NUESTRAS INCUMBENCIAS PROFESIONALES EN LA NORMATIVA SOBRE LA PROTECCIÓN DE DATOS PERSONALES

Área VII: EDUCACION Y POLITICA PROFESIONAL

1) Normas nacionales e internacionales de educación contable.

a) Desarrollo de competencias. Cuáles y cómo.

Autores:
Silvia Iglesias siglesias@itsb.com.ar 011 - 52380707 - 1566710928
Ángel Pozzi apozzi43@hotmail.com 011 - 47905636 - 1557355860

19º Congreso Nacional de Profesionales en Ciencias Económicas.

Bicentenario de la Creación de la Bandera - 1812/2012

“Una profesión sólida se construye desde nuestra historia”

Ciudad de Mendoza, del 17 al 19 de octubre de 2012.

NUESTRAS INCUMBENCIAS PROFESIONALES EN LA NORMATIVA SOBRE LA PROTECCIÓN DE DATOS PERSONALES

INDICE

1.	Introducción
2.	La ley de Protección de Datos Personales
3	Incumbencias profesionales afectadas
4	Inscripción y renovación de bases públicas y privadas
5	Seguridad
6	Licitud en el tratamiento
7	Información al titular del tratamiento y destino de los datos
8	Solicitud del consentimiento para su tratamiento
9	Confidencialidad
10	Cesión
11	Transferencia de datos al exterior
12	Acceso de los datos por el titular
13	Capacitación
14	Bases públicas
15.	Conclusión
16	Bibliografía
17	Anexos
17.1	Ley 25.326, concordada con la Reglamentación (Arts. 1 a 28)
17.2	Disposición Normativa 11/2006 DNPDP

NUESTRAS INCUMBENCIAS PROFESIONALES EN LA NORMATIVA SOBRE LA PROTECCIÓN DE DATOS PERSONALES

1. INTRODUCCIÓN

La existencia de normas legales, como la de Protección de Datos Personales, desarrollada en el presente estudio que, incluyen incumbencias propias de nuestra profesión, sin la expresa mención de quienes pueden efectuar la tarea.

Dicha omisión, voluntaria o no, genera la realización de las mismas por terceros sin la adecuada y legal formación profesional, en deterioro de la prestación y de la sociedad.

Entendemos que la defensa de las mismas debe efectuarse por medio de nuestra Federación, para lograr la modificación de las normas legales, en este caso la ley 25.326, como así también su decreto reglamentario y disposiciones del organismo de control, creado al efecto, que contienen incumbencias exclusivas de nuestras profesiones y se prohíba su realización por terceros.

Todas las normas legales mencionadas en el presente trabajo, se encuentran en el anexo, del trabajo.

2. LA LEY DE PROTECCIÓN DE DATOS PERSONALES

La ley 25. 326, de Protección de Datos Personales, fue sancionada el 4 de octubre de 2000 y promulgada parcialmente el 30 de octubre de 2000, por el Poder Ejecutivo Nacional.

La ley 25.326, fue reglamentada por el Poder Ejecutivo Nacional el 29 de noviembre de 2011.

El organismo de aplicación es la Dirección Nacional de Protección de Datos Personales (DNPDP), creada por la norma legal, antes mencionada.

El objetivo de la ley, tal como se señala en su artículo 1°, es la protección de datos personales, asentados en archivos, registros, banco de datos u otros medios, públicos o privados destinados a dar informes, garantizando la intimidad de las personas, sean humanas o jurídicas y el acceso a ellos.

En adelante, la palabra archivo, según el Art. 2 de la Ley comprende, indistintamente, al conjunto de datos personales, organizados, que sean objeto de tratamiento o procesamiento electrónico o no, cualquiera sea la modalidad de su formación, almacenamiento, organización o acceso.

El concepto de archivo, es clarificado, en la reglamentación señalando que, son todos aquellos que exceden el uso personal, como así también su cesión o transferencias, independientemente que sea a título oneroso o gratuito-

Por todo lo expuesto, es importante señalar que, en nuestra tarea profesional, tenemos información que se encuentra comprendida en las normas de la presente ley, por lo cual estamos obligados a cumplir las disposiciones de la ley de Protección de Datos Personales y también, en general, nuestros clientes.

En su artículo 2°, la norma define ciertos vocablos , tales como datos personales, datos sensibles, archivo, registro, base o banco de datos, tratamiento de datos, responsable del archivo, etc., que son mencionados en los restantes artículos de la misma.

Nuestras incumbencias, en lo referente a las normas legales, relacionadas con la ley de protección de datos personales, se reflejan en lo siguientes tópicos:

1. Inscripción y renovación de Bases Públicas y Privadas
2. Seguridad
3. Licitud en el tratamiento
4. Información al titular del tratamiento y destino de los datos, incluyendo si serán cedidos o transferidos
5. Consentimiento sobre su Tratamiento
6. Confidencialidad
7. Cesión.
8. Transferencias de datos al exterior

9. Acceso de los titulares a los datos almacenados
10. Rectificación y actualización de los datos
11. Supresión de los datos en las bases
12. Capacitación

3. INCUMBENCIAS PROFESIONALES AFECTADAS

A nuestro entender la ley de protección de datos personales y su reglamentación, al no individualizar que profesión debe realizar ciertas tareas, permite que individuos, sin el conocimiento adecuado, explotando el vacío señalado, realicen las mismas, perjudicando a la sociedad, al no estar debidamente preparados científicamente para ello.

Las profesiones afectadas son, principalmente las de los contadores públicos y los licenciados en administración.

La ley 20.488, en su artículo 13, en lo referido a los contadores públicos y el siguiente para los licenciados en administración, norman las incumbencias exclusivas de nuestra profesión.

Las tareas que no son respetadas, por las normas legales referidas a la Protección de Datos Personales, son las siguientes:

ARTÍCULO 13.- Se requerirá título de Contador Público o equivalente:

a) En materia económica y contable cuando los dictámenes sirvan a fines judiciales, administrativos o estén destinados a hacer fe pública en relación con las cuestiones siguientes:

4.-Organización contable de todo tipo de entes.

5.-Elaboración e implantación de políticas, sistemas, métodos y procedimientos de trabajo administrativo-contable.

6.-Aplicación e implantación de sistemas de procesamiento de datos y otros métodos en los aspectos contables y financieros del proceso de información gerencial.

