Congreso de la Nación Argentina
Información Parlamentaria

TEXTO ACTUALIZADO

PROTECCIÓN DE DATOS PERSONALES

Y

NORMAS REGLAMENTARIAS Y COMPLEMENTARIAS

LEY 25.326

TEXTO ACTUALIZADO
POR EL DEPARTAMENTO DE ORDENAMIENTO LEGISLATIVO
DE LA DIRECCIÓN DE INFORMACIÓN PARLAMENTARIA
DEL H. CONGRESO DE LA NACIÓN

DIRECCIÓN DE INFORMACIÓN PARLAMENTARIA
AV. RIVADAVIA 1864 -2º PISO – OFICINA 228
CIUDAD AUTÓNOMA DE BUENOS AIRES
TELÉFONO: (54 9 11) 4127-7100- INTERNOS 3629/30/36
MAIL: dip@diputados.gob.ar

ÍNDICE

Ley 25.326

PROTECCIÓN DE LOS DATOS PERSONALES

Promulgada con observaciones: Octubre 30 de 2000.

Texto actualizado
con las modificaciones de la ley 26.343 (BO 9-1-2008)
Boletín Oficial: Noviembre 2 de 2000

INDICE

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 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, almacena-miento, organización o acceso.

— Tratamiento de datos: Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relaciona-miento, 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 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 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 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° inciso 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 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.

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 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 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 habeas 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 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 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) Órganos 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 alma-cenado 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 con-forme 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 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 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 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 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.

Capítulo V

Control

ARTICULO 29. — (Órgano de Control).

1. El órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley. A tales efectos tendrá las siguientes funciones y atribuciones:

a) Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza;

b) Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley;

c) Realizar un censo de archivos, registros o bancos de datos alcanzados por la ley y mantener el registro permanente de los mismos;

d) Controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos. A tal efecto podrá solicitar autorización judicial para acceder a locales, equipos, o programas de tratamiento de datos a fin de verificar infracciones al cumplimiento de la presente ley;

e) Solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales que se le requieran. En estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados;

f) Imponer las sanciones administrativas que en su caso correspondan por violación a las normas de la presente ley y de las reglamentaciones que se dicten en su consecuencia;

g) Constituirse en querellante en las acciones penales que se promovieran por violaciones a la presente ley;

h) Controlar el cumplimiento de los requisitos y garantías que deben reunir los archivos o bancos de datos privados destinados a suministrar informes, para obtener la correspondiente inscripción en el Registro creado por esta ley.

2. ***Observado por D. 995/2000; B.O: 30/10/2000*****.**

3. ***Observado por D. 995/2000 de Observaciones; B.O: 30/10/2000).***

ARTICULO 30. — (Códigos de conducta).

1. Las asociaciones o entidades representativas de responsables o usuarios de bancos de datos de titularidad privada podrán elaborar códigos de conducta de práctica profesional, que establezcan normas para el tratamiento de datos personales que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de in-formación en función de los principios establecidos en la presente ley.

2. Dichos códigos deberán ser inscriptos en el registro que al efecto lleve el organismo de control, quien podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia.

Capítulo VI

Sanciones

ARTICULO 31. — (Sanciones administrativas).

1. Sin perjuicio de las responsabilidades administrativas que correspondan en los casos de responsables o usuarios de bancos de datos públicos; de la responsabilidad por daños y perjuicios derivados de la inobservancia de la presente ley, y de las sanciones penales que correspondan, el organismo de control podrá aplicar las sanciones de apercibimiento, suspensión, multa de mil pesos ($ 1.000.-) a cien mil pesos ($ 100.000.-), clausura o cancelación del archivo, registro o banco de datos.

2. La reglamentación determinará las condiciones y procedimientos para la aplicación de las sanciones previstas, las que deberán graduarse en relación a la gravedad y extensión de la violación y de los perjuicios derivados de la infracción, garantizando el principio del debido proceso.

ARTICULO 32. — (Sanciones penales).

1. Incorpórase como artículo 117 bis del Código Penal, el siguiente:

"……".

Capítulo VII

Acción de protección de los datos personales

ARTICULO 33. — (Procedencia).

1. La acción de protección de los datos personales o de hábeas data procederá:

a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos;

b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización.

ARTICULO 34. — (Legitimación activa).

La acción de protección de los datos personales o de hábeas data podrá ser ejercida por el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado.

Cuando la acción sea ejercida por personas de existencia ideal, deberá ser interpuesta por sus representantes legales, o apoderados que éstas designen al efecto. En el proceso podrá intervenir en forma coadyuvante el Defensor del Pueblo.

ARTICULO 35. — (Legitimación pasiva).

La acción procederá respecto de los responsables y usuarios de bancos de datos públicos, y de los privados destinados a proveer informes.

ARTICULO 36. — (Competencia).

Será competente para entender en esta acción el juez del domicilio del actor; el del domicilio del demandado; el del lugar en el que el hecho o acto se exteriorice o pudiera tener efecto, a elección del actor.

Procederá la competencia federal:

a) cuando se interponga en contra de archivos de datos públicos de organismos nacionales, y

b) cuando los archivos de datos se encuentren interconectados en redes interjurisdicciones, nacionales o internacionales.

ARTICULO 37. — (Procedimiento aplicable).

La acción de hábeas data tramitará según las disposiciones de la presente ley y por el procedimiento que corresponde a la acción de amparo común y supletoriamente por las normas del Código Procesal Civil y Comercial de la Nación, en lo atinente al juicio sumarísimo.

ARTICULO 38. — (Requisitos de la demanda).

1. La demanda deberá interponerse por escrito, individualizando con la mayor precisión posible el nombre y domicilio del archivo, registro o banco de datos y, en su caso, el nombre del responsable o usuario del mismo. En el caso de los archivos, registros o bancos públicos, se procurará establecer el organismo estatal del cual dependen.

2. El accionante deberá alegar las razones por las cuales entiende que en el archivo, registro o banco de datos individualizado obra información referida a su persona; los motivos por los cuales considera que la información que le atañe resulta discriminatoria, falsa o inexacta y justificar que se han cumplido los recaudos que hacen al ejercicio de los derechos que le reconoce la presente ley.

3. El afectado podrá solicitar que mientras dure el procedimiento, el registro o banco de datos asiente que la información cuestionada está sometida a un proceso judicial.

4. El Juez podrá disponer el bloqueo provisional del archivo en lo referente al dato personal motivo del juicio cuando sea manifiesto el carácter discriminatorio, falso o inexacto de la información de que se trate.

