XXIV Jornadas Profesionales de Contabilidad, XXII de Auditoría y XI de Gestión y Costos. Colegio de Graduados en Ciencias Económicas, Buenos Aires, 2011.

Disposiciones de la Dirección Nacional de Protección de Datos Personales y el Sistema Contable de informción contable microsocial.

Diego Sebastian Escobar.

APORTES DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL SISTEMA DE INFORMACIÓN CONTABLE. NUEVOS CONOCIMIENTOS DEL CONTADOR PÚBLICO EN LA ERA DE LA INFORMACIÓN.

Área: V.2: Sistemas de Información y Gestión

Tema: 2. Auditoría y Seguridad: Auditoría en ambientes computarizados. Fraude informático. Gestión del riesgo.

Código de Identificación: JOV5

Índice

0. Resumen

En el presente trabajo, se plantea analizar la Ley de Protección de Datos Personales y sus aportes en el Sistema de Información Contable. Destacando la importancia de la divulgación de la misma entre los Contadores Públicos, dado que por diferentes factores muchos profesionales desconocen la incidencia en su ámbito de actuación.

A lo largo del trabajo, se desarrollará el marco legal de la protección de datos personales, las partes pertinentes de la ley 25326 y su aplicación en el sistema de información contable, el rol de la Dirección Nacional de Datos Personales, los derechos de los titulares de los datos, las responsabilidades de los usuarios de base de datos, y por último, la seguridad de la información y los servicios tercerizados de datos personales.

Luego del análisis, se concluye en que determinadas bases de datos existentes en las empresas deben ser registradas en los correspondientes organismos de control para cumplir con la normativa legal vigente.

APORTES DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL SISTEMA DE INFORMACIÓN CONTABLE. NUEVOS CONOCIMIENTOS DEL CONTADOR PÚBLICO EN LA ERA DE LA INFORMACIÓN.

1. Introducción

El avance de la tecnología de la información al final del último siglo, produjo un cambio en la organización y desarrollo de los sistemas de información. Surgieron nuevas tecnologías en el tratamiento, recopilación y conservación de datos y registros que mejoraron su eficiencia y confiabilidad.

Con el manejo masivo de la información, se generaron en el mundo nuevas legislaciones sobre los archivos y bases de datos existentes en los estados y en las organizaciones. En el año 2000, la República Argentina dio un paso importantísimo con la promulgación de la ley de Protección de Datos Personales, en donde se estableció, entre otras obligaciones, que las bases de datos o archivos públicos y privados, destinados a proporcionar informes, deben estar inscriptos en un registro especial.

Siguiendo este concepto, en el sistema de información contable existen numerosas bases de datos que contienen y analizan información personal, emitiendo diferentes tipos de informes cuyos archivos deberían estar registrados para cumplir con la Normativa vigente.

Otras profesiones relacionadas con sistemas o derecho, tienen presente esta legislación sobre las bases de datos, pero gran parte de los contadores públicos desconocen esta normativa, que por su estrecha vinculación con el sistema de información contable en la emisión de Estados Contables deberían ser de su conocimiento.

En este trabajo, se analiza la ley de la Protección da Datos personales y su vinculación con la información contenida en los Sistemas de información Contable informatizados. En una primera parte, se analizará el marco legal de la protección de datos personales y el rol de la Dirección Nacional de Datos Personales. Luego, se estudiarán las partes pertinentes de la normativa y su relación con la información contenida en el sistema contable;