10.-Intervención conjuntamente con letrados en los contratos y estatutos de toda clase de sociedades civiles y comerciales cuando se planteen cuestiones de carácter financiero, económico, impositivo y contable.

ARTÍCULO 14.- Se requerirá título de Licenciado en Administración o equivalente:

a) Para todo dictamen destinado a ser presentado ante autoridades judiciales, administrativas o a hacer fe pública en materia de dirección y administración para el asesoramiento en:

1.-Las funciones directivas de análisis, planeamiento, organización, coordinación y control.

2.-la elaboración e implantación de políticas, sistemas, métodos y procedimientos de administración, finanzas, comercialización, presupuestos, costos y administración de personal.

3.-La definición y descripción de la estructura y funciones de la organización.

4.-La aplicación e implantación de sistemas de procesamiento de datos y otros métodos en el proceso de información gerencial.

5.-Lo referente a relaciones industriales, sistemas de remuneración y demás aspectos vinculados al factor humano en la empresa.

6.-Toda otra cuestión de dirección o administración en material económica y financiera con referencia a las funciones que le son propias de acuerdo con el presente artículo.

4. INSCRIPCIÓN Y RENOVACIÓN DE BASES PÚBLICAS Y PRIVADAS

Las tareas comprendidas en este acápite se encuentran desarrolladas en los artículos 3, y 21 a 28, de la ley y su correlación con el decreto reglamentario.

El artículo 3°, se refiere a la validez (licitud) l egal de los archivos de datos, partiendo que para ello deben estar inscriptos, en la Dirección Nacional de Protección de Datos Personales, cumpliendo con todas las disposiciones de la ley y sus reglamentaciones.

En nuestra tarea profesional, tenemos acceso a archivos, con información incluida en esta ley, nos preguntamos ¿Cómo auditor, en mi dictamen sobre los estados

contables, debo manifestar, si el cliente no cumple con las normas sobre protección de datos personales, al no considerársela lícita?

Existen, dos posturas, una mayoritaria, opina que el dictamen es sobre la razonabilidad de los estados contables y por consiguiente, si se cumple con dicho precepto, aun incumpliendo con las normas legales, sobre protección de datos personales, el informe no debe contener salvedades. En este caso, en la carta de control interno, debe mencionarse, si existiese, el incumplimiento, debido a las sanciones que pudiese recibir el cliente.

La minoritaria expresa, si el archivo, de los datos contables, no se encuentra inscripto o no cumple con las disposiciones legales, el dictamen sobre los estados contables debe emitirse, con salvedades.

Participamos de la opinión mayoritaria.

Los artículos 21 a 28, con su correspondiente reglamentación se refieren a la inscripción de los archivos de datos, a los archivos públicos, a los archivos privados, a ciertos supuestos especiales, prestación de servicios por medio de archivos informatizados, prestación de servicios de información crediticia, archivos con fines publicitarios y archivos para encuestas.

Del análisis de estos artículos surgen las siguientes tareas, que estarían alcanzadas por la incumbencia exclusiva de profesionales, en ciencias económicas:

- Identificación de los archivos o base de datos
- Normalización de las bases de datos
- Identificación del tratamiento desde su captura o colección hasta su destrucción
- Contratación de terceros para su tratamiento
- Identificación de los soportes
- Identificación de la licitud (validez) para el pedido de datos y su tratamiento
- Adecuación según el tipo de tratamiento
- Identificación de lass Cesiones
- Adecuación según el tipo de dato
- Creación de las bases, tanto públicas, como privadas

5. SEGURIDAD

La ley de Protección de Datos Personales, en su artículo 9, obliga a que los archivos de datos cuenten con la debida seguridad, adoptando las medidas técnicas y organizativas para ello.

La Dirección Nacional de Protección de Datos Personales, dictó la resolución 11/2006 - "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", estableciendo tres niveles de seguridad (básico, medio y crítico), aplicable a los archivos informáticos o manuales, según se detalla en el anexo 2, de esta presentación.

Esta disposición establece que, los archivos que contengan datos personales, para su tratamiento, deben estar respaldados, por documentación que muestre los procedimientos y medidas de seguridad aplicables a los mismos, debiendo estar en todo momento debidamente actualizada, como así también la información mínima que debe contener, tales como rutinas de control (ingreso sólo de información autorizada), respaldo, defensa ante accesos no autorizados (accesos restringidos, virus, etc.), identificación de los usuarios autorizados (control de contraseñas, etc.), identificación del responsable de seguridad, realización de auditorías, etc..

La función del profesional en ciencias económicas, es desarrollar el documento de seguridad con Implementación a los procesos y procedimientos detallados con controles que aseguren la integridad, confidencialidad y disponibilidad de los datos de todo el ciclo de vida de los datos en proceso y soportes corpóreos o no corpóreos, y esto es de exclusiva incumbencia de los contadores y licenciados en administración y en la auditoría de cumplimiento es incumbencia de los primeros.

6. LICITUD EN EL TRATAMIENTO

La licitud del tratamiento se refiere a la calidad de los datos (artículo 4), a su categorización (artículo 7) y a los datos relativos a la salud (artículo 8).

El artículo 4°, señala que los datos a tratar deben ser válidos, sólo pueden obtenerse por medios legales; no pueden usarse para finalidades distintas a las de su obtención; los datos deben estar actualizados en forma permanente; los datos erróneos deben eliminarse; el titular debe tener acceso permanente a ellos; cuando dejen de ser usados, por innecesarios o por cumplirse el objetivo para el cual fueron colectados,

deben destruirse. En su reglamentación, establece que para determinar la buena fe de la recolección de datos, se hace indispensable partir de procedimientos escritos. La DNPDP está autorizada a efectuar auditorías de cumplimiento, sobre la legalidad del medio de recolección y tratamiento de los datos, verificando la existencia de normas internas de control interno, dictadas al efecto.

Con respecto a la categorización, la norma establece, que las personas no están obligadas a brindar datos sensibles. Estos datos sólo pueden ser colectados y objeto de tratamiento, sólo cuando existe una norma legal que lo autorice y sea de beneficio al interés general. Cuando esos datos se utilicen para fines estadísticos o científicos, los mismos deben ser innominados. Expresa que está prohibida la formación de archivos, que revelen datos sensibles, señalando las excepciones a este requisito.