5. A los efectos de requerir información al archivo, registro o banco de datos involucrado, el criterio judicial de apreciación de las circunstancias requeridas en los puntos 1 y 2 debe ser amplio.

ARTICULO 39. — (Trámite).

1. Admitida la acción el juez requerirá al archivo, registro o banco de datos la remisión de la información concerniente al accionante. Podrá asimismo solicitar informes sobre el soporte técnico de datos, documentación de base relativa a la recolección y cualquier otro aspecto que resulte conducente a la resolución de la causa que estime procedente.

2. El plazo para contestar el informe no podrá ser mayor de cinco días hábiles, el que podrá ser ampliado prudencialmente por el juez.

ARTICULO 40. — (Confidencialidad de la información).

1. Los registros, archivos o bancos de datos privados no podrán alegar la confidencialidad de la información que se les requiere salvo el caso en que se afecten las fuentes de información periodística.

2. Cuando un archivo, registro o banco de datos público se oponga a la remisión del informe solicitado con invocación de las excepciones al derecho de acceso, rectificación o supresión, autorizadas por la presente ley o por una ley específica; deberá acreditar los extremos que hacen aplicable la excepción legal. En tales casos, el juez podrá tomar conocimiento personal y directo de los datos solicitados asegurando el mantenimiento de su confidencialidad.

ARTICULO 41. — (Contestación del informe).

Al contestar el informe, el archivo, registro o banco de datos deberá expresar las razones por las cuales incluyó la información cuestionada y aquellas por las que no evacuó el pedido efectuado por el interesado, de conformidad a lo establecido en los artículos 13 a 15 de la ley.

ARTICULO 42. — (Ampliación de la demanda).

Contestado el informe, el actor podrá, en el término de tres días, ampliar el objeto de la demanda solicitando la supresión, rectificación, confidencialidad o actualización de sus datos personales, en los casos que resulte procedente a tenor de la presente ley, ofreciendo en el mismo acto la prueba pertinente. De esta presentación se dará tras-lado al demandado por el término de tres días.

ARTICULO 43. — (Sentencia).

1. Vencido el plazo para la contestación del informe o contestado el mismo, y en el supuesto del artículo 42, luego de contestada la ampliación, y habiendo sido producida en su caso la prueba, el juez dictará sentencia.

2. En el caso de estimarse procedente la acción, se especificará si la información debe ser suprimida, rectificada, actualizada o declarada confidencial, estableciendo un plazo para su cumplimiento.

3. El rechazo de la acción no constituye presunción respecto de la responsabilidad en que hubiera podido incurrir el demandante.

4. En cualquier caso, la sentencia deberá ser comunicada al organismo de control, que deberá llevar un registro al efecto.

ARTICULO 44. — (Ambito de aplicación).

Las normas de la presente ley contenidas en los Capítulos I, II, III y IV, y artículo 32 son de orden público y de aplicación en lo pertinente en todo el territorio nacional. Se invita a las provincias a adherir a las normas de esta ley que fueren de aplicación exclusiva en jurisdicción nacional. La jurisdicción federal regirá respecto de los registros, archivos, bases o bancos de datos interconectados en redes de alcance interjurisdiccional, nacional o internacional.

ARTICULO 45. — El Poder Ejecutivo Nacional deberá reglamentar la presente ley y establecer el organismo de control dentro de los ciento ochenta días de su promulgación.

ARTICULO 46. — (Disposiciones transitorias).

Los archivos, registros, bases o bancos de datos destinados a proporcionar informes, existentes al momento de la sanción de la presente ley, deberán inscribirse en el registro que se habilite conforme a lo dispuesto en el artículo 21 y adecuarse a lo que dispone el presente régimen dentro del plazo que al efecto establezca la reglamentación.

ARTICULO 47. —*Los bancos de datos destinados a prestar servicios de información crediticia deberán eliminar y omitir el asiento en el futuro de todo dato referido a obligaciones y calificaciones asociadas de las personas físicas y jurídicas cuyas obligaciones comerciales se hubieran constituido en mora, o cuyas obligaciones financieras hubieran sido clasificadas con categoría 2, 3, 4 ó 5, según normativas del Banco Central de la República Argentina, en ambos casos durante el período comprendido entre el 1º de enero del año 2000 y el 10 de diciembre de 2003, siempre y cuando esas deudas hubieran sido canceladas o regularizadas al momento de entrada en vigencia de la presente ley o lo sean dentro de los 180 días posteriores a la misma. La suscripción de un plan de pagos por parte del deudor, o la homologación del acuerdo preventivo o del acuerdo preventivo extrajudicial importará la regularización de la deuda, a los fines de esta ley.*

El Banco Central de la República Argentina establecerá los mecanismos que deben cumplir las Entidades Financieras para informar a dicho organismo los datos necesarios para la

determinación de los casos encuadrados. Una vez obtenida dicha información, el Banco Central de la República Argentina implementará las medidas necesarias para asegurar que todos aquellos que consultan los datos de su Central de Deudores sean informados de la procedencia e implicancias de lo aquí dispuesto.

Toda persona que considerase que sus obligaciones canceladas o regularizadas están incluidas en lo prescripto en el presente artículo puede hacer uso de los derechos de acceso, rectificación y actualización en relación con lo establecido.

Sin perjuicio de lo expuesto en los párrafos precedentes, el acreedor debe comunicar a todo archivo, registro o banco de datos al que hubiera cedido datos referentes al incumplimiento de la obligación original, su cancelación

o regularización. ***(Artículo texto según Ley 26343 art 1° B:O: 9-1-2008)***

ARTICULO 48. — Comuníquese al Poder Ejecutivo.

Decreto 995/2000
(de Observaciones)

Bs. As., 30/10/2000

VISTO el Expediente N° 020-003060/2000 del Registro del MINISTERIO DE ECONOMÍA y el Proyecto de Ley registrado bajo el N° 25326, sancionando por el HONORABLE CONGRESO DE LA NACIÓN el 4 de octubre de 2000, y

CONSIDERANDO:

Que el referido Proyecto de Ley dispone la protección integral de los datos personales, de conformidad a lo establecido en el artículo 43, párrafo tercero de la CONSTITUCIÓN NACIONAL.

Que el artículo 29 del Proyecto de Ley establece la constitución de un Órgano de Control que deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y disposiciones emanados del referido Proyecto.

Que en el punto 2 del citado artículo se establece que el Órgano de Control gozará de autonomía funcional y actuará como organismo descentralizado en el ámbito del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS.