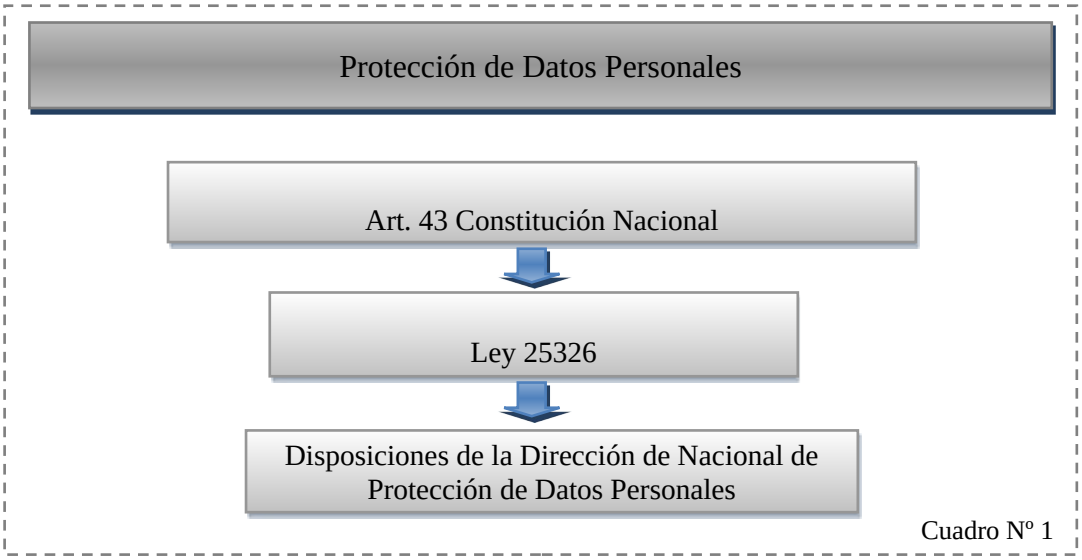
desarrollando los fundamentos para considerar cuáles bases de datos personales deben estar inscriptas.

En la última sección, se expondrán los derechos de los titulares de los datos, las responsabilidades de los usuarios de la base de datos, la seguridad de la información y Servicios tercerizados de datos personales.

2. Marco Legal de la Protección de Datos Personales

La protección de datos personales, está contemplada en el artículo 43, párrafo 3 de la Constitución Nacional Argentina, el cual establece que *"toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos"*[1].

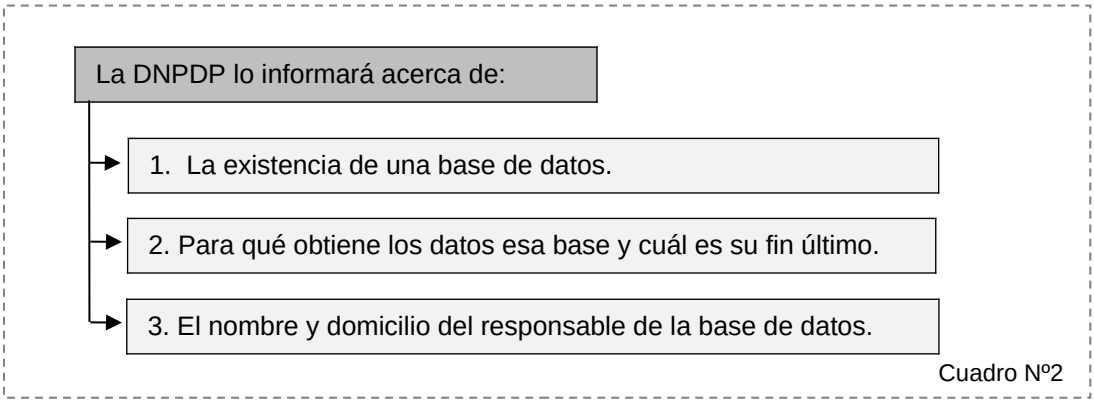
Recién en el año 2000, se sanciona la ley 25.326 de Protección de Datos Personales, convirtiéndose en la primera reglamentación para el Habeas Data en nuestro país. La citada norma crea un organismo de Ámbito Nacional, denominado Dirección Nacional de Protección de Datos Personales (DNPDP), *para la efectiva protección de los datos personales.* (Véase Cuadro Nº1).



Cuadro Nº 1

[1] Congreso de la Nación Argentina (2010), "Constitución Nacional Argentina" accedido de http://www.senado.gov.ar/web/interes/constitucion/capitulo2.php

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*"[2] *(Véase Cuadro 2)*.