Con relación a los datos de la salud, autoriza a los entes que participan de las ciencias de la salud, a guardar la información sobre sus pacientes, bajo estricto secreto profesional. Esto es sólo factible, si se cuenta con procedimientos o normas de control de dicha información.

Por lo expuesto anteriormente, no cabe ninguna duda que, esta temática requiere la participación de profesionales en ciencias económicas, ya que las normas sobre controles y seguridad de la información es una incumbencia de ellos, con la asistencia letrada, para verificar el cumplimiento de todas las regulaciones

7. INFORMACIÓN AL TITULAR DEL TRATAMIENTO Y DESTINO DE LOS DATOS

Por aplicación del artículo 6° de la ley, al titular de los datos se le debe informar, en forma precisa, la finalidad porque se colectan los datos y su tratamiento; su tratamiento por terceros, si ello ocurriese; la existencia del archivo, que se trate y la identificación del responsable (nombre y domicilio) de los mismos; si es de carácter facultativo u obligatorio, la provisión de los mismos; las consecuencias aplicables al titular, si provee los datos, si se niega a hacerlo o lo hace con errores.

Esta normativa, obliga a que el depositario de los datos deba establecer procedimientos que aseguren la privacidad de la información, en el formulario (digital o en papel) en el cual se colecta la información y en el sitio donde se colectan los datos (archivos temporarios o finales).

El establecer procedimientos es una incumbencia propia de los profesionales en ciencias económicas, por aplicación de los artículos 13 y 14, de la ley 20.488, que rige dicha profesión.

8. SOLICITUD DEL CONSENTIMIENTO PARA SU TRATAMIENTO

El artículo 5° de la ley de Protección de Datos Personales establece que, es ilícito el tratamiento de los datos personales, sin el consentimiento previo, libre, por escrito o por cualquier medio que asegure su autoría y autenticidad, previa autorización de la DNPDP. Asimismo, informa las excepciones.

La reglamentación del artículo antes mencionado, señala que el consentimiento, debe estar precedido de una explicación a su titular, en forma adecuada a su nivel cultural y social, de lo establecido en el artículo 6 de la norma en tratamiento.

El consentimiento es revocable, pero no retroactivo-

Por lo expuesto se obliga a que el depositario de los datos deba establecer procedimientos que aseguren la existencia del consentimiento del titular de los datos, en un todo de acuerdo con el presente artículo, en el formulario (digital o en papel) en el cual se colecta la información y en el sitio donde se colectan los datos (archivos temporarios o finales).

El establecer procedimientos es una incumbencia propia de los profesionales en ciencias económicas, por aplicación de los artículos 13 y 14, de la ley 20.488, que rige dicha profesión, esta tarea debe efectuarse con asistencia letrada, por el texto de los consentimientos.

9. CONFIDENCIALIDAD

El deber de confidencialidad de los datos, se encuentra normado en el artículo 10, en donde establece que, el responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos, dicha obligación permanece en el tiempo aun después de finalizada su relación con el titular del archivo de datos, Incluye también las excepciones.

Para ello, se requiere desarrollar procedimientos específicos para asegurar la confidencialidad de los datos, en todo su proceso, incluso cuando se cedan o permitan el acceso, competencia de nuestras profesiones, debiendo, además, recurrirse a la asesoría letrada para los acuerdos de confidencialidad.

10. CESIÓN

Los datos personales, sólo pueden ser transferidos o cedidos si, se lo requiere para cumplir con el objetivo para el cual han sido colectados, siempre y cuando tengan el consentimiento previo de su titular, identificando al cesionario, según reza el artículo 10 de la ley, debiendo cumplir lo normado en el artículo 5 de la ley. Asimismo, establece, también, las excepciones.

El cesionario está alcanzado por todas las responsabilidades que le son aplicables al cedente y ambos responden en forma solidaria.

Esta acción debe tener normas claras, establecidas por procedimientos administrativos y contables, propio de nuestras profesiones, especialmente para la disociación de datos, que debe hacer inidentificable a su titular. La disociación de datos sólo puede efectuarse bajo las normas de seguridad que debe dictar la DNPDP.

Dado que debe existir un contrato entre el cedente y cesionario, es conveniente contar con una adecuada asesoría letrada, para este punto específicamente.

11. TRANSFERENCIA DE DATOS AL EXTERIOR

La transferencia de datos al exterior, ya sea, a organismos internacionales, regionales o mundiales, como así también a otros países, sólo pueden ser efectuados, si se realizan bajo niveles de protección adecuados, según lo establece el artículo 12 de la norma.

Los niveles de protección son aplicables, en donde se originan los datos personales y también en el receptor de ellos.

Es de señalar que la norma y su reglamentación indican las excepciones-

Los niveles de seguridad deben surgir de procedimientos y contratos entre las partes, por ello, encontramos nuevamente nuestra incumbencia profesional, con la asistencia letrada, en la confección del contrato.

12. ACCESO A LOS DATOS POR EL TITULAR

Los titulares de datos personales, de acuerdo con el artículo 14, tienen que tener acceso a los datos almacenados, en los bancos de datos, ya sean públicos o privados; por el artículo 15 deben conocer la información contenida en dichos archivos y el artículo 16, indica la posibilidad del titular de modificar, suprimir o incorporar datos, a los existentes.

La reglamentación, del artículo 14 establece las formas para acceder a la información existente, pero con la garantía que sea el titular, el que lo solicita. Además norma sobre lo que el derecho de acceso significa.

Por aplicación del artículo 15, la información suministrada debe ser de fácil identificación por el titular, es decir, simple, sin codificaciones y completa. Establece, además, en su reglamentación, los medios alternativos para el conocimiento de la información contenida en el archivo.

El siguiente artículo, con su reglamentación, establece el derecho del titular de los datos, a su modificación, eliminación, supresión y el poder solicitar su confidencialidad.

Lo expresado en estos artículos, conlleva la necesidad de tener procedimientos específicos, elaborados por profesionales en Ciencias Económicas, en cada uno de los responsables de la custodia del archivo de datos personales.

13. CAPACITACIÓN

Todo lo relacionado con los artículos precedentes requiere una capacitación del personal a cargo de cada una de las tareas mencionadas, que debe estar a cargo de personal idóneo para ello o sea con profesionales, con incumbencia legal en la materia, en algunos casos, es necesario la participación de profesionales del derecho, limitada, a la legalidad, por ejemplo, de los contratos o acuerdos.