Que el punto 3 del artículo 29 del Proyecto de Ley norma sobre la conducción y administración del Órgano de Control.

Que la constitución del Órgano de Control como organismo descentralizado habrá de implicar, como toda incorporación de una estructura organizativa de este tipo, un incremento en las erogaciones del ESTADO NACIONAL para atender su funcionamiento.

Que el presente Proyecto de Ley no prevé el financiamiento del Órgano de Control y la Ley N° 25237 de Presupuesto de la Administración Nacional para el ejercicio 2000 y el Proyecto de Ley de Presupuesto Nacional para el ejercicio 2001 no contienen previsiones crediticias para su atención.

Que la legislación vigente en materia de Administración Financiera Pública determina que todo incremento de gastos debe prever el financiamiento respectivo.

Que sin perjuicio de lo indicado, se considera pertinente la constitución de un órgano de control, pero que reúna las características organizativas que determine el PODER EJECUTIVO NACIONAL de conformidad con la autorización conferida por el artículo 45 del presente Proyecto de Ley.

Que el artículo 47 del Proyecto de Ley dispone que los bancos de datos prestadores de servicios de información crediticia deberán suprimir, o en su caso, omitir asentar, todo dato referido al incumplimiento o mora en el pago de una obligación, si ésta hubiere sido cancelada al momento de la entrada en vigencia de la presente ley.

Que esta decisión generaría la pérdida de la información histórica respecto al cumplimiento crediticio de muchos deudores del sistema, lo que podría producir un encarecimiento de las operaciones de crédito bancario originado por el mayor riesgo provocado por la in-certidumbre.

Que por los fundamentos expuestos corresponde observar el artículo 29, puntos 2 y 3 y el artículo 47 del Proyecto de Ley registrado bajo el N° 25326.

Que la medida que se propone no altera el espíritu ni la unidad del Proyecto sancionado por el HONORABLE CONGRESO DE LA NACIÓN.

Que la DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS del MINISTERIO DE ECONOMÍA ha tomado la intervención que le compete.

Que el PODER EJECUTIVO NACIONAL se encuentra facultado para dictar el presente en virtud de lo dispuesto por el artículo 80 de la CONSTITUCIÓN NACIONAL.

Por ello,

EL PRESIDENTE DE LA NACIÓN ARGENTINA EN ACUERDO GENERAL DE MINISTROS DECRETA:

Artículo 1 — Obsérvase el artículo 29, puntos 2 y 3 del Proyecto de Ley registrado bajo el N° 25326.

Art. 2 — Obsérvase el artículo 47 del Proyecto de Ley registrado bajo el N° 25326.

Art. 3 — Con las salvedades establecidas en los artículos precedentes, cúmplase, promúlgase y téngase por Ley de la Nación el Proyecto de Ley registrado bajo el N° 25326.

Art. 4 — Dése cuenta al HONORABLE CONGRESO DE LA NACIÓN.

Art. 5 — de forma

NOTAS A LEY 25326

Artículo 29 punto 2. Observado por D. 995/2000; B.O: 30/10/2000.

……punto 3. Observado por D. 995/2000 de Observaciones; B.O: 30/10/2000).

.**Artículo 47**: Texto según Ley 26343 art 1° B.O: 9-1-2008)

LISTA DE NORMAS MODIFICATORIAS

Ley 26343 art. 1 B.O: 9-1-2008

DECRETO 1558/2001 (29/11/2001)

REGLAMENTACIÓN DE LA LEY Nº 25326.

B.O.: 03.12.2001

TEXTO ACTUALIZADO

Con las modificaciones de los decretos 1160/2010 (BO 13-8-2010) y 899/2017 (BO 06-11-2017)

INDICE

VISTO el expediente Nº 128.949/01 del registro del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, la Ley Nº 25326, y

CONSIDERANDO:

Que el artículo 45 de la mencionada Ley establece que el PODER EJECUTIVO NACIONAL deberá reglamentar la misma y establecer el órgano de control a que se refiere su artículo 29 dentro de los CIENTO OCHENTA (180) días de su promulgación.

Que el artículo 46 de la Ley citada establece que la reglamentación fijará el plazo dentro del cual los archivos de datos destinados a proporcionar informes existentes al momento de la sanción de dicha Ley deberán inscribirse en el Registro a que se refiere su artículo 21 y adecuarse a lo que dispone el régimen establecido en dicha norma.

Que el artículo 31, inciso 2, de la Ley Nº 25326 dispone que la reglamentación determinará las condiciones y procedimientos para la aplicación de sanciones, en los términos que dicha norma establece.

Que la DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, la DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS de la SUBSECRETARIA DE ASUNTOS LEGALES de la SECRETARIA LEGAL Y TÉCNICA de la PRESIDENCIA DE LA NACIÓN y la PROCURACIÓN DEL TESORO DE LA NACIÓN han tomado la intervención que les compete.

Que la presente medida se dicta en uso de las facultades conferidas por el artículo 99, inciso 2) de la CONSTITUCIÓN NACIONAL.

Por ello,

EL PRESIDENTE DE LA NACIÓN ARGENTINA DECRETA:

Art. 1 — Apruébase la reglamentación de la Ley Nº 25326 de Protección de los Datos Personales, que como anexo I forma parte del presente.

Art. 2 — Establécese en CIENTO OCHENTA (180) días el plazo previsto en el artículo 46 de la Ley Nº 25326.

Art. 3 — Invítase a las Provincias y a la CIUDAD AUTÓNOMA DE BUENOS AIRES a adherir a las normas de exclusiva aplicación nacional de esta reglamentación.

Art. 4 — Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese. —DE LA RUA. — Chrystian G. Colombo. — Jorge E. De La Rúa.

ANEXO I
REGLAMENTACIÓN DE LA LEY Nº 25.326

CAPITULO I

DISPOSICIONES GENERALES

ARTICULO 1. 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 2º.- Sin reglamentar.

CAPITULO II

PRINCIPIOS GENERALES RLATIVOS A LA PROTECCIÓN DE DATOS

ARTICULO 3.- Sin reglamentar.

ARTICULO 4. 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 25326.

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 DIRECCIÓN NACIONAL DE PROTECCIÓN 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 DIRECCIÓN NACIONAL DE PROTECCIÓN 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. 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 25326.

La DIRECCIÓN NACIONAL DE PROTECCIÓN 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 25326 el concepto de entidad financiera comprende a las personas alcanzadas por la Ley Nº 21526 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 21526.

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 21526.