Cuadro Nº2

3. Reconocimiento de las bases de Datos presente en las Organizaciones. Conceptos y objetivos de la Ley 25.326.

El principal objetivo de la ley 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."* La ley toma en cuenta a los datos de las personas físicas y de existencia ideal.

En la presente sección se analizarán los artículos más significativos de la ley prestando mayor interés a la emisión y conservación de comprobantes comerciales.

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

3.1. Definiciones

A continuación, se presentarán los conceptos básicos enunciados en el artículo 2 de la ley y se vincularán con los existentes en las empresas.

— 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."*[3]

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 se 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]

---

[3] Infoleg (2010), "Ley de 25326 de Habeas Data, Artículo 2" accedido desde www.infoleg.gov.ar

— 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.

La ley establece también en el artículo 21, que todo archivo, registro, base de datos público, y privado *destinado a proporcionar informes debe inscribirse en el Registro* que al efecto habilite el organismo de control.

Asimismo en el artículo 24, específica que *los particulares que formen archivos, registros o bancos de datos que no sean para un uso exclusivamente personal, deberán registrarse conforme lo previsto en el artículo 21*. La información contenida en los sistemas no es exclusivamente para uso interno, las empresas utilizan estos datos para realizar diversos informes, desde la emisión de los Estados Contables destinada a diversos usuarios, informes de Responsabilidad Social Empresaria, en donde pueden informar sobre las empresas cuáles son proveedores de insumos, o el porcentaje de los destinatarios de los productos desarrollados, hasta estudios de mercados para la misma empresa, distribuidos a sucursales o holding al cual pertenecen.

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

Según el artículo 3 de la Ley 25326, 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."* [4] También determina

[4] Infoleg (2010), "Ley de 25326 de Habeas Data, Artículo 3" accedido desde www.infoleg.gov.ar

que los archivos de datos *"no pueden tener finalidades contrarias a las leyes o a la moral pública".*[4]

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."[5]

El tratamiento de datos personales <u>*es ilícito*</u> 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.

El artículo 5 agrega que "*el referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa*

[5] Infoleg (2010), "Ley de 25326 de Habeas Data, Artículo 4" accedido desde www.infoleg.gov.ar

notificación al requerido de datos, de la información descrita en el artículo 6° de la presente ley."[6]

También establece que no será necesario el consentimiento cuando:

"a) Los datos se obtengan de fuentes de acceso público irrestricto;

b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;

c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;

d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;

e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526."

3.3. Obligaciones de las empresas al recabar información.

Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara:

- La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios;
- La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable;
- El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente;
- Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos;
- La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

[6] Infoleg (2010), "Ley de 25326 de Habeas Data, Artículo 5" accedido desde www.infoleg.gov.ar

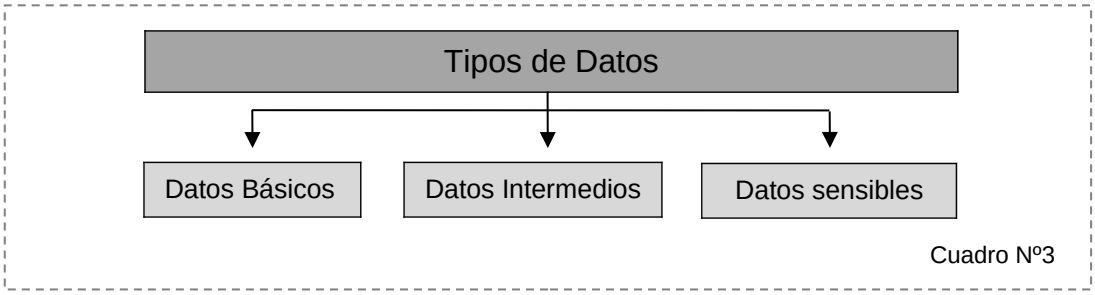
4. Tipo de Datos

La ley 25.328 y las Disposiciones de la Dirección Nacional de Protección de Datos Personales, han establecido una clasificación a los datos personales, en Datos Básicos, Intermedios y Sensibles.