14. BASES PÚBLICAS

Las bases públicas deben contar con un Comité de Seguridad de la Información, siguiendo la normativa de la ONTI, decisión administrativa 669/2004, que adolece del error de no asignar a profesionales competentes, con incumbencia legal, los puestos funcionales jerárquicos, o sea, profesionales en ciencias económicas.

15 CONCLUSIÓN

Es imprescindible, que los profesionales en ciencias económicas, en las normas de protección de datos personales, específicamente, los licenciados en administración y los contadores públicos, tomemos conciencia para evitar que otras profesiones, con nivel universitario o sin él, realicen labores que, legalmente, nos competen, en desmedro de nuestra sociedad.

Es necesario que, nuestra Federación, realice todas las tareas necesarias, para que, en las normas relacionadas con la Protección de Datos Personales, requiera de las autoridades correspondientes, se especifique, en las disposiciones aplicables, nuestras incumbencias.

16. BIBLIOGRAFÍA

- Iglesias, S. – Ley 25.326, concordada con su reglamentación
- Comisión de Estudio sobre Sistemas de Registro, su Integridad y Autenticidad Documental (CPCECABA) – Cuadro de Incumbencias Profesionales y la Ley de Protección de Datos Personales
- Iglesias S. – Cuaderno N° 58 (CPCECABA) – Ley 25,3 26 – Ley de Protección de Datos Personales (Habeas Data)

17. ANEXO

17.1. Ley 25.326, concordada con la Reglamentación (Arts. 1 a 28)

En letra cursiva, se encuentra identificada la reglamentación. Sólo se transcriben los artículos mencionados en la presentación.

CAPÍTULO I

DISPOSICIONES GENERALES

ARTICULO 1°— (Objeto).

La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.

Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal.

En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas.

ARTICULO 1º.- A los efectos de esta reglamentación, quedan comprendidos en el concepto de archivos, registros, bases o bancos de datos privados destinados a dar informes, aquellos que exceden el uso exclusivamente personal y los que tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito.

ARTICULO 2°— (Definiciones).

A los fines de la presente ley se entiende por:

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

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

— Archivo, registro, base o banco de datos: 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.

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

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

— **Datos informatizados:** Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.

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

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

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

Capítulo II

Principios generales relativos a la protección de datos

ARTICULO 3° — (Archivos de datos – Licitud).

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.

Los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública.

ARTICULO 4° — (Calidad de los datos).

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.

ARTICULO 4º.- Para determinar la lealtad y buena fe en la obtención de los datos personales, así como el destino que a ellos se asigne, se deberá analizar el procedimiento efectuado para la recolección y, en particular, la información que se haya proporcionado al titular de los datos de acuerdo con el artículo 6º de la Ley Nº 25.326.

Cuando la obtención o recolección de los datos personales fuese lograda por interconexión o tratamiento de archivos, registros, bases o bancos de datos, se deberá analizar la fuente de información y el destino previsto por el responsable o usuario para los datos personales obtenidos.

El dato que hubiera perdido vigencia respecto de los fines para los que se hubiese obtenido o recolectado debe ser suprimido por el responsable o usuario sin necesidad de que lo requiera el titular de los datos.

La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES efectuará controles de oficio sobre el cumplimiento de este principio legal, y aplicará las sanciones pertinentes al responsable o usuario en los casos que correspondiere.

La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES procederá, ante el pedido de un interesado o de oficio ante la sospecha de una ilegalidad, a verificar el

cumplimiento de las disposiciones legales y reglamentarias en orden a cada una de las siguientes etapas del uso y aprovechamiento de datos personales:

a) legalidad de la recolección o toma de información personal;

b) legalidad en el intercambio de datos y en la transmisión a terceros o en la interrelación entre ellos;

c) legalidad en la cesión propiamente dicha;

d) legalidad de los mecanismos de control interno y externo del archivo, registro, base o banco de datos.

ARTICULO 5°— (Consentimiento).

1. 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.

El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6° de la presente ley.

2. 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.

ARTICULO 5º.- El consentimiento informado es el que está precedido de una explicación, al titular de los datos, en forma adecuada a su nivel social y cultural, de la información a que se refiere el artículo 6º de la Ley Nº 25.326.

La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES establecerá los requisitos para que el consentimiento pueda ser prestado por un medio distinto a la forma escrita, el cual deberá asegurar la autoría e integridad de la declaración.

El consentimiento dado para el tratamiento de datos personales puede ser revocado en cualquier tiempo. La revocación no tiene efectos retroactivos.

A los efectos del artículo 5º, inciso 2 e), de la Ley Nº 25.326 el concepto de entidad financiera comprende a las personas alcanzadas por la Ley Nº 21.526 y a las empresas emisoras de

tarjetas de crédito, los fideicomisos financieros, las ex entidades financieras liquidadas por el BANCO CENTRAL DE LA REPUBLICA ARGENTINA y los sujetos que expresamente incluya la Autoridad de Aplicación de la mencionada Ley.

No es necesario el consentimiento para la información que se describe en los incisos a), b), c) y d) del artículo 39 de la Ley Nº 21.526.

En ningún caso se afectará el secreto bancario, quedando prohibida la divulgación de datos relativos a operaciones pasivas que realicen las entidades financieras con sus clientes, de conformidad con lo dispuesto en los artículos 39 y 40 de la Ley Nº 21.526.

ARTICULO 6° — (Información).

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

a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios;

b) 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;

c) 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;

d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos;

e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

ARTICULO 7°— (Categoría de datos).

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.

ARTICULO 8°— (Datos relativos a la salud).

Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional.

ARTICULO 9° — (Seguridad de los datos).

1. 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.

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

ARTICULO 9º.- La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES promoverá la cooperación entre sectores públicos y privados para la elaboración e implantación de medidas, prácticas y procedimientos que susciten la confianza en los sistemas de información, así como en sus modalidades de provisión y utilización.

ARTICULO 10. — (Deber de confidencialidad).

1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos.

2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

ARTICULO 11. — (Cesión).

1. Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo.

2. El consentimiento para la cesión es revocable.

3. El consentimiento no es exigido cuando:

a) Así lo disponga una ley;

b) En los supuestos previstos en el artículo 5° inc iso 2;

c) Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias;

d) Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados;

e) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables.

