Un Río y Dos Orillas en Protección de Datos Personales

Protección de datos personales y la familia de normas ISO 27.000

Por: Oscar Giudice, TecnoIntegración

http://oscargiudice.wordpress.com/category/datos-personales/

Primera Parte

El día 14 de diciembre de 2009 venció el plazo para realizar el registro de las bases de datos que contengan datos personales. El registro debe realizarse en la URCDP, Unidad Reguladora y de Control de Datos Personales. La puesta en vigencia de la Ley y el organismo de regulación pertinente son un paso fundamental en la protección de los datos de las personas y en el derecho a la intimidad. Esta Ley permite a Uruguay ser considerado "país seguro" (en cuanto al tratamiento de datos personales) dentro de la CE y en algunos países de América Latina, que ya cuentan con este tipo de normativa, como la Rep. Argentina.

La inscripción de las bases es sólo una parte de la obligación, para que éstas se encuentren inscriptas debidamente se debe adecuar métodos, procedimientos y sistemas a lo solicitado por la Ley, entre otras cosas "***Asegurar la Información***"

En cuanto a seguridad se refiere el texto del decreto 414/009 dice:

"Artículo 7º.- Medidas de seguridad. Tanto el responsable como el encargado de la base de datos o tratamiento deberán proteger los datos personales que sometan a tratamiento, mediante aquellas medidas técnicas y organizativas que resulten idóneas para garantizar su integridad, confidencialidad y disponibilidad."

Vemos que la Ley nos habla de:

Medidas técnicas y organizativas que resulten idóneas para garantizar integridad, confidencialidad y disponibilidad.

El significado de esto según la norma UNIT-ISO/IEC 27000:2009 (tecnología de la información – visión general y vocabulario) es:

Integridad [2.25]**: "*es la Propiedad de salvaguardar la exactitud y completitud de los activos*"**.

En otras palabras: La información es íntegra cuando es completa, precisa y se encuentra protegida contra modificaciones no autorizadas.

Confidencialidad [2.25]**:"*es la Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados*"**

En otras palabras: La información sólo puede ser accedida por aquellas personas que están debidamente autorizadas y para lo cual están autorizadas.

Disponibilidad[2.7]**: *es la "Propiedad de ser accesible y utilizable por solicitud de una entidad autorizada"***.

En otras palabras: Que la información esté disponible y utilizable cuando sea lo requiera.

Nota: *Los números entre paréntesis son las referencias UNIT-ISO/IEC 27000:2009*

Hasta aquí todo parece bastante claro, pero *¿Qué nos quieren decir con Medidas técnicas y organizativas que resulten idóneas?*

El término "idóneo", si de seguridad hablamos, me parece un poco vago e impreciso y en lo que a seguridad de la información se refiere no nos podemos permitir vaguedades e imprecisiones, mucho más si nos vamos a referir a datos personales, y en particular a aquellos que se consideran datos sensibles o especialmente protegidos, esto son:

Datos sensibles o especialmente protegidos

"los datos personales que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual".

Una manera de salir de la imprecisión es la adoptar un estándar o norma reconocida internacionalmente, en este caso y por lo que puede averiguar asistiendo a distintas charlas y conferencias la propuesta es: la familia de normas UNIT-ISO/IEC 27000, en particular la ISO 27002 – "Código de buenas prácticas para la gestión de la seguridad de la información"

Qué nos provee esta familia de normas:

ISO 27002 es el nuevo nombre de ISO 17799:2005 (año de edición). Está *es una guía de buenas prácticas que describe: objetivos de control (39 objetivos), controles recomendables (133 controles), éstos se encuentran agrupados en 11 dominios*, siendo estos:

- Política de seguridad
- Aspectos organizativos para la seguridad
- Clasificación y control de activos
- Seguridad ligada al personal
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de accesos
- Desarrollo y mantenimiento de sistemas
- Gestión de incidentes de seguridad de la información
- Gestión de continuidad de negocio
- Conformidad

Dentro de cada dominio o sección, se especifican los objetivos de los distintos controles y para cada uno de éstos controles se indica una guía para su implantación, dentro de sus alcances leemos:

"Este Estándar Internacional establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos delineados en este Estándar Internacional proporcionan un

lineamiento general sobre los objetivos de gestión de seguridad de la información generalmente aceptados.

Los objetivos de control y los controles de este Estándar Internacional son diseñados para ser implementados para satisfacer los requerimientos identificados por una evaluación del riesgo.

