizados; gestión de contraseña de usuarios; medidas contractuales; subcontratación de tratamiento de PII; y acceso a datos en espacio de almacenamiento pre-utilizado.

Todos estos puntos regulan distintos aspectos vinculados a la seguridad de la información, y a la necesidad de encriptar ya sea los dispositivos que contienen información como aquella información que se comunica, al igual que un control importante sobre la gestión de los usuarios y sus contraseñas, al igual que los mecanismos para asegurar la efectiva destrucción de la información y las medidas para asegurar el cumplimiento de las obligaciones tanto del encargado de tratamiento como del responsable en el tratamiento de los datos personales.

Se reitera en este punto los artículos 10º de la Ley Nº 18.331, 7 y 8 del decreto Nº 414/009 y el Anexo III del decreto Nº 92/014 en materia de organismos públicos.

k) Adecuación a la privacidad.

Este principio hace referencia a la ubicación geográfica de la PII y al destino de la misma.

Según la recomendación, la identificación de los países donde se guardará la PII debería de hacerse disponible al consumidor, tanto sea respecto del proveedor de servicios de nube encargado de tratamiento como de los subcontratistas. Deberían además de identificarse contractualmente los casos de transferencias internacionales, así como los potenciales cambios en las condiciones que procure realizar el proveedor de los servicios de nube.

Cabe aclarar en este punto nuevamente que el uso de servicios de nube por parte de los organismos públicos se encuentra definido en el decreto Nº 92/014 que en su artículo 3º impone para la Administración Central la obligación de alojar sus sistemas informáticos en centros de datos seguros situados en territorio nacional, exceptuándose aquéllos que no constituyan un riesgo para el organismo, de acuerdo con los “Lineamientos para la implementación y uso de centros de datos seguros” (Anexo III).

Asimismo, y en caso de servicios de nube provistos fuera del territorio nacional corresponde para los restantes obligados la aplicación del artículo 23 de la Ley 18.331 de transferencia internacional de datos. Dicho artículo 23 establece: Se prohíbe la transferencia de datos personales de cualquier tipo con países u organismos internacionales que no proporcionen niveles de protección adecuados de acuerdo a los estándares del Derecho Internacional o Regional en la materia.

"La prohibición no regirá cuando se trate de:

1) *Cooperación judicial internacional, de acuerdo al respectivo instrumento internacional, ya sea Tratado o Convención, atendidas las circunstancias del caso.*

2) *Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado por razones de salud o higiene públicas.*

3) *Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable.*

4) *Acuerdos en el marco de tratados internacionales en los cuales la República*

Oriental del Uruguay sea parte.

5) *Cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.*

También será posible realizar la transferencia internacional de datos en los siguientes supuestos:

A) *Que el interesado haya dado su consentimiento inequívocamente a la transferencia prevista.*

B) *Que la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado.*

C) *Que la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero.*

D) *Que la transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.*

E) *Que la transferencia sea necesaria para la salvaguardia del interés vital del interesado.*

F) *Que la transferencia tenga lugar desde un registro que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para su consulta.*

Sin perjuicio de lo dispuesto en el primer inciso de este artículo, la Unidad Reguladora y de Control de Protección de Datos Personales podrá autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel adecuado de protección, cuando el responsable del tratamiento ofrezca garantías suficientes respecto a la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos.

Dichas garantías podrán derivarse de cláusulas contractuales apropiadas".

Los artículos 33 y 34 del decreto Nº 414/009 establecen el procedimiento para las citadas transferencias.

Resulta de importancia señalar que el dictamen Nº 8/2014 de 23 de Julio de 2014 del Consejo de la URCDP marca la opinión de la unidad con respecto al uso de servicios en modalidad SaaS (Software as a Service) de proveedores en la nube, en un servidor ubicado fuera del país, señalando en definitiva que la situación se enmarca en los artículos 3 de la Ley Nº 18.331 y 3 literales A y B del decreto Nº 414/009. Es importante destacar que en el caso esa utilización de servicios se enmarca en una transferencia internacional de datos, siendo aplicables los artículos arriba referidos, circunstancia que debe ser tenida en cuenta por cualquier consumidor de servicios de nube.[6]

De acuerdo a lo expresado entonces, la transferencia internacional de datos debe realizarse a países con un nivel adecuado de protección en la materia. A la hora de almacenar datos en la nube se debe considerar en primer lugar el país de ubicación para determinar así su nivel de protección. De acuerdo a la Resolución N° 17 de 12 de junio de 2009 de la URCDP, se consideran países con normas de protección adecuadas y medios para asegurar la tutela de los datos aquellos que sean miembros de la Unión Europea y aquellos que la Comisión Europea considere garantizan lo antes dicho. En ese marco, la Comisión ha entendido en la Decisión 200/520/CE de 26 de Julio de 2000 que ofrecen garantías adecuadas las entidades estadounidenses adheridas a los principios de Puerto Seguro o Safe Harbor (la lista de entidades adheridas a los principios está disponible en http://www.export.gov/safeharbor).