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

ARTICULO 11.- Al consentimiento para la cesión de los datos le son aplicables las disposiciones previstas en el artículo 5º de la Ley Nº 25.326 y el artículo 5º de esta reglamentación.

En el caso de archivos o bases de datos públicas dependientes de un organismo oficial que por razón de sus funciones específicas estén destinadas a la difusión al público en general, el requisito relativo al interés legítimo del cesionario se considera implícito en las razones de interés general que motivaron el acceso público irrestricto.

La cesión masiva de datos personales de registros públicos a registros privados sólo puede ser autorizada por ley o por decisión del funcionario responsable, si los datos son de acceso público y se ha garantizado el respeto a los principios de protección establecidos en la Ley Nº 25.326. No es necesario acto administrativo alguno en los casos en que la ley disponga el acceso a la base de datos pública en forma irrestricta. Se entiende por cesión masiva de datos personales la que comprende a un grupo colectivo de personas.

La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES fijará los estándares de seguridad aplicables a los mecanismos de disociación de datos.

El cesionario a que se refiere el artículo 11, inciso 4, de la Ley Nº 25.326, podrá ser eximido total o parcialmente de responsabilidad si demuestra que no se le puede imputar el hecho que ha producido el daño.

ARTICULO 12. — (Transferencia internacional).

1. Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados.

2. La prohibición no regirá en los siguientes supuestos:

a) Colaboración judicial internacional;

b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto se realice en los términos del inciso e) del artículo anterior;

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

d) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte;

e) Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

ARTICULO 12.- La prohibición de transferir datos personales hacia países u organismos internacionales o supranacionales que no proporcionen niveles de protección adecuados, no rige cuando el titular de los datos hubiera consentido expresamente la cesión.

No es necesario el consentimiento en caso de transferencia de datos desde un registro público que esté legalmente constituido para facilitar información al público y que esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones legales y reglamentarias para la consulta.

Facúltase a la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES a evaluar, de oficio o a pedido de parte interesada, el nivel de protección proporcionado por las normas de un Estado u organismo internacional. Si llegara a la conclusión de que un Estado u organismo no protege adecuadamente a los datos personales, elevará al PODER EJECUTIVO NACIONAL un proyecto de decreto para emitir tal declaración. El proyecto deberá ser refrendado por los Ministros de Justicia y Derechos Humanos y de Relaciones Exteriores, Comercio Internacional y Culto.

El carácter adecuado del nivel de protección que ofrece un país u organismo internacional se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración de tratamiento o de los tratamientos previstos, el lugar de destino final, las normas de derecho, generales o sectoriales, vigentes en el país de que se trate, así como las normas profesionales, códigos de conducta y las medidas de seguridad en vigor en dichos lugares, o que resulten aplicables a los organismos internacionales o supranacionales.

Se entiende que un Estado u organismo internacional proporciona un nivel adecuado de protección cuando dicha tutela se deriva directamente del ordenamiento jurídico vigente, o de sistemas de autorregulación, o del amparo que establezcan las cláusulas contractuales que prevean la protección de datos personales.

Capítulo III

DERECHOS DE LOS TITULARES DE DATOS

ARTICULO 13. — (Derecho de Información).

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.

El registro que se lleve al efecto será de consulta pública y gratuita.

ARTICULO 14. — (Derecho de acceso).

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.

ARTICULO 14.- La solicitud a que se refiere el artículo 14, inciso 1, de la Ley Nº 25.326, no requiere de fórmulas específicas, siempre que garantice la identificación del titular. Se puede efectuar de manera directa, presentándose el interesado ante el responsable o usuario del archivo, registro, base o banco de datos, o de manera indirecta, a través de la intimación

fehaciente por medio escrito que deje constancia de recepción. También pueden ser utilizados otros servicios de acceso directo o semidirecto como los medios electrónicos, las líneas telefónicas, la recepción del reclamo en pantalla u otro medio idóneo a tal fin. En cada supuesto, se podrán ofrecer preferencias de medios para conocer la respuesta requerida.

Si se tratara de archivos o bancos de datos públicos dependientes de un organismo oficial destinados a la difusión al público en general, las condiciones para el ejercicio del derecho de acceso podrán ser propuestas por el organismo y aprobadas por la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, la cual deberá asegurar que los procedimientos sugeridos no vulneren ni restrinjan en modo alguno las garantías propias de ese derecho.

El derecho de acceso permitirá:

a) conocer si el titular de los datos se encuentra o no en el archivo, registro, base o banco de datos;

b) conocer todos los datos relativos a su persona que constan en el archivo;

c) solicitar información sobre las fuentes y los medios a través de los cuales se obtuvieron sus datos;

d) solicitar las finalidades para las que se recabaron;

e) conocer el destino previsto para los datos personales;

f) saber si el archivo está registrado conforme a las exigencias de la Ley Nº 25.326.

Vencido el plazo para contestar fijado en el artículo 14, inciso 2 de la Ley Nº 25.326, el interesado podrá ejercer la acción de protección de los datos personales y denunciar el hecho ante la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES a los fines del control pertinente de este organismo.

En el caso de datos de personas fallecidas, deberá acreditarse el vínculo mediante la declaratoria de herederos correspondiente, o por documento fehaciente que verifique el carácter de sucesor universal del interesado.

ARTICULO 15. — (Contenido de la información).

1. La información debe ser suministrada en forma clara, exenta de codificaciones y en su caso acompañada de una explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen.

2. La información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento sólo comprenda un aspecto de los datos personales. En ningún caso el informe podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con el interesado.

3. La información, a opción del titular, podrá suministrarse por escrito, por medios electrónicos, telefónicos, de imagen, u otro idóneo a tal fin.

ARTICULO 15.- El responsable o usuario del archivo, registro, base o banco de datos deberá contestar la solicitud que se le dirija, con independencia de que figuren o no datos personales del afectado, debiendo para ello valerse de cualquiera de los medios autorizados en el artículo 15, inciso 3, de la Ley Nº 25.326, a opción del titular de los datos, o las preferencias que el interesado hubiere expresamente manifestado al interponer el derecho de acceso.

La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES elaborará un formulario modelo que facilite el derecho de acceso de los interesados.