ARTICULO 6. Sin reglamentar.

ARTICULO 7. Sin reglamentar.

ARTICULO 8. Sin reglamentar.

ARTICULO 9. La DIRECCIÓN NACIONAL DE PROTECCIÓN 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. Sin reglamentar.

ARTICULO 11. Al consentimiento para la cesión de los datos le son aplicables las disposiciones previstas en el artículo 5º de la Ley Nº 25326 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 25326. 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 DIRECCIÓN NACIONAL DE PROTECCIÓN 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 25326, 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. 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 DIRECCIÓN NACIONAL DE PROTECCIÓN 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.

CAPITULO III

DERECHOS DE LOS TITULARES DE DATOS

ARTICULO 13. Sin reglamentar.

ARTICULO 14. La solicitud a que se refiere el artículo 14, inciso 1, de la Ley Nº 25326, 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 DIRECCIÓN NACIONAL DE PROTECCIÓN 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 25326.

Vencido el plazo para contestar fijado en el artículo 14, inciso 2 de la Ley Nº 25326, el interesado podrá ejercer la acción de protección de los datos personales y denunciar el hecho ante la DIRECCIÓN NACIONAL DE PROTECCIÓN 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. 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 25326, a opción del titular de los datos, o las preferencias que el interesado hubiere expresamente manifestado al interponer el derecho de acceso.

La DIRECCIÓN NACIONAL DE PROTECCIÓN 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. En las disposiciones de los artículos 16 a 22 y 38 a 43 de la Ley Nº 25326 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 25326, 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 NACIÓN, 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 25326 mediante la modificación de los datos realizada a través de los mismos medios empleados para su divulgación.

ARTICULO 17. Sin reglamentar.

ARTICULO 18. Sin reglamentar.

ARTICULO 19. Sin reglamentar.

ARTICULO 20. Sin reglamentar.

CAPITULO IV

USUARIOS Y RESPONSABLES DE ARCHIVOS, REGISTROS Y BANCOS DE DATOS

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. Sin reglamentar.

ARTICULO 23. Sin reglamentar.

ARTICULO 24. Sin reglamentar.

ARTICULO 25. Los contratos de prestación de servicios de tratamiento de datos personales deberán contener los niveles de seguridad previstos en la Ley Nº 25326, esta reglamentación y las normas complementarias que dicte la DIRECCIÓN NACIONAL DE PROTECCIÓN 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 25326 incumben también al encargado del tratamiento.

ARTICULO 26. A los efectos del artículo 26, inciso 2, de la Ley Nº 25326, 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 25326 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 económicofinanciera de una persona, conforme lo establecido en el artículo 26, inciso 4, de la Ley Nº 25326, 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 25326, 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. 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 DIRECCIÓN NACIONAL DE PROTECCIÓN 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 25326, se inscribirán únicamente las cámaras, asociaciones y colegios profesionales del sector que dispongan de un Código de Conducta homologado por la DIRECCIÓN NACIONAL DE PROTECCIÓN 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 25326.

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 25326 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 25326 y la mención de su derecho a solicitar el retiro de la base de datos.

ARTICULO 28. Los archivos, registros, bases o bancos de datos mencionados en el artículo 28 de la Ley Nº 25326 son responsables y pasibles de las multas previstas en el artículo 31 de la ley citada cuando infrinjan sus disposiciones.

CAPITULO V

CONTROL

ARTICULO 29. La AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA, conforme los términos del artículo 19 de la Ley N° 27.275, sustituido por el artículo 11 del Decreto N° 746/17, es el órgano de control de la Ley Nº 25.326.

(Texto según Decreto 899/2017, art. 1 - BO 06-11-2017)

ARTICULO 30. La DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES alentará la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por la Ley Nº 25326 y esta reglamentación.

Las asociaciones de profesionales y las demás organizaciones representantes de otras categorías de responsables o usuarios de archivos, registros, bases o bancos de datos públicos o privados, que hayan elaborado proyectos de códigos éticos, o que tengan la intención de modificar o prorrogar códigos nacionales existentes, podrán someterlos a consideración de la DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES, la cual aprobará el ordenamiento o sugerirá las correcciones que se estimen necesarias para su aprobación.

CAPITULO VI

SANCIONES

ARTICULO 31.

1. Las sanciones administrativas establecidas en el artículo 31 de la Ley Nº 25326 serán aplicadas a los responsables o usuarios de archivos, registros, bases o bancos de datos públicos, y privados destinados a dar información, se hubieren inscripto o no en el registro correspondiente.

   La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, los daños y perjuicios causados a las personas interesadas y a terceros, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuricidad y de culpabilidad presentes en la concreta actuación infractora. Se considerará reincidente a quien habiendo sido sancionado por una infracción a la Ley Nº 25326 o sus reglamentaciones incurriera en otra de similar naturaleza dentro del término de TRES (3) años, a contar desde la aplicación de la sanción.

2. El producido de las multas a que se refiere el artículo 31 de la Ley Nº 25326 se aplicará al financiamiento de la DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES.

3. *El procedimiento se ajustará a las siguientes disposiciones:*

   a) La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES (DNPDP) iniciará actuaciones administrativas en caso de presuntas infracciones a las disposiciones de la Ley Nº 25326, sus normas reglamentarias y complementarias, de oficio o por denuncia de quien invocare un interés particular, del Defensor del Pueblo de la Nación o de asociaciones de consumidores o usuarios.

   b) Para el cumplimiento de sus cometidos, la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES podrá:

   I) Comprobar la legitimidad de todas las 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.

   II) Constatar el funcionamiento adecuado de los mecanismos de control interno y externo del archivo, registro, base o banco de datos para el efectivo resguardo de los datos personales que contiene.

III) Verificar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos.

IV) Velar por el cumplimiento de los plazos establecidos en los artículos 14 y 16 de la Ley Nº 25326 para el ejercicio de los derechos de acceso, rectificación, supresión, actualización y confidencialidad reconocidos a los titulares de datos personales.

V) Realizar investigaciones e inspecciones, así como requerir de los responsables o usuarios de bancos de datos personales y de su tratamiento, información, antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales que estime necesario y también solicitar el auxilio de los cuerpos técnicos y/o, en su caso, la autorización judicial que corresponda, a sus efectos.

VI) Solicitar la presentación de informes a los responsables de bancos de datos y de su tratamiento.

VII) Formular requerimientos ante las autoridades nacionales, provinciales y municipales.

