

Dirección Nacional de Protección de Datos Personales

PROTECCION DE DATOS PERSONALES

Disposición 11/2006

Apruébanse 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".

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° 25.326 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° 25.326, 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° 25.326 (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° 25.326).

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 como 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 como 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° 25.326 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:

Artículo 1° — Apruébense las "Medidas de Seguridad para el Tratamiento y Conservación de los Datos Personales Contenidos en Archivos, Registros, Bancos y Bases de Datos Públicos no estatales y Privados", cuyo texto como Anexo I forma parte del presente.

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

(Nota Infoleg: por art. 1° de la Disposición N° 9/2008 de la Dirección Nacional de Protección de Datos Personales, B.O. 3/9/2008, se prorroga el plazo establecido en el presente artículo para la implementación de las medidas de seguridad de los Niveles Medio y Crítico, los que serán exigibles dentro de DOCE (12) y VEINTICUATRO (24) meses, respectivamente, a contar desde la entrada en vigencia de la referida disposición)

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

ANEXO I

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

- MEDIDAS DE SEGURIDAD DE NIVEL BASICO:

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

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

Deberá contener:

1. Funciones y obligaciones del personal.

2. Descripción de los archivos con datos de carácter personal y los sistemas de información que los tratan.

3. Descripción de las rutinas de control de datos de los programas de ingreso de datos y las acciones a seguir ante los errores detectados a efectos de su corrección. Todos los programas de ingreso de datos, cualquiera sea su modo de procesamiento (batch, interactivo, etc.), deben incluir en su diseño, rutinas de control, que minimicen la posibilidad de incorporar al sistema de información, datos ilógicos, incorrectos o faltantes.

4. Registros de incidentes de seguridad.

4.1. Notificación, gestión y respuesta ante los incidentes de seguridad.

5. Procedimientos para efectuar las copias de respaldo y de recuperación de datos.

6. Relación actualizada entre Sistemas de Información y usuarios de datos con autorización para su uso.

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

8. Control de acceso de usuarios a datos y recursos necesarios para la realización de sus tareas para lo cual deben estar autorizados.

9. Adoptar medidas de prevención a efectos de impedir amenazas de software malicioso (virus, troyanos, etc.) que puedan afectar archivos con datos de carácter personal. Entre otras: 1) Instalar y actualizar, con la periodicidad pertinente, software de detección y reparación de virus, ejecutándolo rutinariamente; 2) Verificar, antes de su uso, la inexistencia de virus en archivos recibidos a través de la web, correo electrónico y otros cuyos orígenes sean inciertos.

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

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

- MEDIDAS DE SEGURIDAD DE NIVEL MEDIO:

Los archivos, registros, bases y bancos de datos de las empresas privadas que desarrollen actividades de prestación de servicios públicos, así como los archivos, registros, bases y bancos de datos pertenecientes a entidades que cumplan una función pública y/o privada que, más allá de lo dispuesto por el artículo 10 de la Ley N° 25.326, deban guardar secreto de la información personal por expresa disposición legal (v.g.: secreto bancario), además de las medidas de seguridad de nivel Básico, deberán adoptar las que a continuación se detallan:

1. El Instructivo de seguridad deberá identificar al Responsable (u órgano específico) de Seguridad.

2. Realización de auditorías (internas o externas) que verifiquen el cumplimiento de los procedimientos e instrucciones vigentes en materia de seguridad para datos personales.

Los informes de auditoría pertinentes, serán presentados al Responsable del Archivo a efectos de que se adopten las medidas correctivas que correspondan. La Dirección Nacional de Protección de Datos Personales, en las inspecciones que realice, deberá considerar obligatoriamente, con

carácter no vinculante, los resultados de las auditorías referidas precedentemente, siempre que las mismas hayan sido realizadas dentro de un período máximo de un año.

3. Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

4. Se establecerá un control de acceso físico a los locales donde se encuentren situados los sistemas de información con datos de carácter personal.

5. Gestión de Soportes e información contenida en ellos,

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

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

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

6. Los registros de incidentes de seguridad, en el caso de tener que recuperar datos, deberán identificar la persona que recuperó y/o modificó dichos datos. Será necesaria la autorización en forma fehaciente del responsable del archivo informatizado.

7. Las pruebas de funcionamiento de los sistemas de información, realizadas con anterioridad a su puesta operativa no se realizarán con datos/archivos reales, a menos que se aseguren los niveles de seguridad correspondientes al tipo de datos informatizados tratados.

- MEDIDAS DE SEGURIDAD DE NIVEL CRITICO:

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

1. Distribución de soportes: cuando se distribuyan soportes que contengan archivos con datos de carácter personal —incluidas las copias de respaldo—, se deberán cifrar dichos datos (o utilizar cualquier otro mecanismo) a fin de garantizar que no puedan ser leídos o manipulados durante su transporte.

2. Registro de accesos: se deberá disponer de un registro de accesos con información que identifique al usuario que accedió, cuando lo hizo (fecha y hora), tipo de acceso y si ha sido autorizado o denegado. En el caso que el acceso haya sido autorizado se deberá identificar el dato accedido y el tratamiento que se le dio al mismo (baja, rectificación, etc.). Este registro de accesos deberá ser analizado periódicamente por el responsable de seguridad y deberá ser conservado como mínimo 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.