Podrán ofrecerse como medios alternativos para responder el requerimiento, los siguientes:

a) visualización en pantalla;

b) informe escrito entregado en el domicilio del requerido;

c) informe escrito remitido al domicilio denunciado por el requirente;

d) transmisión electrónica de la respuesta, siempre que esté garantizada la identidad del interesado y la confidencialidad, integridad y recepción de la información;

e) cualquier otro procedimiento que sea adecuado a la configuración e implantación material del archivo, registro, base o banco de datos, ofrecido por el responsable o usuario del mismo.

ARTICULO 16. — (Derecho de rectificación, actualización o supresión).

1. Toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos.

2. El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad.

3. El incumplimiento de esta obligación dentro del término acordado en el inciso precedente, habilitará al interesado a promover sin más la acción de protección de los datos personales o de hábeas data prevista en la presente ley.

4. En el supuesto de cesión, o transferencia de datos, el responsable o usuario del banco de datos debe notificar la rectificación o supresión al cesionario dentro del quinto día hábil de efectuado el tratamiento del dato.

5. La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos.

6. Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá o bien bloquear el archivo, o consignar al proveer información relativa al mismo la circunstancia de que se encuentra sometida a revisión.

7. Los datos personales deben ser conservados durante los plazos previstos en las disposiciones aplicables o en su caso, en las contractuales entre el responsable o usuario del banco de datos y el titular de los datos.

ARTICULO 16.- En las disposiciones de los artículos 16 a 22 y 38 a 43 de la Ley Nº 25.326 en que se menciona a algunos de los derechos de rectificación, actualización, supresión y confidencialidad, se entiende que tales normas se refieren a todos ellos.

En el caso de los archivos o bases de datos públicas conformadas por cesión de información suministrada por entidades financieras, administradoras de fondos de jubilaciones y pensiones y entidades aseguradoras, de conformidad con el artículo 5º, inciso 2, de la Ley Nº 25.326, los derechos de rectificación, actualización, supresión y confidencialidad deben ejercerse ante la entidad cedente que sea parte en la relación jurídica a que se refiere el dato impugnado. Si

procediera el reclamo, la entidad respectiva debe solicitar al BANCO CENTRAL DE LA REPUBLICA ARGENTINA, a la SUPERINTENDENCIA DE ADMINISTRADORAS DE FONDOS DE JUBILACIONES Y PENSIONES o a la SUPERINTENDENCIA DE SEGUROS DE LA NACION, según el caso, que sean practicadas las modificaciones necesarias en sus bases de datos. Toda modificación debe ser comunicada a través de los mismos medios empleados para la divulgación de la información.

Los responsables o usuarios de archivos o bases de datos públicos de acceso público irrestricto pueden cumplir la notificación a que se refiere el artículo 16, inciso 4, de la Ley Nº 25.326 mediante la modificación de los datos realizada a través de los mismos medios empleados para su divulgación.

ARTICULO 17. — (Excepciones).

1. Los responsables o usuarios de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación o la supresión en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros.

2. La información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser fundada y notificada al afectado.

3. Sin perjuicio de lo establecido en los incisos anteriores, se deberá brindar acceso a los registros en cuestión en la oportunidad en que el afectado tenga que ejercer su derecho de defensa.

ARTICULO 18. — (Comisiones legislativas).

Las Comisiones de Defensa Nacional y la Comisión Bicameral de Fiscalización de los Organos y Actividades de Seguridad Interior e Inteligencia del Congreso de la Nación y la Comisión de Seguridad Interior de la Cámara de Diputados de la Nación, o las que las sustituyan, tendrán acceso a los archivos o bancos de datos referidos en el artículo 23 inciso 2 por razones fundadas y en aquellos aspectos que constituyan materia de competencia de tales Comisiones.

ARTICULO 19. — (Gratuidad).

La rectificación, actualización o supresión de datos personales inexactos o incompletos que obren en registros públicos o privados se efectuará sin cargo alguno para el interesado.

ARTICULO 20. — (Impugnación de valoraciones personales).

1. Las decisiones judiciales o los actos administrativos que impliquen apreciación o valoración de conductas humanas, no podrán tener como único fundamento el resultado del tratamiento informatizado de datos personales que suministren una definición del perfil o personalidad del interesado.

2. Los actos que resulten contrarios a la disposición precedente serán insanablemente nulos.

Capítulo IV

Usuarios y responsables de archivos, registros y bancos de datos

ARTICULO 21. — (Registro de archivos de datos. Inscripción).

1. Todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control.

2. El registro de archivos de datos debe comprender como mínimo la siguiente información:

a) Nombre y domicilio del responsable;

b) Características y finalidad del archivo;

c) Naturaleza de los datos personales contenidos en cada archivo;

d) Forma de recolección y actualización de datos;

e) Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos;

f) Modo de interrelacionar la información registrada;

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.

3) Ningún usuario de datos podrá 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 el capítulo VI de la presente ley.

ARTICULO 21.- El registro e inscripción de archivos, registros, bases o bancos de datos públicos, y privados destinados a dar información, se habilitará una vez publicada esta reglamentación en el Boletín Oficial.

Deben inscribirse los archivos, registros, bases o bancos de datos públicos y los privados a que se refiere el artículo 1º de esta reglamentación.

A los fines de la inscripción de los archivos, registros, bases y bancos de datos con fines de publicidad, los responsables deben proceder de acuerdo con lo establecido en el artículo 27, cuarto párrafo, de esta reglamentación.

ARTICULO 22. — (Archivos, registros o bancos de datos públicos).

1. Las normas sobre creación, modificación o supresión de archivos, registros o bancos de datos pertenecientes a organismos públicos deben hacerse por medio de disposición general publicada en el Boletín Oficial de la Nación o diario oficial.

2. Las disposiciones respectivas, deben indicar:

a) Características y finalidad del archivo;

b) Personas respecto de las cuales se pretenda obtener datos y el carácter facultativo u obligatorio de su suministro por parte de aquéllas;

c) Procedimiento de obtención y actualización de los datos;

d) Estructura básica del archivo, informatizado o no, y la descripción de la naturaleza de los datos personales que contendrán;

e) Las cesiones, transferencias o interconexiones previstas;

f) Organos responsables del archivo, precisando dependencia jerárquica en su caso;

g) Las oficinas ante las que se pudiesen efectuar las reclamaciones en ejercicio de los derechos de acceso, rectificación o supresión.

