GESTION ESTRATEGICA DE LA SEGURIDAD INFORMATICA II. Maestría en Seguridad Informática, Ciudad Autónoma de Buenos Aires, 2011.

PROTECCIÓN DE DATOS PERSONALES EN SUDAMÉRICA: UN ANÁLISIS DEL ESTADO ACTUAL EN ARGENTINA Y COLOMBIA.

Diego Sebastian Escobar, MARROQUÍN, KARIN, Jacobo Zambrano Barón, Germán Villota Narváez y VIRREIRA, FLAVIA.

Cita:

Diego Sebastian Escobar, MARROQUÍN, KARIN, Jacobo Zambrano Barón, Germán Villota Narváez y VIRREIRA, FLAVIA (Julio, 2011). *PROTECCIÓN DE DATOS PERSONALES EN SUDAMÉRICA: UN ANÁLISIS DEL ESTADO ACTUAL EN ARGENTINA Y COLOMBIA. GESTION ESTRATEGICA DE LA SEGURIDAD INFORMATICA II. Maestría en Seguridad Informática, Ciudad Autónoma de Buenos Aires.*

Dirección estable: https://www.aacademica.org/escobards/10

ARK: https://n2t.net/ark:/13683/ptuD/Phw

UNIVERSIDAD DE BUENOS AIRES
FACULTADES DE CIENCIAS ECONÓMICAS,
CIENCIAS EXACTAS Y NATURALES E INGENIERÍA

MAESTRÍA EN SEGURIDAD INFORMÁTICA

GESTION ESTRATEGICA DE LA SEGURIDAD INFORMATICA II

PROTECCIÓN DE DATOS PERSONALES EN SUDAMÉRICA:

UN ANÁLISIS DEL ESTADO ACTUAL EN ARGENTINA Y COLOMBIA.

INTEGRANTES:

ESCOBAR, DIEGO SEBASTIÁN

MARROQUÍN, KARIN

VILLOTA, GERMÁN

VIRREIRA, FLAVIA

ZAMBRANO, JACOBO

2011

1. Resumen

A lo largo del presente documento se presenta la estructura y características de la ley de protección de datos personales implementada en la República Argentina y del proyecto de ley que está en proceso de aprobación en Colombia, con el fin de profundizar sobre los conceptos de cumplimiento de leyes y regulaciones, y establecer la relación práctica de estas con lo especificado por la familia de normas ISO27000.

Inicialmente se describen los antecedentes, estructura y características de las leyes objeto del análisis, para posteriormente establecer criterios que permitan realizar una comparación entre las mismas.

Finalmente se describen otros niveles de cumplimiento de nivel internacional, y se presenta la relación con las normas ISO anteriormente mencionadas.

Palabras claves.

Cumplimiento, Leyes, Datos Personales.

2. Introducción

“Datos Personales: El nuevo petróleo de la internet y la nueva moneda del mundo digital” [4]

Con la masificación de las comunicaciones globales, y la posibilidad de comercializar grandes cantidades de información traspasando las fronteras físicas, la información específica de cada individuo se ha convertido en una mercancía que cada día adquiere más valor, ya que ésta se puede organizar de tal manera que logra aumentar significativamente la eficiencia y efectividad de la publicidad y disminuir el riesgo de las entidades crediticias a la hora de otorgar productos financieros, pero en conjunto con esta clasificación de las personas, se han implementado nuevas fuentes de discriminación y se han reforzado otras ya existentes. Ante esta problemática los gobiernos se han puesto en la tarea de implementar protecciones legales a través de leyes como un primer paso básico para el manejo de los datos personales de los ciudadanos que estén almacenados en cualquier tipo de medio sea digital o físico.

Con este contexto en mente la información y los datos de las personas son elementos fundamentales para tomar múltiples determinaciones de negocios hoy en día. Prueba de esto es que ya es una realidad que las entidades públicas y privadas posean sistemas de información conformados por redes de telecomunicaciones y bases de datos que diariamente se alimentan de información personal, es aquí donde se hace crucial que el sistema de gestión de seguridad de la información involucre el cumplimiento de las leyes vigentes respecto a la protección de los datos personales.

Para el desarrollo del presente documento se han tomado como base las leyes relacionadas con la protección de datos personales existente en Argentina y la que está en desarrollo en Colombia Adicionalmente se hace referencia a la Directiva 95/46/C de la Comisión Europea, en la que se establece cual es el nivel adecuado de protección de los datos personales, para la transferencia internacional de dicha información.

3. Objetivos

Los objetivos principales a desarrollar a lo largo del presente documento son:

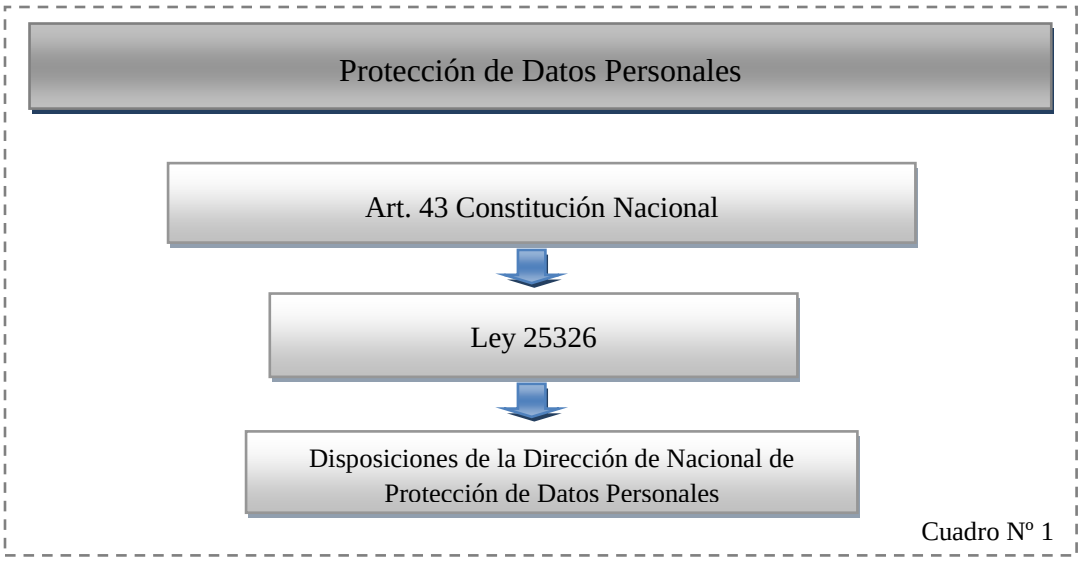
- Establecer criterios de comparación que permitan el análisis de la estructura y características de la ley argentina 25326 y el proyecto de ley 46 de 2010 de Colombia.
- Identificar y resaltar los beneficios que puede traer la aplicación y control de estas leyes en los países suramericanos.
- Relacionar los aspectos de seguridad mencionados por las leyes, con los lineamientos establecidos en la norma ISO27000 - Gestión de la seguridad informática.

4. Estructura y Características de las Leyes.

4.1. Ley 25.326 – Argentina.

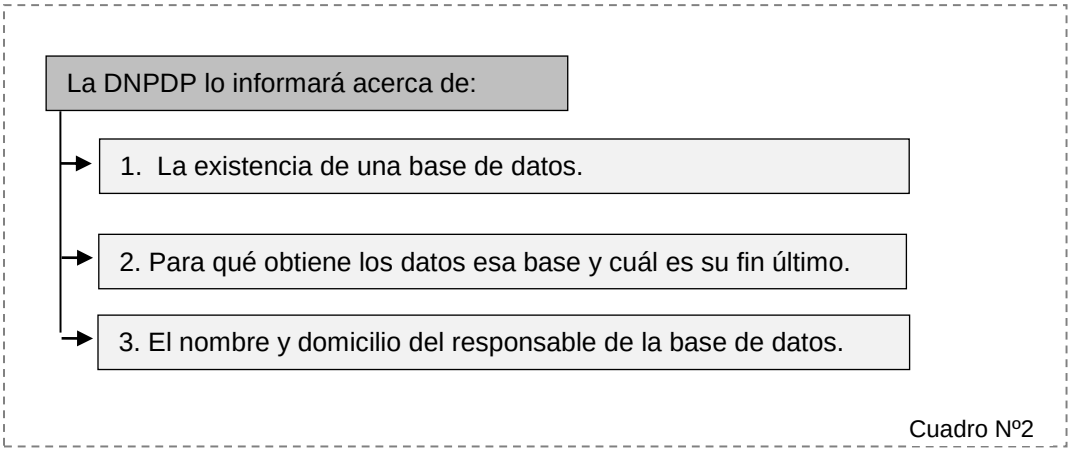
La protección de datos personales en Argentina, es un derecho establecido en la Constitución Nacional luego de la reforma de 1994. En año 2000, se sanciona la ley 25.326 de Protección de Datos Personales, el convirtiéndose en la primera reglamentación para el Habeas Data en nuestro país.

Citada norma crea un organismo de Ámbito Nacional, denominado Dirección de Nacional de Protección de Datos Personales (DNPDP), para la efectiva protección de los datos personales. (Véase Cuadro Nº1).



Cuadro Nº 1

La DNPDP, tiene a su cargo el Registro de las Bases de Datos, instrumento organizado a fin de conocer y controlar las bases de datos. También "asesora y asiste a los titulares de datos personales recibiendo las denuncias y reclamos efectuados contra los responsables de los registros, archivos, bancos o bases de datos por violar los derechos de información, acceso, rectificación, actualización, supresión y confidencialidad en el tratamiento de los datos" [1] (Véase Cuadro 2).



Cuadro Nº2

[1] Dirección Nacional de Protección de Datos Personales (2010), "Funciones del DNPDP" accedido de http://www.jus.gov.ar/dnpdp/

4.2. **Proyecto de Ley 46 – COLOMBIA**

En el proyecto de Colombia, es establecer la unificación de la normativa vinculada y establecer un organismo de de contralor del las bases de datos utilizadas. Consideramos importante destacar el Artículo Nº 1 de la Ley 1266 de 2008, Habeas – Data – Colombia, el cual establece que “tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países.” [1].

5. Criterios.

A continuación se analizarán los puntos más relevantes a considerar entre la Ley 25.326 de la Argentina y Proyecto de Ley Estatutaria Nº 046 de 2010 Cámara, por el Cual se dictan disposiciones Generales para la Protección de Datos Personales en el Congreso de Colombia.

- Conceptos y objetivos.

El principal objetivo de la ley argentina es 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.”[8]

Del mismo modo, en el Artículo 1 del Proyecto colombiano se establece que “La presente ley tiene por objeto desarrollar el derecho constitucional que tiene todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o

archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política". [9]

El espíritu de ambas normativas es contemplar el derecho de la protección de los datos de las personas físicas y de existencia ideal.