- 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.



Cuadro Nº3

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."[7]

A continuación se presenta la documentación presente en las empresas, en donde se incluyen datos personales, con la clasificación de sus datos contenidos.

✓ Comprobantes y documentación de Comercio:

- Facturas - Si determina el cliente – Datos Intermedios
- Notas de Débito - Si determina el cliente – Datos Intermedios
- Notas de Crédito - Si determina el cliente – Datos Intermedios
- Remitos - Si determina el cliente – Datos Intermedios
- Cupones de Tarjeta de Crédito / Debito. - Si determina el cliente – Datos Intermedios

✓ Comprobantes Internos:

- Órdenes de Pago (Si determina el Cliente) - Datos Intermedios
- Órdenes de Fabricación (Si determina el Cliente) - Datos Intermedios
- Legajos de Clientes - Datos Intermedios
- Asientos Diarios - Datos Intermedios
- Papeles de Trabajo que determinan Clientes. - Datos Intermedios

La información contenida en los comprobantes y documentación de comercio con la identificación de los clientes o proveedores, es considerada intermedia porque con los datos contenidos en los mismos se pueden determinar el ingreso y el consumo de los mismos, sus gustos y preferencias por determinados productos o marcas, entre otras cosas.

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

Con respecto a las Bases de Datos existentes en una empresa, encontramos:

- ✓ Relacionados con los empleados:
  - Legajos Personales. - Datos Sensibles
  - Recibos de Sueldos y Jornales. - Datos Intermedios
  - Declaraciones Juradas. - Datos Intermedios
  - Formularios de Contribuciones Sociales. - Datos Sensibles

- ✓ Relacionados con otras personas físicas y jurídicas:
  - Sistemas de órdenes de compra / ordenes de pago.
  Si determina el cliente – Datos Intermedios
  - Facturas, Nota debito / Crédito, Remitos, etc.
  Si determina el cliente – Datos Intermedios

En el caso de las bases de datos con información de sus empleados, están conformados por datos intermedios y sensibles, que son utilizados para confeccionar declaraciones juradas, aportes y contribuciones, asignaciones familiares, entre otros.
Como se aclaró precedentemente, en las organizaciones existen numerosas bases de datos con información personal para confeccionar diversos informes, que deberían estar registradas en la DNPDP. No se debería considerar únicamente como una obligación, sino también como una ventaja competitiva en el manejo de la información.

5. Derecho de los titulares de los Datos

Los titulares de la información, en el caso de un sistema de información en una empresa comercial, corresponderían a los clientes, proveedores y empleados, los cuales tienen derechos establecidos en el artículo 13. Citado artículo establece que "*toda persona puede solicitar información al organismo de control relativa a la existencia de archivos, registros, bases o*

bancos de datos personales, sus finalidades y la identidad de sus responsables."[8]

El registro llevado al efecto por la Dirección Nacional de Protección de Datos Personales será de consulta pública y gratuita.

Los titulares de la información tienen derecho al acceso de la información:

"1. El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes.

2. El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente.

Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data prevista en esta ley.

3. El derecho de acceso a que se refiere este artículo sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto.

4. El ejercicio del derecho al cual se refiere este artículo en el caso de datos de personas fallecidas le corresponderá a sus sucesores universales. "[9]

5.1. Responsabilidades de los usuarios de las Bases de Datos

Como se citó en sección anterior, la ley 25326 específica que los particulares que formen archivos, registros o banco de datos que no sean para un uso exclusivamente personal *deberán estar adecuadamente registrados*.

En la emisión, confección y posterior conservación de la documentación respaldatoria de los Sistemas de Información Contable, 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;

[8] Infoleg (2010), "Ley de 25326 de Habeas Data, Artículo 13" accedido desde www.infoleg.gov.ar

[9] Infoleg (2010), "Ley de 25326 de Habeas Data, Artículo 14" accedido desde www.infoleg.gov.ar

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." [10]

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.