*Este Estándar Internacional puede servir como un lineamiento práctico para desarrollar estándares de seguridad organizacional y prácticas de gestión de seguridad efectivas y para ayudar a elaborar la confianza en las actividades inter-organizacionales". **

Nota: *cita textual de la Norma.*

Es importante tener en cuenta que cada el estándar habla de "lineamientos y principios generales" por lo cual queda en manos de cada organización considerar previamente cuantos y que controles serán realmente los aplicables según sus propias necesidades, posibilidades y objetivos.

En una próxima entrega nos adentraremos en los controles que son aplicables a las bases de datos de carácter personal.

Segunda Parte

En la primer parte de esta serie de notas sobre la familia de normas ISO 27.000 y las leyes de protección de datos me referí, en particular, a la Ley Uruguaya de PDP (Protección de Datos Personales) 18.331 y el decreto 414-009.

Poco tiempo después de posteada esa nota la AGESIC [(1)] desarrolla y publica las "Directrices para la aplicación de la Ley 18.331" esta recomendación o guía de buenas prácticas se encuentra basada en la familia de normas UNIT-ISO/IEC 27.000 en particular en la 27.002. Cabe aclarar que esto no es merito personal alguno, nada tuve que ver en ello. Lo que si tuve fue la visión de cuál era el camino adecuado, al menos según mi criterio y pareciera que el de AGESIC también.

Distinto es el caso de Argentina, país donde nací. La Ley de protección de datos personales, Ley 25.326, se sanciono (octubre de 2000) esto es bastante tiempo antes que la Ley Uruguaya homóloga se sancionase. En Argentina 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" fueron establecidas por la DNPDP [(2)] mediante la Disposición 11/2006 (Publicación en B.O.: 22/9/2006). Estas medidas se estructuran en tres categorías según la clasificación de los datos que se almacene, medidas de seguridad de nivel: básico (personales en gral.), medio (ej. Datos bancarios) y alto (datos sensibles). Esta clasificación es similar a la LOPD [(3)] de la AEPD [(4)].

A mi parecer a las medidas de seguridad emitidas por el órgano de control Argentino les falta la referencia o marco de un estándar internacional como son los ISO. Si bien muchos de los puntos exigidos por la DNPDP en las medidas de seguridad se encuentran detallados en la ISO 27.002 en ningún documento se hace mención a esta. Resulta rara esta situación cuando en distintos documentos del ArCERT [(5)] y del ONTI [(6)] se mencionan a las normas de la familia IRAM/ISO 27.000 o su antecesora la IRAM/ISO 17.799.

Más allá de todo esto y, a modo de ejemplo, veamos un caso práctico de aplicación de la noma ISO 27.002 para el cumplimiento de las leyes de protección de datos personales. Voy a tomar para este ejemplo el ***principio de legalidad o licitud*** aplicado a una base de datos de carácter personal.

La Ley argentina 25.326 en su artículo 3ro. Habla sobre la licitud de de los archivos de datos, y dice textualmente:

> *"La formación de archivos de datos será lícita cuando se encuentren debidamente inscriptos, observando en su operación los principios que establece la presente ley y las reglamentaciones que se dicten en su consecuencia."*

Mientras tanto la Ley Uruguaya 18.331 dice textualmente en su artículo 6to:

> *"La formación de bases de datos será lícita cuando se encuentren debidamente inscriptas, observando en su operación los principios que establecen la presente ley y las reglamentaciones que se dicten en consecuencia."*

Pero… ¿Qué nos quieren decir con esto y que controles de la norma ISO 27.002 podemos aplicar?

a) Que una base de datos de carácter personal no será "legal" o "licita" si no se encentra inscripta en el registro pertinente, DNPDP para Argentina, URCDP [7] para Uruguay.

b) Que a su vez se deben cumplir los principios que establecen estas leyes, esto son: ***Legalidad, veracidad, finalidad, previo consentimiento informado, seguridad de los datos, reserva, responsabilidad.***

c) Luego habla de "y ***las reglamentaciones que se dicten en su consecuencia***" esto significa que debemos estar atentos a las modificaciones o nuevas exigencias que puedan surgir respecto de la protección de datos personales, en el país que corresponda.

Hasta aquí la descripción del principio de legalidad. Si bien el presente artículo no pretende ser de estudio sobre temas legales, es imprescindible conocer y comprender la Ley para poder aplicar las normas ISO como herramienta para el cumplimiento ésta; así que ahora continúo con la ISO 27.002 y para trabajar con ella tomaremos como ejemplo el punto "a" , solo con éste tenemos bastante en que ocuparnos.