- Definiciones.

En el Artículo 3 del proyecto colombiano, se establecen las siguientes definiciones:

"a. Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.

b. Base de Datos: Conjunto organizado de datos personales que sea objeto de tratamiento.

c. Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas determinadas o determinables.

d. Encargado del tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del Responsable del Tratamiento.

e. Responsable del tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.

f. Titular: Persona cuyos datos personales sean objeto de tratamiento.

g. Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión."[10]

En la Legislación Argentina en el artículo 2 de la ley se establecen las siguientes deficiones:

— Archivo, registro, base o banco de datos: "Indistintamente, designan al 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."[11]

En las empresas, existen numerosas bases de datos, originadas por el curso normal de las actividades, como por ejemplo, facturas, clientes, análisis de marketing, etc.

— Datos personales: “Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.”[3]

Al confeccionar diferentes comprobantes comerciales como facturas, Notas de Débitos, Notas de Créditos, se registran datos personales.

— Tratamiento de datos: “Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, 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.” [3]

Las empresas, dependiendo de su envergadura, poseen sistemas de tratamiento y conservación de los datos, por el desarrollo de sus actividades.

— 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.” [3]

— Datos informatizados: “Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.” [3]

— 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.” [3]

— 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.” [3]

— Disociación de datos: “Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.”[3]

Con las definiciones contenidas en la ley, podemos identificar diferentes bases de datos confeccionadas y registradas en las compañías con el objetivo de realizar informes para uso interno y externo.

- Licitud de los archivos, tratamiento y recolección de datos.

Según el artículo 3 de la ley argentina, la formación de archivos de datos será lícita “cuando se encuentren debidamente inscriptos, observando en su operación los principios que establecen la presente ley y las reglamentaciones que se dicten en su consecuencia.” También determina que los archivos de datos “no pueden tener finalidades contrarias a las leyes o a la moral pública”.[12]

En el artículo 4 de la ley, se establecen los requisitos en la recolección de la información incluida en las Bases de datos. Los datos deben cumplir con las siguientes características de calidad:

“1. 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.

2. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley.

3. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.

4. Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario.

5. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la presente ley.

6. Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.

7. Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.” [13]

El proyecto Colombiano, en su artículo 4 establece los principios para el “tratamiento de datos personales. En el desarrollo, la interpretación y aplicación de la presente ley, se aplicarán, de

manera armónica e integral, los siguientes principios…” [14] siendo los más importantes los seleccionados en el siguiente cuadro:

Los Principios Rectores más importantes	
Principio de legalidad en materia de Tratamiento de Datos	El tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen.
Principio de finalidad	El tratamiento debe obtener a una finalidad con la Constitución y la Ley, la cual debe ser informada al titular.
Principio de libertad	El tratamiento sólo puede ejercerse con el consentimiento libre, previo y expreso del titular y no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia del mandato legal o judicial que revele el consentimiento.
Cuadro Nº3	

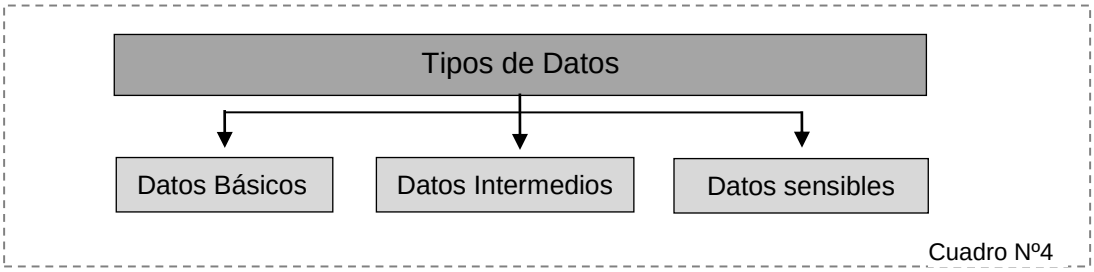
Ambos documentos establecen que el tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias.

- Clasificación de los Datos Personales.

En el artículo 5 del proyecto colombiano, se especifican datos sensibles como “aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas

o filosóficas, la permanencia a sindicatos, así como los datos referidos a la vida sexual y los datos biométricos.” [15]

La ley Argentina, del mismo modo se definen los datos sensibles. Pero en el decreto reglamentario y las Disposiciones de la Dirección Nacional de Protección de Datos Personales, se establece una clasificación a los datos personales, los cuales son clasificados en Datos Básicos, Intermedio y Sensibles.



Cuadro Nº4

- Los datos considerados básicos, corresponden a los presentes en el padrón electoral. Entre ellos encontramos al Número de Identidad, Nombre y Apellido, CUIT, CUIL, Domicilio, Fecha de Nacimiento, entre otros.
- Los datos Intermedios son los que superan a los básicos y no son sensibles. Por ejemplo, estado civil, Ingresos y egresos, etc.
- Los datos sensibles son 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.

Con respecto a la categoría de datos, el artículo 7 de la Ley establece que:

“1. Ninguna persona puede ser obligada a proporcionar datos sensibles.

2. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.

3. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros.

4. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas.” [16]

- Responsabilidad de los usuarios de la Base de Datos

En el proyecto de ley Colombiana son denominados a los usuarios, a los encargados del tratamiento. En el artículo 18, establece que a los encargados “deberán cumplir los siguientes deberes… entre otros los siguientes:

a. Garantizar al titular en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

b. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

c. Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley.

d. Actualizar la información reportada por los responsables del tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo.

e. Tramitar las consultas y los reclamos formulados por los Titulares en los señalamos en la presente ley.

f. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los titulares.” [17]

En la ley Argentina se establece que los particulares que formen archivos, registros o banco de datos que no sean para un uso exclusivamente personal deberán estar debidamente registrados.