3. En las disposiciones que se dicten para la supresión de los registros informatizados se establecerá el destino de los mismos o las medidas que se adopten para su destrucción.

ARTICULO 23. — (Supuestos especiales).

1. Quedarán sujetos al régimen de la presente ley, los datos personales que por haberse almacenado para fines administrativos, deban ser objeto de registro permanente en los bancos de datos de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia; y aquellos sobre antecedentes personales que proporcionen dichos bancos de datos a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales.

2. El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o inteligencia, sin consentimiento de los afectados, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad.

3. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

ARTICULO 24. — (Archivos, registros o bancos de datos privados).

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.

ARTICULO 25. — (Prestación de servicios informatizados de datos personales).

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

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

ARTICULO 25.- Los contratos de prestación de servicios de tratamiento de datos personales deberán contener los niveles de seguridad previstos en la Ley Nº 25.326, esta reglamentación y las normas complementarias que dicte la DIRECCION NACIONAL DE PROTECCION DE

DATOS PERSONALES, como así también las obligaciones que surgen para los locatarios en orden a la confidencialidad y reserva que deben mantener sobre la información obtenida.

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

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

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

ARTICULO 26. — (Prestación de servicios de información crediticia).

1. En la prestación de servicios de información crediticia sólo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito, obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

2. Pueden tratarse igualmente datos personales relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial, facilitados por el acreedor o por quien actúe por su cuenta o interés.

3. A solicitud del titular de los datos, el responsable o usuario del banco de datos, le comunicará las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y domicilio del cesionario en el supuesto de tratarse de datos obtenidos por cesión.

4. Sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico-financiera de los afectados durante los últimos cinco años. Dicho plazo se reducirá a dos años cuando el deudor cancele o de otro modo extinga la obligación, debiéndose hace constar dicho hecho.

5. La prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión, ni la ulterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios.

ARTICULO 26.- A los efectos del artículo 26, inciso 2, de la Ley Nº 25.326, se consideran datos relativos al cumplimiento o incumplimiento de obligaciones los referentes a los contratos de mutuo, cuenta corriente, tarjetas de crédito, fideicomiso, leasing, de créditos en general y toda otra obligación de contenido patrimonial, así como aquellos que permitan conocer el nivel de cumplimiento y la calificación a fin de precisar, de manera indubitable, el contenido de la información emitida.

En el caso de archivos o bases de datos públicos dependientes de un organismo oficial destinadas a la difusión al público en general, se tendrán por cumplidas las obligaciones que surgen del artículo 26, inciso 3, de la Ley Nº 25.326 en tanto el responsable de la base de datos le comunique al titular de los datos las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido difundidas durante los últimos SEIS (6) meses.

Para apreciar la solvencia económico-financiera de una persona, conforme lo establecido en el artículo 26, inciso 4, de la Ley Nº 25.326, se tendrá en cuenta toda la información disponible desde el nacimiento de cada obligación hasta su extinción. En el cómputo de CINCO (5) años, éstos se contarán a partir de la fecha de la última información adversa archivada que revele que dicha deuda era exigible. Si el deudor acredita que la última información disponible coincide con la extinción de la deuda, el plazo se reducirá a DOS (2) años. Para los datos de cumplimiento sin mora no operará plazo alguno para la eliminación.

A los efectos del cálculo del plazo de DOS (2) años para conservación de los datos cuando el deudor hubiere cancelado o extinguido la obligación, se tendrá en cuenta la fecha precisa en que se extingue la deuda.

A los efectos de dar cumplimiento a lo dispuesto por el artículo 26, inciso 5, de la Ley Nº 25.326, el BANCO CENTRAL DE LA REPUBLICA ARGENTINA deberá restringir el acceso a sus bases de datos disponibles en Internet, para el caso de información sobre personas físicas, exigiendo el ingreso del número de documento nacional de identidad o código único de identificación tributaria o laboral del titular de los datos, obtenidos por el cesionario a través de una relación contractual o comercial previa.

ARTICULO 27. **— (Archivos, registros o bancos de datos con fines de publicidad).**

1. En la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento.

2. En los supuestos contemplados en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno.

3. El titular podrá en cualquier momento solicitar el retiro o bloqueo de su nombre de los bancos de datos a los que se refiere el presente artículo.

ARTICULO 27.- Podrán recopilarse, tratarse y cederse datos con fines de publicidad sin consentimiento de su titular, cuando estén destinados a la formación de perfiles determinados, que categoricen preferencias y comportamientos similares de las personas, siempre que los titulares de los datos sólo se identifiquen por su pertenencia a tales grupos genéricos, con más los datos individuales estrictamente necesarios para formular la oferta a los destinatarios.

Las cámaras, asociaciones y colegios profesionales del sector que dispongan de un Código de Conducta homologado por la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, al que por estatuto adhieran obligatoriamente todos sus miembros, junto con la Autoridad de Aplicación, implementarán, dentro de los NOVENTA (90) días siguientes a la publicación de esta reglamentación, un sistema de retiro o bloqueo a favor del titular del dato que quiera ser excluido de las bases de datos con fines de publicidad. El retiro podrá ser total o parcial, bloqueando exclusivamente, a requerimiento del titular, el uso de alguno o algunos de los medios de comunicación en particular, como el correo, el teléfono, el correo electrónico u otros.

En toda comunicación con fines de publicidad que se realice por correo, teléfono, correo electrónico, Internet u otro medio a distancia a conocer, se deberá indicar, en forma expresa y destacada, la posibilidad del titular del dato de solicitar el retiro o bloqueo, total o parcial, de su nombre de la base de datos. A pedido del interesado, se deberá informar el nombre del responsable o usuario del banco de datos que proveyó la información.

A los fines de garantizar el derecho de información del artículo 13 de la Ley Nº 25.326, se inscribirán únicamente las cámaras, asociaciones y colegios profesionales del sector que dispongan de un Código de Conducta homologado por la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, al que por estatuto adhieran obligatoriamente todos sus miembros. Al inscribirse, las cámaras, asociaciones y colegios profesionales deberán acompañar una nómina de sus asociados indicando nombre, apellido y domicilio.

Los responsables o usuarios de archivos, registros, bancos o bases de datos con fines de publicidad que no se encuentren adheridos a ningún Código de Conducta, cumplirán el deber de información inscribiéndose en el Registro a que se refiere el artículo 21 de la Ley Nº 25.326.