VIII) Realizar inspecciones y labrar el Acta de Inspección pertinente, la que junto con las comprobaciones técnicas que se dispusieren, constituirá prueba suficiente de los hechos así

comprobados.

IX) Solicitar al juez competente el auxilio de la fuerza pública para realizar el allanamiento de domicilios; la Clausura de registros; el secuestro de documentación y toda otra medida tendiente al cabal cumplimiento de la actividad investigativa.

c) Para el inicio del procedimiento, el denunciante deberá presentar ante la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES un escrito, el que deberá contener fecha, firma y aclaración; documento de identidad (DNI-CUIL-CUIT), domicilio, la relación del hecho denunciado con las circunstancias de lugar, tiempo y modo de ejecución y demás elementos que puedan conducir a su comprobación, como mínimo. Deberá acompañar en el mismo acto la documentación y antecedentes que confirmen sus dichos y acreditar en el momento de la interposición de la denuncia, las gestiones previas ante el responsable de la base de datos, cuando se tratare de cuestiones referidas a los derechos de acceso, actualización, rectificación, supresión, confidencialidad o bloqueo, regulados en los artículos 14, 16 y 27 de la Ley Nº 25326. La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES podrá habilitar un sistema telemático para facilitar la interposición de la denuncia.

d) Iniciado el procedimiento, se requerirá del responsable de la base de datos sobre la que recae la denuncia, un informe acerca de los antecedentes y circunstancias que hicieren al objeto de la denuncia o actuación de oficio, así como de otros elementos de juicio que permitan dilucidar la cuestión sujeta a investigación o control. La información requerida deberá ser contestada dentro de los DIEZ (10) días hábiles, salvo que el denunciado solicite en tiempo y forma una prórroga la que no podrá superar los DIEZ (10) días hábiles. Este plazo podrá ampliarse en casos debidamente justificados teniendo en cuenta la magnitud y dimensión de la base de datos. En su primera presentación, el denunciado deberá acreditar personería y constituir domicilio legal.

e) El funcionario actuante admitirá las pruebas que estime pertinentes sólo cuando existieren hechos controvertidos y siempre que no resultaren manifiestamente inconducentes. La denegatoria de las medidas de prueba no será recurrible.

f) En las distintas etapas del procedimiento, se podrá requerir al denunciante que aporte información o documentación que sea pertinente para la dilucidación de la investigación.

g) Cuando se considere "prima facie" que se han transgredido algunos de los preceptos de la Ley Nº 25326, sus normas reglamentarias y complementarias, se labrará un Acta de Constatación, la que deberá contener: lugar y fecha, nombre, apellido y documento de identidad del denunciante; una relación sucinta de los hechos; la indicación de las diligencias realizadas y su resultado y la o las disposiciones presuntamente infringidas, como mínimo. En ésta se dispondrá citar al presunto infractor para que, dentro del plazo de DIEZ (10) días hábiles, presente por escrito su descargo y, en caso de corresponder, acompañe las pruebas que hagan a su derecho.

h) Concluida la investigación y previo dictamen del servicio permanente de asesoramiento jurídico del MINISTERIO DE JUSTICIA, SEGURIDAD Y DERECHOS HUMANOS, el Director Nacional de Protección de Datos Personales dictará la respectiva disposición, la que deberá declarar:

I) que los hechos investigados no constituyen una irregularidad, o

II) que los hechos investigados constituyen una infracción, quiénes son sus responsables y cuál es la sanción administrativa que corresponde aplicar, conforme lo dispuesto en la Ley Nº 25326, sus normas reglamentarias y complementarias y lo establecido en la Disposición DNPDP Nº 7 de fecha 8 de noviembre de 2005. La resolución que se dicte deberá ser notificada al infractor.

i) Contra la resolución definitiva procederá la vía recursiva prevista en el REGLAMENTO DE PROCEDIMIENTOS ADMINISTRATIVOS (Decreto Nº 1759/72 - t.o. 1991) y sus modificatorios.

j) Dictada la resolución que impone una sanción administrativa, la constancia de la misma deberá ser incorporada en el REGISTRO DE INFRACTORES LEY Nº 25326, que lleva la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES. Las constancias de dicho Registro relativas a aquellas sanciones aplicadas que se encuentren firmes deberán publicarse en el sitio de Internet de la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES (www.jus. gov.ar/dnpdpnew).

k) Resultarán de aplicación supletoria la LEY NACIONAL DE PROCEDIMIENTOS ADMINISTRATIVOS Nº 1.549; el REGLAMENTO DE PROCEDIMIENTOS ADMINISTRATIVOS (Decreto Nº 1759/72 - t.o. 1991) y sus modificatorios y el CODIGO PROCESAL CIVIL Y COMERCIAL DE LA NACION.
(***Texto según decreto 1160/2010 art 1° - BO 13-8-2010)***

ARTICULO 32. Sin reglamentar.

CAPITULO VII

ACCIÓN DE PROTECCIÓN DE LOS DATOS PERSONALES

ARTÍCULOS 33 a 46. Sin reglamentar.

.-.-.-.-.-.-.-.-.

NOTAS AL DECRETO 1558/2001 (29/11/2001)

Artículo 29: Texto según Decreto 899/2017, artículo1° - BO 06-11-2017

Artículo 31: Texto según decreto 1160/2010 art 1° - BO 13-8-2010

LISTA DE NORMAS MODIFICATORIAS

Decreto 1160/2010 BO 13-8-2010)

Disposición 7/2005
Direcc Nac de Protección de Datos Personales

CLASIFICACIÓN DE INFRACCIONES Y GRADUACIÓN LAS SANCIONES
Deroga la Disposición Nº 1/2003.

TEXTO ACTUALIZADO
CON LAS MODIFICACIONES DE LA DISPOSICIÓN 9/2015 DNPDP BO 24.2.2015)

INDICE

Bs. As., 8/11/2005 BO 11-11-2005

VISTO las competencias atribuidas a esta DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES por la Ley Nº 25326 y su reglamentación aprobada por Decreto Nº 1558/01, la Disposición DNPDP Nº 1 del 25 de junio de 2003,

y CONSIDERANDO:

Que entre las atribuciones asignadas a la DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES se encuentra la de imponer las sanciones administrativas que en su caso correspondan por violación a las normas de la Ley Nº 25326 y de las reglamentaciones dictadas en su consecuencia.

Que en virtud de ello, oportunamente se dictó la Disposición DNPDP Nº 1/2003, la que estableció una clasificación de las infracciones en “leves”, “graves” y “muy graves” y una graduación de la sanción administrativa de multa a aplicar ante las infracciones que pudieran comprobarse, determinada dentro de los parámetros de monto fijados en el artículo 31 de la citada norma legal.