En la emisión, confección y posterior conservación de la documentación respaldatoria de los Sistemas de Información, las organizaciones deberían cumplir con los siguientes requisitos de inscripción y registro de archivos de Datos enunciados en el artículo 21 de la Ley, el cual comprende 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;

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.”[18]

Por ningún motivo los usuarios, podrán poseer datos personales de naturaleza distinta a los declarados en el registro. El incumplimiento de estos requisitos dará lugar a las sanciones administrativas previstas en la presente ley.

- Seguridad de los Datos

En la Legislación Argentina, el responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, 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.

Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

A los interesados en profundizar en Medidas de seguridad establecidas por las Disposiciones de la Dirección Nacional de Protección de Datos Personales, en la República Argentina, en el Anexo 1 del presente trabajo se especificarán brevemente.

- Sanciones.

En el proyecto colombiano se establece que la autoridad de control podrá imponer las siguientes sanciones los responsables del tratamiento y encargados del tratamiento las sanciones especificadas en el siguiente cuadro:

Sanciones Establecidas en el Proyecto Colombiano	
Multas de carácter personal e institucional a favor de la Superintendencia de Industria y Comercio.	Hasta por un equivalente de dos mil salarios mínimos mensuales legales al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó.
Suspensión de las actividades relacionadas con el tratamiento.	Hasta 6 meses.
Cierre temporal de las operaciones relacionadas con el tratamiento	Transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por una autoridad de control.
Cierre inmediato y definitivo.	De la operación que involucre el tratamiento de datos sensibles.
Cuadro Nº 5	

En el siguiente cuadro se especifican las Sanciones Judiciales y Administrativas establecidas por la ley de habeas data en Argentina:

Sanciones especificadas en la República Argentina	
Leves: Incumplimiento	- Hasta 2 apercibimientos y/o multa de $ 1000 a $ 3000.

Graves: Incumplimiento persistente	- Hasta 4 apercibimientos - Suspensión de 1 a 30 días y/o multa de $3001 a $50000
Muy Graves: Reiterados incumplimientos y obstaculizar	- Hasta 6 apercibimientos - Suspensión de 31 a 365 días. - Clausura o cancelación de banco de datos y/o multa de $ 50001 a $100000.

Cuadro Nº 6
Fuente: Silvia Iglesias, El rol del Profesional en Ciencias Económicas ante la Ley 25.326 de Protección de Datos Personales. Consejo Profesional en Ciencias Económicas de la Ciudad de Buenos Aires. Presentación realizada 14/07/2011.

Destacamos también que la legislación argentina dispone que también dispone los artículos de en el código penal relacionados con el delito informático.

ARTICULO 117 bis.

- La pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales.

- La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona.

- Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el de la condena. [19]

ARTICULO 157 bis.

-Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:

1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2. Ilegítimamente proporcionare o revelare 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.

3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años. [20]

6. Cumplimiento. Directiva 95/46/CE24 Europa.

El cumplimiento es un concepto que no solo se refiere a la validación de que ciertos procesos se estén realizando de determinada forma, sino que incluye el garantizar que dicha forma es la más adecuada respecto a otras.

Acorde a lo anterior, es importante resaltar que para el caso de la protección de datos personales, la implementación de dichas regulaciones al interior de cada país, tiene alcances internacionales, en lo referente al intercambio de este tipo de información con otras naciones.

Existen muchas razones y justificaciones para la transferencia de información personal entre países, la cual puede ser de tipo comercial, económico, de seguridad nacional y/o mundial, etc.

Desde 1970 se han expedido leyes para la protección de datos personales en Estados Unidos y Europa que defienden los derechos de los dueños de la información pero que no impiden su tratamiento.

Sin embargo para que la transferencia de datos entre países, no afecte los recaudos tomados al interior de estos, el parlamento Europeo emitió el 24 de Octubre de 1995, la Directiva 95/46/CE24 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos. [6].

Dicha directiva establece que la transferencia a un tercer país de datos personales sólo puede realizarse cuando “el país tercero del que se trate garantice un nivel de protección adecuado”[5].

Esto se refiere a que el país que recibe la información debe contar con un grado de protección superior o igual al que el estado emisor le garantiza al dueño de la información.

Como antecedente a la directiva mencionada, el convenio 108 del Consejo de Europa, del 28 de Enero de 1981, estableció flujo libre de información de datos personales entre los países pertenecientes al convenio y prohibido o restringido a países no pertenecientes. En el 2001 se

modifica el convenio, estableciendo que el flujo está permitido con países que tengan un nivel adecuado de protección. [5].

El nivel adecuado de protección indica que los países emisores y/o receptores de información de datos personales, deben manejarla acorde a ciertas condiciones, las cuales se mencionan a continuación.

Condiciones de carácter regulatorio:

- Derechos del titular de los datos.
- Deberes de quienes procesan la información o ejercen control sobre este tratamiento.

Requisitos de procedimiento y aplicación:

- Mecanismos judiciales y no judiciales que garanticen el cumplimiento de las normas.
- Sanciones por incumplimiento.
- Derecho a reparación del dueño de los datos.
- Autoridad independiente que regule el cumplimiento y garantice la protección de los datos personales.