6. Servicios de Tercerización de Base de Datos

Las empresas se dedicadas a tercerización, o servicios integrados correspondientes a otras empresas en procesamientos de datos, como por ejemplo, facturación, liquidación de sueldos, deben registrar en la DNPDP sus bases de datos porque trabajan con información personal perteneciente a otras empresas.

El artículo 25, trata exclusivamente la Prestación de servicios informatizados de datos personales, el cual establece:

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

2. Una vez cumplida la prestación contractual los datos personales tratados deberán ser destruidos, salvo que medie autorización expresa de aquel por

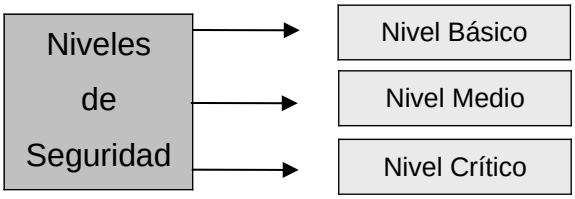
[10] Infoleg (2010), "Ley de 25326 de Habeas Data, Artículo 21" accedido desde www.infoleg.gov.ar

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."[11]

7. 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 consultar de la página web indicada en la bibliografía del presente trabajo, la resolución completa Nº 11/2006 de la DNPDP.



Cuadro Nº4

[11] Infoleg (2010), "Ley de 25326 de Habeas Data, Artículo 25" accedido desde www.infoleg.gov.ar

• MEDIDAS DE SEGURIDAD DE NIVEL BASICO:[12]

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.

[12] Infoleg (2010), “Disposición 11/2006, Medidas de Seguridad de Nivel Básico” accedido desde www.infoleg.gov.ar

• MEDIDAS DE SEGURIDAD DE NIVEL MEDIO:[13]

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:[14]

Los archivos, registros, bases y bancos de datos que contengan datos personales, definidos como "datos sensibles", con la excepción que se

[13] Infoleg (2010), “Disposición 11/2006, Medidas de Seguridad de Nivel Medio” accedido desde www.infoleg.gov.ar

[14] Infoleg (2010), “Disposición 11/2006, Medidas de Seguridad de Nivel Crítico” accedido desde www.infoleg.gov.ar

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.

8. Conclusiones

En el desarrollo el presente trabajo, he pretendido contribuir con la difusión de la Ley de Protección de Datos Personales y la aplicación de las diferentes disposiciones de la Dirección Nacional de Protección de Datos Personales

en el Sistema de Información Contable, ya que gran parte de los Contadores Públicos desconocen la incidencia en este ámbito de actuación.

La ley establece 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. La información contenida en los sistemas contables no es exclusivamente para uso interno, ya que las empresas utilizan estos datos para realizar diversos informes como: Estados Contables, informes de Responsabilidad Social Empresaria, reportes de marketing, etc., distribuidos usuarios, sucursales o holding al cual pertenecen.

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.

Cabe destacar que el incumplimiento de estos requisitos establecidos en la legislación, dará lugar a sanciones administrativas previstas en la ley. Asimismo creo que no se debería considerarse exclusivamente como una nueva obligación de las organizaciones, sino como una ventaja competitiva en el manejo de la información.

8. Bibliografía

Congreso de la Nación Argentina (2010), “Constitución Nacional Argentina” accedido de http://www.senado.gov.ar/web/interes/constitucion/capitulo2.php

Dirección Nacional de Protección de Datos Personales (2010), “Funciones del DNPDP” accedido de http://www.jus.gov.ar/dnpdp/

Infoleg (2010), “Ley de 25326 de Habeas Data” accedido desde www.infoleg.gov.ar

Infoleg (2010), “Disposición 11/2006, Medidas de Seguridad de Nivel Básico” accedido desde www.infoleg.gov.ar_

Silvia Iglesias, “La seguridad de los datos Personales: Obligación Legal y Oportunidad Competitiva”, 21/05/2009, CPCECABA.

Suarez Kimura, E – Scavone G. (2002) “El Comercio Electrónico analizado desde la Perspectiva Contable”. Editorial La Ley. Buenos Aires.