Que la misma normativa prevé que el órgano de control también podrá aplicar otras sanciones tales como apercibimiento, suspensión y clausura o cancelación del archivo, registro o banco de datos.

Que la experiencia ha demostrado, a pesar del breve período en que la mencionada Disposición se ha encontrado vigente, que resulta menester incorporar en el régimen sancionatorio por ella previsto, también a las otras sanciones que contempla el artículo 31 de la Ley Nº 25326, con el objeto de otorgar a la DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES un adecuado margen de actuación al momento de determinar la cuantía de las

sanciones a aplicar, oportunidad en la que deberá considerar los criterios previstos en el segundo párrafo del artículo 31 del Decreto Reglamentario Nº 1558/ 01.

Que asimismo es oportuno incorporar nuevos hechos u omisiones que implican transgresiones a la normativa de protección de datos personales.

Que en consecuencia, cabe entonces reformular el régimen de infracciones y sanciones vigente, continuando en la postura antes sustentada al dictar la misma, de contar con un listado de carácter meramente enunciativo y por ende no taxativo, de aquellas conductas que se consideran violatorias de la Ley Nº 25326 y su reglamentación.

Que a los fines indicados precedentemente sería conveniente aplicar a los casos de "infracciones leves" las sanciones de "hasta DOS (2) apercibimientos" y/o "multa de PESOS UN MIL ($ 1.000.) a PESOS TRES MIL ($ 3.000.); a las "infracciones graves", las sanciones de "hasta CUATRO (4) apercibimientos", "suspensión de UNO (1) a TREINTA (30) días" y/ o "multa de PESOS TRES MIL UNO ($ 3.001.) a PESOS CINCUENTA MIL ($ 50.000.) y finalmente, a los casos de "infracciones muy graves" las sanciones de "hasta SEIS (6) apercibimientos", "suspensión de TREINTA Y UN (31) a TRESCIENTOS SESENTA Y CINCO (365) días", "clausura o cancelación del archivo, registro o banco de datos" y/o "multa de PESOS CINCUENTA MIL UNO ($50.001.) a PESOS CIEN MIL ($ 100.000.).

Que asimismo, resulta conveniente que la DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES organice y mantenga actualizado un registro de los responsables de la comisión de las infracciones contempladas en la presente medida, en particular con el objeto de establecer antecedentes individuales para la evaluación de la cuantía de las sanciones, especialmente respecto del rubro reincidencia.

Que la DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS y la PROCURACIÓN DEL TESORO DE LA NACIÓN han tomado la intervención que les compete.

Que la presente medida se dicta en uso de las facultades conferidas en el artículo 29 inciso b) y f) de la Ley Nº 25326.

Por ello,

EL DIRECTOR NACIONAL DE PROTECCIÓN DE DATOS PERSONALES

DISPONE:

Artículo 1 — Derógase la Disposición DNPDP Nº 1 del 25 de junio de 2003.

Art. 2 — Apruébase la "Clasificación de Infracciones" y la "Graduación de las Sanciones", que como ANEXOS I y II, respectivamente, forman parte integrante de la presente medida.

Art. 3 — Créase el Registro de Infractores Ley Nº 25326, el que tendrá como objetivos:

a) organizar y mantener actualizado, con las constancias provenientes de las actuaciones labradas en el marco del procedimiento de denuncias ante la DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES, un registro de los responsables de la comisión de las infracciones contempladas en el ANEXO I de la presente medida.

b) hacer constar, en el legajo que se instrumente al respecto, la calidad de la falta cometida, la sanción aplicada, el grado de acatamiento de la misma, los recursos planteados, la decisión final recaída, la calidad de reincidente y todo otro elemento de juicio que sea de interés para la DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES.

Art. 4 — La DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES será el órgano responsable del archivo creado en el artículo precedente y ante sus dependencias deberán ejercerse los derechos de acceso, rectificación o supresión.

Art. 5 — Comuníquese, publíquese, dése a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL y archívese. — Juan A. Travieso.

ANEXO I
CLASIFICACION DE LAS INFRACCIONES

(Anexo I: texto según Disposición 9/2015 DNPDP BO 24.2.2015)

1.- Serán consideradas INFRACCIONES LEVES, sin perjuicio de otras que a juicio de la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES también las constituyan:

a) No proporcionar en tiempo y forma la información que solicite la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES en el ejercicio de las competencias que tiene atribuidas.

b) No cumplir con todas las etapas del procedimiento previsto en el Anexo III de la Disposición DNPDP N° 2 del 14 de febrero de 2005 para que la inscripción ante el REGISTRO NACIONAL DE BASES DE DATOS se perfeccione.

c) No informar en tiempo y forma modificaciones o bajas ante el REGISTRO NACIONAL DE BASES DE DATOS. Esta infracción incluye no informar cambios de domicilio.

d) No efectuar, en los casos que corresponda, la renovación anual de la inscripción ante el REGISTRO NACIONAL DE BASES DE DATOS, de conformidad con lo establecido en el artículo 7° de la Disposición DNPDP N° 2 del 14 de febrero de 2005.

e) No acompañar en tiempo y forma la documentación requerida en el marco de un procedimiento de inspección.

f) No respetar el principio de gratuidad previsto en el artículo 19 de la Ley N° 25326.

g) Incumplir el deber de secreto establecido en el artículo 10 de la Ley N° 25326, salvo que constituya la infracción grave prevista en el punto 2, apartado j) o la infracción muy grave contemplada en el punto 3, apartado n) o el delito contemplado en el artículo 157 bis, inciso 2) del CÓDIGO PENAL.

h) Utilizar los servicios de telefonía en cualquiera de sus modalidades para publicitar, ofertar, vender o regalar bienes o servicios sin utilizar números identificables por el identificador de llamadas.

i) No aportar el listado de las llamadas salientes cuando ello fuere requerido por la DIRECCION NACIONAL DE PROTECCIÓN DE DATOS PERSONALES en el marco de las actuaciones administrativas iniciadas por presunta infracción a la Ley N° 26951.