A continuación se presenta una lista básica de referencia, para establecer si un país cuenta con un nivel adecuado de protección a los datos personales.

PRINCIPIOS BÁSICOS.[2]
Limitación de la finalidad.
Calidad de los datos y proporcionalidad.
Transparencia.
Seguridad.
Acceso, rectificación y oposición.
Restricciones a las transferencias sucesivas a otros terceros países.
Cuadro Nº 7

ASPECTOS APLICABLES A TRATAMIENTOS ESPECIALES. [3]
Datos sensibles.
Mercadeo Directo.
Decisión individual automatizada.
Cuadro Nº8

El único país latinoamericano que cumple el nivel adecuado de protección de datos personales exigido por la directiva europea es Argentina, otros países como Uruguay y México cuentan con leyes pero no con la acreditación, Colombia, Perú y Chile están trabajando en sus respectivas leyes para cumplir con dicho requerimiento.

2 Fuente: Nelson Remolina Angarita [5]:

3 Fuente: Nelson Remolina Angarita [5]:

6.1. Beneficios.

Contar con la acreditación del parlamento europeo respecto del tratamiento de los datos personales, trae beneficios como:

- ✓ Contar con un grado de protección jurídica de los derechos de los dueños de los datos.
- ✓ Incrementar sus posibilidades de ser escenarios para la realización de negocios que impliquen intercambio de información con otros países.
- ✓ Poseer una ventaja competitiva ante el mercado internacional para la creación de nuevos negocios.
- ✓ Contribuir a mejorar servicio a los clientes.
- ✓ Incrementar el flujo de inversión extranjera.

Particularmente en Colombia el Ministerio de Comercio, Industria y Turismo, considera que la acreditación ayudara al crecimiento del sector de servicios, teniendo en cuenta que las transferencias internacionales de información a países de la región, indican diferencias al ser un país no certificado, pues las transferencias provenientes de países europeos no está permitida. [7].

En los últimos meses la Organización de Estados Americanos - OEA, ha estado trabajando en iniciativas que permitan establecer un tratado internacional que regule los derechos a la protección de los datos personales, con el fin de que América se convierte en un puerto seguro para el intercambio de éstos, lo cual potenciará el crecimiento en el sector de tecnologías de la información. [2].

7. Familia de normas ISO27000.

Cuando se trabaja con datos personales dentro de una entidad, sin importar cuál sea el área a la que se dedica, y en algún punto se almacenan, trasmiten o procesan datos personales entonces se tiene que demostrar el cumplimiento de la ley de protección de dichos datos.

Para demostrar el buen manejo de este tipo de información específica, se hará necesario mantener actualizada una serie de evidencias y registros del control que se hace del cumplimiento de la normativa. La manera más aconsejable de llevar al día estas evidencias consiste en incorporar el cumplimiento de la ley dentro del sistema de gestión de seguridad de la información, Partiendo de una clasificación de la información especificada precedentemente.

Una vez concluida la clasificación, considerar a cada nivel como un activo de la empresa, evaluando el impacto que tiene sobre el negocio, cualquier incidente de seguridad que se relacione con alguno de estos niveles, de esta forma impulsar que esta clasificación sea incluida dentro del sistema de gestión de riesgos.

Teniendo en cuenta lo que las diferentes leyes de protección de datos personales tienen en común, presentamos una serie de controles para ser tenidos en cuenta dentro del sistema de gestión de seguridad de la información, sugerido por la familia de normas ISO 27000.

Controles para ser tenidos en cuenta dentro del sistema de gestión de seguridad de la información		
A.6.1.4	Procedimiento de autorización para instalaciones de procesamiento de datos personales	Implementar un proceso para autorizar nuevas instalaciones que vayan a trabajar con datos personales.
A.6.1.5	Acuerdos de confidencialidad	Se deben identificar y revisar periódicamente los requerimientos de confidencialidad o acuerdos de no divulgación que reflejan las necesidades de protección de datos personales
A.6.2.1	Identificación de riesgos relacionados con las terceras partes	Identificar los riesgos para la información de datos personales y de los procesos de negocios que involucren terceras partes que manipulen estos datos.
A.6.2.3	Asignación de la seguridad en acuerdos con terceras partes	Los acuerdos con terceras partes que involucren el acceso, procesamiento, comunicación o gestión de datos personales recopilados por la organización deben cubrir todos los requerimientos de seguridad que puedan comprometer a la organización.