Por lo expuesto más arriba en "a" tenemos ubicar e identificar dentro de la organización todas las bases de datos, para ello tendremos que realizar un ***inventario de activos de la información*** este inventario se encuentra contemplado en la ISO 27.002 mediante el control 7.1.1, el cual dice:

> ***7.1.1 Inventario de los activos***
> *"Se debieran identificar todos los activos y se debiera elaborar y mantener un inventario de todos los activos importantes."*

Pero sucede que no todas las bases de datos contienen datos personales, es decir muchas de estas no nos interesará registrar, por lo cual deberíamos ***clasificar los activos inventariados***, para esto nos podemos valer del control 7.2:

7.2 Clasificación de la información
"Se debiera clasificar la información en términos de su valor, requerimientos legales, sensibilidad y grado crítico para la organización."

Aquí témenos ya dos grandes tareas: realizar el inventario y clasificar la información inventariada. Leyendo un poco más en profundidad veremos que el punto 7.1.1. de la ISO 27.002 dice **mantener un inventario**, esto no nos está diciendo que ese inventario debe estar actualizado, debe mantenerse al día, en otras palabras: nuestro inventarió deberá reflejar los cambios que puedan ocurrir en las bases ya inventariadas además de incluir las que puedan aparecer.

Tanto en Uruguay como en Argentina ésta es una tarea sumamente importante aún luego de registrada la base. En Uruguay la Ley 18.331 obliga a comunicar, en caso de producirse variaciones en la base de datos, los cabios en forma trimestral a la Unidad Reguladora. Ejemplo de cambios son: creación o supresión de campos, aumento o disminución de la cantidad de personas físicas o jurídicas registradas en más de un 20%, cambio de las medidas de seguridad, cambio de destinatarios de los datos, cambio de ubicación de los servidores, cambio de terceros a los cuales se le envían datos u otros cambios. En Argentina las cosas son un poco distintas. Existe la obligación de renovar la inscripción, anualmente, es en ese momento que se notifican los cambios a la Dirección Nacional de PDP.

Vimos hasta aquí la importancia de realizar un inventario de las bases de datos que contengan datos personales y el porqué mantener actualizado ese inventario. Esta tarea no es más, ni menos, que una revisión periódica. La misma revisión periódica que las buenas prácticas instauradas en la norma ISO 27.002 nos recomienda realizar.

Hasta aquí hemos tomado como referencia la Ley y buscamos dentro de la norma los puntos de control que nos podrían ayudar con ésta. Hagamos ahora al revés, tomemos la cláusula o dominio "k" de la ISO 27.002, es el dominio que nos habla sobre el cumplimiento y conformidad, y en parte nos dice:

15.1 Cumplimiento de los requisitos legales
"Objetivo: *Evitar los incumplimientos de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requisito de seguridad.*
El diseño, operación, uso y gestión de los sistemas de información pueden estar sujetos a Requisitos de seguridad estatutarios, reguladores y contractuales.", y sigue….

Por lo expresado en el punto 15.1. de la norma ISO 27.002 esta nos insta a identificar las normas y la legislación que puedan ser aplicables a nustros sistemas de información. Aquí se abre otro mundo, vamos a encontrar normas y leyes que son de aplicación horizontal (delito informático, propiedad intelectual, etc.) y otras que son de aplicación vertical (protección de datos personales, historia clinica electrónica, comunicaciones de los bancos centrales o de las instituciones de regulación finaciera y monetaria, etc.)

Aquí nuevamente vuelve a aparecer la necesidad de revisar periódicamente al grado de cumplimiento, pues día a día aparecen nuevas, nomas, disposiciones, leyes, etc. Que quizás deban cumplir nuestras instalaciones, sistemas y archivos.

[i] ***Agradecimientos:***

Agradezco la colaboración del Dr. Gustavo Tanús (Argentina) y del Dr. Martín Pesce (Uruguay) dos abogados amigos que permanentemente me ayudan con su saber jurídico.

[ii] ***Referencias:***

1. AGESIC, Uruguay: Agencia de Gobierno Electrónico y Sociedad de la Información.
2. DNPDP, Argentina: Dirección de Protección de Datos Personales
3. LOPD, España: Ley Orgánica de Protección de Datos de Carácter Personal (Ley Orgánica 15/1999, de 13 de diciembre)
4. AEPD, España: Agencia Española de Protección de Datos (Real Decreto 428/1993, de 26 de marzo)
5. ArCERT, Argentina: Coordinación de Emergencia en Redes Teleinformáticas, Subsecretaría de la Gestión Pública.
6. ONTI, Argentina: Oficina Nacional de Tecnologías de Información, Subsecretaría de la Gestión Pública.
7. URCDP, Uruguay: Unidad Reguladora y de Control de Datos Personales.