2.- Serán consideradas INFRACCIONES GRAVES, sin perjuicio de otras que a juicio de la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES también las constituyan:

a) Recoger datos de carácter personal sin proporcionar a los titulares de los mismos la información exigida por el artículo 6° de Ley N° 25.326 o sin recabar su consentimiento libre, expreso e informado en los casos en que ello sea exigible.

b) No atender en tiempo y forma la solicitud de acceso, rectificación o supresión de los datos personales objeto de tratamiento cuando legalmente proceda.

c) Efectuar tratamiento de datos personales sin encontrarse inscripto ante el REGISTRO NACIONAL DE BASES DE DATOS en infracción a lo dispuesto por el artículo 3° de la Ley N° 25326.

d) No efectuar la renovación anual de la inscripción ante el REGISTRO NACIONAL DE BASES DE DATOS, de conformidad con lo establecido en el artículo 7° de la Disposición DNPDP N° 2 del 14 de febrero de 2005, cuando hubiere sido intimado para ello por la DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES.

e) Mantener por más tiempo que el establecido legalmente, el registro, archivo o cesión de los datos significativos para evaluar la solvencia económico-financiera de los titulares de los datos.

f) Tratar, dentro de la prestación de servicios de información crediticia, datos personales patrimoniales que excedan la información relativa a la solvencia económica y al crédito del titular de tales datos.

g) Tratar, en los archivos, registros o bancos de datos con fines publicitarios, datos que excedan la calidad de aptos para establecer perfiles con fines promocionales o hábitos de consumo.

h) No retirar o bloquear el nombre y dirección de correo electrónico de los bancos de datos destinados a publicidad cuando su titular lo solicite de conformidad con lo previsto en el artículo 27, inciso 3 de la Ley N° 25326.

i) Proceder al tratamiento de datos de carácter personal que no reúnan las calidades de ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.

j) Incumplir el deber de confidencialidad exigido por el artículo 10 de la Ley N° 25326 sobre los datos de carácter personal incorporados a registros, archivos, bancos o bases de datos.

k) Mantener bases de datos locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

I) Obstruir el ejercicio de la función de inspección y fiscalización a cargo de la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES.

m) Hacer ilegalmente uso del isologotipo creado a través de la Disposición DNPDP N° 6 del 1° de setiembre de 2005, por el que se identifica a los responsables inscriptos ante el REGISTRO NACIONAL DE BASES DE DATOS.

n) Contactar con el objeto de publicidad, oferta, venta o regalo de bienes o servicios utilizando los servicios de telefonía en cualquiera de sus modalidades a quienes se encontraren debidamente inscriptos ante el REGISTRO NACIONAL "NO LLAME" creado por la Ley N° 26951.

o) Utilizar los servicios de telefonía en cualquiera de sus modalidades para publicitar, ofertar, vender o regalar bienes o servicios sin haber obtenido de la Autoridad de Aplicación la habilitación de usuario autorizado para la descarga de la lista de inscriptos ante el REGISTRO NACIONAL "NO LLAME".

p) Utilizar los servicios de telefonía en cualquiera de sus modalidades para publicitar, ofertar, vender o regalar bienes o servicios sin consultar, en forma previa al procedimiento de contacto y con una periodicidad de TREINTA (30) días corridos, la última versión de la lista de inscriptos ante el REGISTRO NACIONAL "NO LLAME" creado por la Ley N° 26.951, proporcionada por la Autoridad de Aplicación.

q) No adoptar las medidas adecuadas que propicien el cumplimiento de la Ley N° 26.951, cuando se trate de campañas contratadas en el exterior que utilicen los servicios de telefonía en cualquiera de sus modalidades para publicitar, ofertar, vender o regalar bienes o servicios.

r) Contactar a los titulares o usuarios de servicios de telefonía en cualquiera de sus modalidades que se hubieran inscripto en el REGISTRO NACIONAL "NO LLAME" creado por la Ley N° 26951, haciendo uso indebido de las excepciones previstas en el artículo 8 de la citada norma legal.

3.- Serán consideradas INFRACCIONES MUY GRAVES, sin perjuicio de otras que a juicio de la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES también las constituyan:

a) No inscribir la base de datos de carácter personal en el registro correspondiente, cuando haya sido requerido para ello por la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES.

b) Declarar datos falsos o inexactos al efectuar la registración ante el REGISTRO NACIONAL DE BASES DE DATOS.

c) No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el titular y/o por la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES.

d) Recoger datos de carácter personal mediante ardid, engaño o fraude a la ley.

e) Conformar un archivo de datos cuya finalidad sea contraria a las leyes o a la moral pública.

f) Tratar los datos de carácter personal en forma ilegítima o con menosprecio de los principios y garantías establecidos en Ley N° 25326 y normas reglamentarias.

g) Realizar acciones concretas tendientes a impedir u obstaculizar el ejercicio por parte del titular de los datos del derecho de acceso o negarse a facilitarle la información que sea solicitada.

h) Mantener datos personales inexactos o no efectuar las rectificaciones, actualizaciones o supresiones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la Ley N° 25.326 ampara y haya sido intimado previamente por la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES.

I) Transferir datos personales de cualquier tipo a países u organismos internacionales o supranacionales que no proporcionen niveles de protección adecuados, salvo las excepciones legales previstas en el artículo 12, inciso 2, de la Ley N° 25326, sin haber cumplido los demás recaudos legales previstos en la citada ley y su reglamentación.

j) Ceder ilegítimamente los datos de carácter personal fuera de los casos en que tal accionar esté permitido.

k) Recolectar y tratar los datos sensibles sin que medien razones de interés general autorizadas por ley o tratarlos con finalidades estadísticas o científicas sin hacerlo en forma disociada.

I) Formar archivos, bancos o registros que almacenen información que directa o indirectamente revelen datos sensibles, salvo en los casos expresamente previstos en el artículo 7°, inciso 3 de la Ley N° 25326.

m) Tratar los datos de carácter personal de forma ilegitima o con menosprecio de los principios y garantías reconocidos constitucionalmente, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

n) Incumplir el deber de confidencialidad respecto de los datos sensibles, así como de los que hayan sido recabados y tratados para fines penales y contravencionales.

o) Realizar maniobras tendientes a sustraerse o impedir el desarrollo de la actividad de contralor de la DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES.

p) Omitir denunciar, con motivo del tratamiento de datos personales en Internet, el domicilio legal y demás datos identificatorios del responsable de la base de datos, sea ante el REGISTRO NACIONAL DE BASES DE DATOS como ante otros organismos oficiales que requieran su identificación para el ejercicio de la actividad, de modo tal que mediante dicha conducta afecte el ejercicio de los derechos del titular del dato y la actividad de contralor que por la normativa vigente compete a la DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES.