A.7.1.1	Inventario de los datos personales	Se deben identificar claramente que datos personales son indispensables para la organización y mantener un conteo adecuado del número de registros de datos personales que se está manejando de la misma manera que se actualiza un inventario de los activos.
A.7.1.2	Propiedad de los datos personales dentro de la organización	Todos los datos personales que se manejen dentro de la organización deben estar bajo la responsabilidad directa, clara y especifica de algún sector de la organización.
A.7.1.3	Uso aceptable de los datos personales	Se deben identificar, documentar e implementar reglas para el uso aceptable de los datos personales.
A.7.2.1	Directrices para la clasificación de datos personales	Los datos personales según su valor, requerimientos legales, sensibilidad, y criticidad para la organización se clasifican en: **Nivel Básico**: datos de carácter personal como pueden ser nombre y apellidos, correos electrónicos, direcciones etc. **Nivel Medio**: datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, de solvencia patrimonial y de crédito. Se incluyen datos personales que permitan obtener una evaluación de personalidad. **Nivel Alto**: datos sobre ideología, religión, creencias, origen racial, salud o vida sexual.
A.7.2.2	Rotulado y manejo de los datos persoanles	Se debe desarrollar e implementar un apropiado conjunto de procedimientos para rotular y manipular la información, en concordancia con el esquema de clasificación adoptado por la organización.
A.10.7.3	Procedimientos del manejo de datos personales	Se deben establezcan procedimientos para el manejo y almacenamiento de los datos personales, para protegerlos contra su uso inadecuado o divulgación no autorizada.
A.10.8.1	Políticas y procedimientos de intercambio de datos personales	Se deben establecer políticas, procedimientos y controles formales para proteger el intercambio de información a través del uso de todos los tipos de las instalaciones de comunicación.
A.10.8.2	Acuerdo de intercambio	Se deben establecer acuerdos de intercambio de información que contenga datos personales entre la organización y las terceras partes.
A.10.10.1	Registro de auditoría	Se deben producir y mantener registros de auditorías en los cuales se registren las actividades, excepciones, y eventos de seguridad, especificamente referentes al manejo de datos personales, por un período acordado para ayudar en futuras investigaciones y el seguimiento del control de acceso.
A.11.1.1	Política de control de accesos	Se debe establecer, documentar y revisar una política de control de accesos a los datos personales, basada en los requerimientos de acceso de seguridad y del negocio.
A.11.2.2	Administración de privilegios	La asignación y el uso de los privilegios sobre los repositorios de datos personales debe ser estrictamente restringido y controlado.
A.11.6.2	Aislamiento de sistemas sensibles	Los sistemas que almacenen datos personales deben considerarse como sensibles y por ende se deben encontrar en un ambiente informático dedicado (aislado).
A.12.2.1	Validación de los datos de entrada	Los datos de entrada en los sistemas de manejo de datos personales deben ser validados para asegurar que los mismos son correctos y apropiados.
A.12.2.2	Controles de procesamiento interno	Las verificaciones de validación deben ser incorporadas a las aplicaciones para detectar cualquier caso de corrupción de los datos personales a través del procesamiento de errores o actos deliberados.
A.12.2.4	Validación de los datos de salida	Se debe validar la salida de datos de una aplicación para garantizar que el procesamiento de los datos personales almacenados son correctos y adecuados a las circunstancias.

T

A.12.4.2	Protección de los datos de prueba del sistema	Los datos de prueba deben ser seleccionados cuidadosamente, protegidos y controlados.
A.12.5.4	Fuga de la información	Se deben prevenir las oportunidades de fuga de la información.
A.15.1.1	Identificación de la legislación aplicable	Todos los requerimientos legales, de la ley argentina 25326 respecto a la protección de datos personales, deben ser definidos y documentados y se deben mantener actualizados para cada sistema de información y para la organización
A.15.1.4	Protección de los datos y privacidad de la información personal	La protección y privacidad de los datos debe estar garantizada según se requiera en las legislaciones y regulaciones relevantes, y si es aplicable, en las cláusulas contractuales.

Cuadro Nº 9

8. Conclusiones.

En el desarrollo el presente trabajo, se ha pretendido contribuir con la difusión de la Ley de Protección de Datos Personales y el Proyecto de Ley Estatutaria Nº 046 de 2010 Cámara, por el Cual se dictan disposiciones Generales para la Protección de Datos Personales en el Congreso de Colombia.

Ambos cuerpos normativos establecen que las Bases de Datos existentes en las organizaciones, moderadoras de datos personales destinados a proporcionar informes, deben inscribirse en el Registro que al efecto habilite el organismo de control, cumpliendo con Normas y Procedimientos establecidos por diferentes organismos.

Conjuntamente con la registración de las bases de datos con información personal, las empresas deben adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, para evitar su adulteración, pérdida, consulta o tratamiento no autorizado, 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.

Ambas normativas establecen sanciones Judiciales y Administrativas por incumplimiento de las disposiciones establecidas, en la legislación Argentina, como en proyecto de ley colombiano. Se resalta que por el Habeas Data, pueden establecerse sanciones por vulnerarse el derecho al acceso, y en lo referente Derechos Personales, pueden establecerse sanciones por derechos personales del Fuero Civil y por derechos del Consumidor.

Se considera necesario la instrucción de estos conceptos a los profesionales relacionados con el uso y desarrollo de las tecnologías de información, para prevenir posibles incumplimientos de las normativas legales, como también generar una cultura de la seguridad de la información que contribuya a brindar un mejor servicio en el tratamiento de la misma.

9. Referencias Bibliográficas.

[1] Congreso de Colombia. Proyecto de Ley Estatutaria Número 0046 Cámara. http://www.habeasdata.org.co/wp-content/uploads/2010/08/proyecto-de-ley-46-de-2010-camara.pdf

[2] Consejo permanente de la OEA - Organización de los Estados Americanos. Departamento de Derecho Internacional de la Secretaría de Asuntos Jurídicos. Proyecto de principios y recomendaciones preliminares sobre la protección de datos personales. noviembre, 2010. http://www.oas.org/dil/esp/CP-CAJP-2921-10_esp.pdf.

[3] Ley 25.326. Protección de datos personales. http://www.infoleg.gov.ar/

[4] Meglena Kuneva, European Consumer Commissioner, Roundtable: Keynote Speech(Bruselas, 31 de marzo, 2009), citada por Katitza Rodríguez-Pereda. Ponencia presentada en el I Seminario Euro-Iberoamericano de protección de datos: La protección de los menores, Cartagena, 26-28 de mayo de 2009.