Los datos vinculados a la salud sólo podrán ser tratados, a fin de realizar ofertas de bienes y servicios, cuando hubieran sido obtenidos de acuerdo con la Ley Nº 25.326 y siempre que no causen discriminación, en el contexto de una relación entre el consumidor o usuario y los proveedores de servicios o tratamientos médicos y entidades sin fines de lucro. Estos datos no podrán transferirse a terceros sin el consentimiento previo, expreso e informado del titular de los datos. A dicho fin, este último debe recibir una noticia clara del carácter sensible de los datos que proporciona y de que no está obligado a suministrarlos, junto con la información de los artículos 6º y 11, inciso 1, de la Ley Nº 25.326 y la mención de su derecho a solicitar el retiro de la base de datos.

ARTICULO 28. — (Archivos, registros o bancos de datos relativos a encuestas).

1. Las normas de la presente ley no se aplicarán a las encuestas de opinión, mediciones y estadísticas relevadas conforme a Ley 17.622, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, en la medida que los datos recogidos no puedan atribuirse a una persona determinada o determinable.

2. Si en el proceso de recolección de datos no resultara posible mantener el anonimato, se deberá utilizar una técnica de disociación, de modo que no permita identificar a persona alguna.

ARTICULO 28.- Los archivos, registros, bases o bancos de datos mencionados en el artículo 28 de la Ley Nº 25.326 son responsables y pasibles de las multas previstas en el artículo 31 de la ley citada cuando infrinjan sus disposiciones

17.2. Decisión Administrativa 11/2006

EL DIRECTOR NACIONAL DE PROTECCION DE DATOS PERSONALES

DISPONE:

Artículo 1° — Apruébense 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", cuyo texto como Anexo I forma parte del presente.

Art. 2° — Establécese que el plazo para la implementación de las medidas de seguridad a contar desde la fecha del dictado del presente acto, será de DOCE (12) meses para las de Nivel Básico, de VEINTICUATRO (24) meses para las de Nivel Medio y de TREINTA Y SEIS (36) meses para las de Nivel Crítico, los que serán prorrogables a pedido de la parte interesada y por razones debidamente fundadas.

Art. 3° — Comuníquese, publíquese, dése a la DIRECCION NACIONAL DEL REGISTRO OFICIAL y archívese. — Juan A. Travieso.

ANEXO I

"MEDIDAS DE SEGURIDAD PARA EL TRATAMIENTO Y CONSERVACION DE LOS DATOS PERSONALES CONTENIDOS EN ARCHIVOS, REGISTROS, BANCOS Y BASES DE DATOS PUBLICOS NO ESTATALES Y PRIVADOS"

• MEDIDAS DE SEGURIDAD DE NIVEL BASICO:

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:

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.

4.1. Notificación, gestión y respuesta ante los 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. La relación entre el usuario autorizado y el/los sistemas de información a los que puede acceder debe mantenerse actualizada. En el caso en que el mecanismo de autenticación utilice contraseña, la misma será asignada por el responsable de seguridad de acuerdo a un procedimiento que garantice su confidencialidad. Este procedimiento deberá prever el cambio periódico de la contraseña (lapso máximo de vigencia) las que deberán estar almacenadas en forma ininteligible.

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. Entre otras: 1) Instalar y actualizar, con la periodicidad pertinente, software de detección y reparación de virus, ejecutándolo rutinariamente; 2) Verificar, antes de su uso, la inexistencia de virus en archivos recibidos a través de la web, correo electrónico y otros cuyos orígenes sean inciertos.

10. Procedimiento que garantice una adecuada Gestión de los Soportes que contengan datos de carácter personal (identificación del tipo de información que contienen, almacenamiento en lugares de acceso restringidos, inventarios, autorización para su salida fuera del local en que están ubicados, destrucción de la información en desuso, etc.).

Nota: Cuando los archivos, registros, bases y bancos contengan una serie de datos personales con los cuales, a través de un determinado tratamiento, se permita establecer el perfil de personalidad o determinadas conductas de la persona, se deberán garantizar las medidas de seguridad del presente nivel más las establecidas en los puntos 2, 3, 4 y 5 del siguiente.

• MEDIDAS DE SEGURIDAD DE NIVEL MEDIO:

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 N° 25.326, deban guardar secreto de la información personal por expresa disposición legal (v.g.: 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.

Los informes de auditoría pertinentes, serán presentados al Responsable del Archivo a efectos de que se adopten las medidas correctivas que correspondan. La Dirección Nacional de Protección de Datos Personales, en las inspecciones que realice, deberá considerar obligatoriamente, con carácter no vinculante, los resultados de las auditorías referidas precedentemente, siempre que las mismas hayan sido realizadas dentro de un período máximo de un año.

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,

5.1. Se dispondrá de un registro de entradas y salidas de los soportes informáticos de manera de identificar, día y hora de entrada y salida del soporte, receptor, emisor, forma de envío, etc.

5.2. Se adoptarán las medidas necesarias para impedir cualquier recuperación de la información con posterioridad a que un soporte vaya a ser desechado o reutilizado, o que la información deba ser destruida, por la causa que correspondiere. Asimismo se deberán adoptar similares medidas cuando los soportes, o la información (ej.: cuando se hacen copias de respaldo a través de una red de transmisión de datos, la información sale de un soporte local y viaja hasta otro remoto vía dicha red.), vaya a salir fuera de los locales en que se encuentren ubicados,

5.3. Deberá disponerse de un procedimiento de recuperación de la información de respaldo y de tratamiento de la misma en caso de contingencias que pongan no operativo el/los equipos de procesamiento habituales.

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 CRITICO:

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 comunicación1, deberán serlo cifrados o utilizando cualquier otro mecanismo que impida su lectura y/o tratamiento por parte de personas no autorizadas.

Nota: Quedan exceptuados de aplicar las medidas de seguridad de nivel crítico, los archivos, registros, bases y bancos de datos que deban efectuar el tratamiento de datos sensibles para fines administrativos o por obligación legal. No obstante, ello no excluye que igualmente deban contar con aquellas medidas de resguardo que sean necesarias y adecuadas al tipo de dato.

[1]se trata de comunicaciones que salgan fuera de la red de la organización.