3.- Conclusiones.

La cuestión de la provisión de servicios en la nube ya ha sido referida por la URCDP a través del Dictamen 8/2014 -ya reseñado-, enmarcándola dentro del concepto de transferencia internacional de datos, en caso en que los servidores de los proveedores se encuentren fuera del país.

---

[6] *Se transcribe el dictamen señalado: "1.- Indicar que en la situación planteada en la consulta formulada por xxxxxxxxxxxxxxx en estos obrados existe transferencia internacional de datos en el sentido de lo establecido en la Ley 18.331 y su decreto reglamentario 414/009, en especial su art. 4° Literal H).*

2.- Hacer saber que en virtud de la legislación citada en el numeral anterior, tanto el servicio como los respaldos, deberán ubicarse en países adecuados en materia de protección de datos personales.

3.- Notifíquese, publíquese y oportunamente archívese".

La ISO/IEC 27.018 contiene una serie de buenas prácticas a efectos de que los proveedores de servicios de nube que realizan tratamiento de datos cuenten con un conjunto de requerimientos mínimos a fin de facilitar el cumplimiento de la normativa de protección de datos por los responsables que se constituyen en sus clientes.

Aún en ese caso, es importante señalar que el cumplimiento de las prácticas reseñadas no importa necesariamente la adecuación a la normativa nacional en materia de protección de datos. En consecuencia es fundamental que antes de contratar cualquier servicio por parte de los responsables con un proveedor de servicio en la nube, aun cuando éste cumpla con la ISO en análisis, se tenga confirmación de que el responsable podrá cumplir con la normativa uruguaya en la materia.

Anexo I (Definiciones)

ISO/IEC 27.018:2014	REGULACIÓN NACIONAL
Data breach: Cualquier compromiso a la seguridad que derive en una destrucción, pérdida, alteración, revelación no autorizada o acceso -accidental o no- a los datos transmitidos, guardados o procesados.	**Incidente de Seguridad Informática:** es una violación o una amenaza inminente de violación a una política de seguridad de la información implícita o explícita, así como un hecho que comprometa la seguridad de un sistema (confidencialidad, integridad o disponibilidad) (Art. 3 literal d) del decreto Nº 451/009 de 28 de setiembre de 2009). **Principio de seguridad de los datos:** El responsable o usuario de la base de datos debe adoptar las medidas que resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales. Dichas medidas tendrán por objeto evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. Los datos deberán ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular. Queda prohibido registrar datos personales en bases de datos que no reúnan condiciones técnicas de integridad y seguridad (Artículo 10 Ley Nº 18.331). **Vulneración de seguridad:** Cuando el responsable o encargado de la base de datos o tratamiento conozca de la ocurrencia de vulneraciones de seguridad en cualquier fase del tratamiento que realice, que sean susceptibles de afectar de forma significativa los derechos de los interesados, deberán informarles de este extremo (Artículo 8 Decreto Nº 414/009).
personally identifiable information (PII): Cualquier información que: i) se pueda utilizar para identificar a la persona	**Dato personal:** información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables (Artículo 4

a la que refiere dicha información ; ii) esté o pueda estar directa o indirectamente vinculada al persona a la que refiere la misma.	literal D de la Ley Nº 18.331).
PII controller: Es el interesado que determina los propósitos y medios para el procesamiento de PII, excepto personas físicas que utilicen los datos con fines domésticos.	**Responsable de la base de datos o del tratamiento:** persona física o jurídica, pública o privada, propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento (Artículo 4 literal K de la Ley Nº 18.331). **Creación, modificación o supresión.-** Las personas físicas o jurídicas privadas que creen, modifiquen o supriman bases de datos de carácter personal, que no sean para un uso exclusivamente individual o doméstico, deberán registrarse conforme lo previsto en el artículo siguiente (Artículo 28 de la Ley Nº 18.331).
PII principal: Persona física a la cual refieren la PII.	**Titular de los datos:** persona cuyos datos sean objeto de un tratamiento incluido dentro del ámbito de acción de la presente ley (Artículo 4 literal L de la Ley Nº 18.331).
PII processor: Aquellos interesados que procesan PII en nombre y con instrucciones de un PII controller.	**Encargado del tratamiento:** persona física o jurídica, pública o privada, que sola o en conjunto con otros trate datos personales por cuenta del responsable de la base de datos o del tratamiento (Artículo 4 literal H de la Ley Nº 18.331)
processing of PII: operación o conjunto de operaciones realizadas sobre PII.	**Tratamiento de datos:** operaciones y procedimientos sistemáticos, de carácter automatizado o no, que permitan el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias (Artículo 4 literal M de la Ley Nº 18.331).
public cloud service provider: Parte que hace disponibles servicios de nube según el modelo de nube pública.	N/D