[5] Remolina-Angarita Nelson, ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?, 16 International Law, Revista Colombiana de Derecho Internacional, 489-524 (2010). http://www.habeasdata.org.co/wp-content/uploads/2010/08/colombia-y-nivel-adecuado-de-proteccion-de-datos-nelson-remolina-il-julio-de-2010.pdf

[6] Parlamento Europeo. Directiva 95/46/CE de 24 de octubre de 1995, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:ES:HTML

[7] Portafolio.co. Ley de protección de datos favorece al sector de servicios. Diciembre 2010. http://www.portafolio.co/economia/ley-proteccion-datos-favorece-al-sector-servicios.

[8] Dirección Nacional de Protección de Datos Personales. Preguntas Frecuentes, Ley de Protección de Datos Personales Nº 25.326 (Art.1º Objeto), http://www.jus.gov.ar/datos-personales/preguntas-frecuentes.aspx

[9] OBSERVATORIO DE LA PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA HABEAS DATA.ORG.CO, Artículo 1 Proyecto de Ley Estatutaria Nº 046 de 2010 Cámara. "Por el Cual se dictan disposiciones Generales para la Protección de Datos Personales" En el Congreso de Colombia. http://www.habeasdata.org.co/wp-content/uploads/2010/08/proyecto-de-ley-46-de-2010-camara.pdf

[10] OBSERVATORIO DE LA PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA HABEAS DATA.ORG.CO, Artículo 3 Proyecto de Ley Estatutaria Nº 046 de 2010 Cámara. "Por el Cual se dictan disposiciones Generales para la Protección de Datos Personales" En el Congreso de Colombia. http://www.habeasdata.org.co/wp-content/uploads/2010/08/proyecto-de-ley-46-de-2010-camara.pdf

[11] Infoleg (2011), "Ley de 25326 de Habeas Data, Artículo 2" accedido desde www.infolef.gov.ar

[12] Infoleg (2011), "Ley de 25326 de Habeas Data, Artículo 3" accedido desde www.infolef.gov.ar

[13] Infoleg (2011), "Ley de 25326 de Habeas Data, Artículo 4" accedido desde www.infolef.gov.ar

[14] OBSERVATORIO DE LA PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA HABEAS DATA.ORG.CO, Artículo 4 Proyecto de Ley Estatutaria Nº 046 de 2010 Cámara. "Por el Cual se dictan disposiciones Generales para la Protección de Datos Personales" En el Congreso de Colombia. http://www.habeasdata.org.co/wp-content/uploads/2010/08/proyecto-de-ley-46-de-2010-camara.pdf

[15] OBSERVATORIO DE LA PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA HABEAS DATA.ORG.CO, Artículo 5 Proyecto de Ley Estatutaria Nº 046 de 2010 Cámara. "Por el Cual se dictan disposiciones Generales para la Protección de Datos Personales" En el Congreso de Colombia. http://www.habeasdata.org.co/wp-content/uploads/2010/08/proyecto-de-ley-46-de-2010-camara.pdf

[16] Infoleg (2010), "Ley de 25326 de Habeas Data, Artículo 7" accedido desde www.infolef.gov.ar

[17] OBSERVATORIO DE LA PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA HABEAS DATA.ORG.CO, Artículo 18 Proyecto de Ley Estatutaria Nº 046 de 2010 Cámara. "Por el Cual se dictan disposiciones Generales para la Protección de Datos Personales" En el Congreso de Colombia. http://www.habeasdata.org.co/wp-content/uploads/2010/08/proyecto-de-ley-46-de-2010-camara.pdf

[18] Infoleg (2011), "Ley de 25326 de Habeas Data, Artículo 21" accedido desde www.infolef.gov.ar

[19] Infoleg (2011), Código Penal. http://www.infoleg.gov.ar/infolegInternet/anexos/15000-19999/16546/texact.htm#16

[20] Infoleg (2011), Código Penal. http://www.infoleg.gov.ar/infolegInternet/anexos/15000-19999/16546/texact.htm#19

Anexo 1: Medidas de la Disposición Nacional de Protección de Datos Personales de la República Argentina en la Seguridad de los Datos.

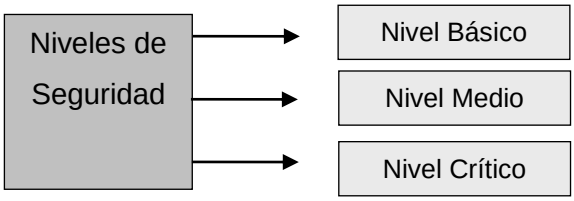
El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

En la disposición 11/2006, la Dirección Nacional de Protección de Datos Personales, establece diferentes niveles de seguridad, para el tratamiento y conservación de los datos personales contenidos en archivos, registros, bancos y bases de datos publicas no estatales y privadas.

Los niveles de seguridad dependen del tipo de datos que contengan. (Véase Cuadro Nº4)

A continuación, se enunciarán las características más importantes de cada nivel de seguridad. A los interesados en el tema, invito a descargar de la página web indicada en la bibliografía del presente trabajo, la resolución completa Nº 11/2006 de la DNPDP.