ANEXO II

GRADUACIÓN DE LAS SANCIONES

(Anexo II: texto según Disposición 9/2015 DNPDP BO 24.2.2015)

1. Ante la comisión de INFRACCIONES LEVES se podrán aplicar hasta DOS (2) APERCIBIMIENTOS y/o una MULTA de PESOS UN MIL ($ 1.000,00) a PESOS VEINTICINCO MIL ($ 25.000,00).

2. En el caso de las INFRACCIONES GRAVES la sanción a aplicar será de hasta CUATRO (4) APERCIBIMIENTOS, SUSPENSION DE UNO (1) a TREINTA (30) DIAS y/o MULTA de PESOS VEINTICINCO MIL UNO ($ 25.001,00) a PESOS SESENTA MIL ($ 80.000,00).

3. En el caso de INFRACCIONES MUY GRAVES se aplicarán hasta SEIS (6) APERCIBIMIENTOS, SUSPENSION DE TREINTA Y UNO (31) a TRESCIENTOS SESENTA Y CINCO (365) DIAS, CLAUSURA o CANCELACION DEL ARCHIVO, REGISTRO O BANCO DE DATOS y/o MULTA de PESOS SESENTA MIL UNO ($ 80.001,00) a PESOS CIEN MIL ($ 100.000,00).

4. Superados los SEIS (6) APERCIBIMIENTOS no podrá aplicarse nuevamente este tipo de sanción.

5. Las sanciones previstas precedentemente serán de aplicación a los responsables o usuarios de archivos, registros, bases o bancos de datos públicos y privados destinados a dar informes, se hubieren inscripto o no en el registro correspondiente, ello sin perjuicio de las responsabilidades administrativas que pudieran corresponder a los responsables o usuarios de bancos de datos públicos; de la responsabilidad por daños y perjuicios derivados de la inobservancia de la presente ley y de las sanciones penales que correspondan.

6. La aplicación y cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

7. Cada infracción deberá ser sancionada en forma independiente, debiendo acumularse cuando varias conductas sancionables se den en las mismas actuaciones.

8. La reincidencia se configura cuando quien habiendo sido sancionado por una de las infracciones previstas en las Leyes Nros. 25326 y 26951 y/o sus reglamentaciones, incurriera en otra de similar naturaleza dentro del término de TRES (3) años, a contar desde la aplicación de la sanción.

9. La multa deberá ser abonada dentro de los DIEZ (10) días hábiles administrativos desde su notificación.

10. La falta de pago de las multas aplicadas hará exigible su cobro por ejecución fiscal, constituyendo suficiente título ejecutivo el testimonio autenticado de la resolución condenatoria firme.

11. Sin perjuicio de las sanciones que se apliquen, la DIRECCION NACIONAL DE PROTECCIÓN DE DATOS PERSONALES podrá imponer a la sancionada una obligación de hacer con el objeto de que cese en el incumplimiento que diera origen a la sanción.

-.-.-.-.-.-.-.

NOTAS A LA DISPOSICIÓN 7/2007 DNPDP

Anexo I: texto según Disposición 9/2015 DNPDP BO 24.2.2015

Anexo II: texto según Disposición 9/2015 DNPDP BO 24.2.2015

LISTA DE NORMAS MODIFICATORIAS

Disposición 9/2015 DNPDP BO 24.2.2015

Disposición 11/2006
Direcc. Nac. de Protección de Datos Personales

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

Boletín Oficial 22-09-2006

INDICE

Bs. As., 19/9/2006 VISTO el Expediente N° 153.743/06 del registro del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, las competencias atribuidas a esta DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES por la Ley N° 25326 y su reglamentación aprobada por Decreto N° 1558 del 29 de noviembre de 2001, y

CONSIDERANDO:

Que de conformidad con lo prescripto por el artículo 9° de la Ley N° 25326, el responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad y confidencialidad de los datos personales, a fin 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.

Que por su parte, entre las atribuciones asignadas a la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES se encuentra la de dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas en la Ley N° 25326 (artículo 29, inciso 1, apartado b) y específicamente la de dictar normas administrativas y de procedimientos técnicos relativos al tratamiento y condiciones de seguridad de los archivos, registros y bases o bancos de datos públicos y privados (artículo 29, inciso 5, apartado a, del Anexo al del Decreto N° 1558/01), así como la de controlar la observancia de las normas sobre integridad y seguridad de los datos por parte de los archivos, registros o bancos de datos (artículo 29, inciso 1, apartado d, de la Ley N° 25326).

Que como consecuencia de ello y en cumplimiento de la facultad que este Organo de Control tiene para el dictado de normas relativas a las condiciones de seguridad de los archivos, registros

y bases o bancos de datos, corresponde aprobar las medidas de seguridad para el tratamiento y conservación de los datos personales, que deberán observar los responsables y usuarios de archivos, registros, bases y bancos de datos públicos no estatales y privados.

Que a tal fin, se establece un "Documento de Seguridad de Datos Personales", como instrumento para la especificación de la normativa de seguridad, el que deberá adecuarse en todo momento a las disposiciones vigentes en la materia dictadas por la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES.

Que asimismo, se establecen TRES (3) niveles de seguridad: BASICO, MEDIO y CRITICO, conforme la naturaleza de la información tratada, pautas aplicables también a los archivos no informatizados (registro manual).

Que para cada uno de los niveles antes mencionados se han previsto distintas medidas de seguridad, establecidas teniendo en cuenta la mayor o menor necesidad de garantizar la confidencialidad e integridad de la información contenida en el banco de datos respectivo; la naturaleza de los datos y la correcta administración de los riesgos a que están expuestos, así corno también el mayor o menor impacto que tendría en las personas el hecho de que la información registrada en los archivos no reúna las condiciones de integridad y confiabilidad debidas.

Que se han establecido distintos plazos para la implementación de las medidas de seguridad que se propician, teniendo en consideración el nivel de seguridad de que se trate, así corno también la posibilidad de otorgar una prórroga previa solicitud debidamente fundamentada.

Que la DIRECCION GENERAL DE ASUNTOS JURIDICOS del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS ha tomado la intervención que le compete. Que la presente medida se dicta el uso de las facultades conferidas en el artículo 29, inciso 1, apartado b, de la Ley N° 25326 y artículo 29, inciso 5, apartado a, del Anexo al Decreto N° 1558/01.

Por ello,

EL DIRECTOR NACIONAL DE PROTECCION DE DATOS PERSONALES

DISPONE:

Art 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° 25326, 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.

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

-.-.-.-.-.-.-.-.-.-.-.-.-.-