Cuadro Nº10

• MEDIDAS DE SEGURIDAD DE NIVEL BASICO:[4]

Los archivos, registros, bases y bancos de datos que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de Nivel Básico que a continuación se detallan:

Disponer del Documento de Seguridad de Datos Personales en el que se especifiquen, entre otros, los procedimientos y las medidas de seguridad a observar sobre los archivos, registros, bases y bancos que contengan datos de carácter personal. Deberá mantenerse en todo momento actualizado y ser revisado cuando se produzcan cambios en el sistema de información.

Deberá contener entre otras:

1. Funciones y obligaciones del personal.
2. Descripción de los archivos con datos de carácter personal y los sistemas de información que los tratan.
3. Descripción de las rutinas de control de datos de los programas de ingreso de datos y las acciones a seguir ante los errores detectados a efectos de su corrección. Todos los programas de ingreso de datos, cualquiera sea su modo de procesamiento (batch, interactivo, etc.), deben incluir en su diseño, rutinas de control, que minimicen la posibilidad de incorporar al sistema de información, datos ilógicos, incorrectos o faltantes.
4. Registros de incidentes de seguridad.
5. Procedimientos para efectuar las copias de respaldo y de recuperación de datos.
6. Relación actualizada entre Sistemas de Información y usuarios de datos con autorización para su uso.
7. Procedimientos de identificación y autenticación de los usuarios de datos autorizados para utilizar determinados sistemas de información.
8. Control de acceso de usuarios a datos y recursos necesarios para la realización de sus tareas para lo cual deben estar autorizados.
9. Adoptar medidas de prevención a efectos de impedir amenazas de software malicioso (virus, troyanos, etc.) que puedan afectar archivos con datos de carácter personal.

[4] Infoleg (2011), “Disposición 11/2006, Medidas de Seguridad de Nivel Básico” accedido desde www.infolef.gov.ar

• MEDIDAS DE SEGURIDAD DE NIVEL MEDIO:[5]

Los archivos, registros, bases y bancos de datos de las empresas privadas que desarrollen actividades de prestación de servicios públicos, así como los archivos, registros, bases y bancos de datos pertenecientes a entidades que cumplan una función pública y/o privada que, más allá de lo dispuesto por el artículo 10 de la Ley Nº 25.326, deban guardar secreto de la información personal por expresa disposición legal (como el secreto bancario), además de las medidas de seguridad de nivel Básico, deberán adoptar las que a continuación se detallan:

1. El Instructivo de seguridad deberá identificar al Responsable (u órgano específico) de Seguridad.
2. Realización de auditorías (internas o externas) que verifiquen el cumplimiento de los procedimientos e instrucciones vigentes en materia de seguridad para datos personales.
3. Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.
4. Se establecerá un control de acceso físico a los locales donde se encuentren situados los sistemas de información con datos de carácter personal.
5. Gestión de Soportes e información contenida en ellos.
6. Los registros de incidentes de seguridad, en el caso de tener que recuperar datos, deberán identificar la persona que recuperó y/o modificó dichos datos. Será necesaria la autorización en forma fehaciente del responsable del archivo informatizado.
7. Las pruebas de funcionamiento de los sistemas de información, realizadas con anterioridad a su puesta operativa no se realizarán con datos/archivos reales, a menos que se aseguren los niveles de seguridad correspondientes al tipo de datos informatizados tratados.

• MEDIDAS DE SEGURIDAD DE NIVEL CRÍTICO:[6]

[5] Infoleg (2011), “Disposición 11/2006, Medidas de Seguridad de Nivel Medio” accedido desde www.infoleg.gov.ar

Los archivos, registros, bases y bancos de datos que contengan datos personales, definidos como "datos sensibles", con la excepción que se señalará más abajo, además de las medidas de seguridad de nivel Básico y Medio, deberán adoptar las que a continuación se detallan:

1. Distribución de soportes: cuando se distribuyan soportes que contengan archivos con datos de carácter personal —incluidas las copias de respaldo—, se deberán cifrar dichos datos (o utilizar cualquier otro mecanismo) a fin de garantizar que no puedan ser leídos o manipulados durante su transporte.
2. Registro de accesos: se deberá disponer de un registro de accesos con información que identifique al usuario que accedió, cuando lo hizo (fecha y hora), tipo de acceso y si ha sido autorizado o denegado. En el caso que el acceso haya sido autorizado se deberá identificar el dato accedido y el tratamiento que se le dio al mismo (baja, rectificación, etc.). Este registro de accesos deberá ser analizado periódicamente por el responsable de seguridad y deberá ser conservado como minino por el término de un TRES (3) años.
3. Copias de respaldo: además de las que se mantengan en la localización donde residan los datos deberán implementarse copias de resguardo externas, situadas fuera de la localización, en caja ignífuga y a prueba de gases o bien en una caja de seguridad bancaria, cualquiera de ellas situadas a prudencial distancia de la aludida localización. Deberá disponerse de un procedimiento de recuperación de esa información y de tratamiento de la misma en caso de contingencias que pongan no operativo el/los equipos de procesamiento habituales.
4. Transmisión de datos: los datos de carácter personal que se transmitan a través de redes de comunicación, deberán serlo cifrados o utilizando cualquier otro mecanismo que impida su lectura y/o tratamiento por parte de personas no autorizadas.

Conjuntamente con la registración de las bases de datos con información personal, las empresas deben implementar el nivel de seguridad acorde con el tipo de datos que manejen, cabe destacar que el incumplimiento de estos requisitos dará lugar a las sanciones administrativas previstas en la presente ley.

---

[6] Infoleg (2011), “Disposición 11/2006, Medidas de Seguridad de Nivel Crítico” accedido desde www.infoleg.gov.ar