Dirección Nacional de Protección de Datos Personales

PROTECCION DE DATOS PERSONALES

Disposición 9/2008

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. Prorrógase el plazo establecido por la Disposición Nº 11/2006.

Bs. As., 1/9/2008

VISTO el Expediente Nº 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 Nº 25.326 y su reglamentación aprobada por Decreto Nº 1558 del 29 de noviembre de 2001, y

CONSIDERANDO:

Que por Disposición DNPDP Nº 11, de fecha 19 de setiembre de 2006, se aprobaron 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".

Que asimismo se establecieron distintos plazos para la entrada en vigencia de las medidas de seguridad según que, por la naturaleza de la información tratada, correspondiere adoptar las de Nivel Básico, Medio o Crítico.

Que se determinó que a los DOCE (12) meses de entrada en vigencia de la citada disposición, serían obligatorias las Medidas de Seguridad de Nivel Básico, así como que a los VEINTICUATRO (24) meses ocurriría lo mismo con las de Nivel Medio y a los TREINTA Y SEIS (36) meses con las de Nivel Crítico.

Que la norma prevé la prorrogabilidad de tales plazos a pedido de parte interesada y por razones debidamente fundadas.

Que el 22 de setiembre del corriente año entrarán en vigencia las Medidas de Seguridad de Nivel Medio.

Que habiéndose observado que aún no se han internalizado adecuadamente las Medidas de Seguridad de Nivel Básico, resulta conveniente prorrogar el plazo de entrada en vigencia de los Niveles Medio y Crítico con carácter general, de modo que los requisitos contemplados en el Nivel Medio sean exigibles recién dentro de DOCE (12) meses y los de Nivel Crítico a partir de los VEINTICUATRO (24) meses, en ambos casos contados a partir de la fecha del presente.

Que la citada disposición también estableció que los archivos, registros, bases y bancos de datos personales debían disponer de un "Documento de Seguridad de Datos Personales", en el que se especificara la normativa de seguridad aplicable.

Que a fin de facilitar la implementación del referido documento y la efectiva puesta en funcionamiento de medidas técnicas que garanticen la seguridad y la confidencialidad en el tratamiento de datos personales, resulta adecuado propiciar desde este Organo de Control un Modelo de Documento de Seguridad que contenga lineamientos indispensables mínimos que permitan a los obligados diseñar un instrumento que se adecue a las necesidades de su organización y cumpla con las normas dictadas en la materia.

Que la necesidad de proponer un texto de "Documento de Seguridad", se fundamenta en la circunstancia de haberse advertido dificultades en la elaboración del referido documento por parte de algunos responsables y usuarios de bases de datos personales.

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 en uso de las facultades conferidas en el artículo 29, inciso 1, apartado b, de la Ley Nº 25.326 y artículo 29, inciso 5, apartados a y e, del Anexo al Decreto Nº 1558/01.

Por ello,

EL DIRECTOR NACIONAL DE PROTECCION DE DATOS PERSONALES

DISPONE:

Artículo 1º — Prorrógase el plazo establecido por la Disposición DNPDP Nº 11/06 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 del presente acto. Dicho plazo será prorrogable a pedido de la parte interesada y por razones debidamente fundadas.

Art. 2º — Apruébase el "Documento de Seguridad de Datos Personales", que como Anexo I forma parte integrante del presente.

Art. 3º — Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese. — Juan A. Travieso.

ANEXO I

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

————————————————————————

Responsable de los Datos: (nombre de la firma /organización)

CUIT: (CUIT de la firma)

Domicilio: (calle - Nº - piso/of. - Cód. Post. - Ciudad – Provincia)

Teléfono: Nº **Email:**

Inscripción en el Registro Nacional de Bancos de Datos Nº: (indicar número de inscripción)

Fecha de la última Renovación: dd/mm/aa *Validez UN año.*

Persona de contacto de la firma / organización: (nombre, apellido y datos para contactarla)

————————————————————————

Responsable de la gestión de la seguridad en la firma: (nombre y apellido)

Categoría / Jerarquía / Rango:

CUIT o CUIL: (CUIL del responsable)

————————————————————————

Fecha de revisión y aplicación: dd/mm/aa

Vencimiento: dd/mm/aa

————————————————————————————

Alcance:

Estas medidas de seguridad son las definidas como de NIVEL BASICO, un mínimo que puede ser mejorado; y se aplican a la información consignada en las inscripciones realizadas en la DNPDP, y a sus sistemas de gestión (programas, archivos, tareas contratadas, etc.).

Su finalidad es mantener la Integridad, Accesibilidad y Confidencialidad de los datos personales, y se revisan y/o actualizan al menos una vez al año.

1- Funciones y obligaciones del personal o contratados.

Se informa adecuadamente y se compromete a todo el personal y/o proveedores con acceso a los datos personales, a observar estricta confidencialidad de la información que posee la empresa mediante la firma de una "Obligación de confidencialidad" como la que se transcribe, o similar.

Obligación de confidencialidad: El que suscribe …(nombre apellido, CUIT-CUIL)…, empleado (o proveedor con acceso a los datos), asume el compromiso de mantener estricto secreto y confidencialidad de la información a la que accede, no debiendo exteriorizarla parcial ni totalmente sin autorización. Por el presente me notifico del carácter confidencial que reviste la información que posee el responsable de los datos y me comprometo a no usarla ni revelarla sin su consentimiento. Los datos personales presentes, su mera posesión, tratamiento, cesión o divulgación se hallan protegidos y regulados por la Ley Nº 25.326 de Hábeas Data (http://www.jus.gov.ar/datospersonales/pdf/ley_ 25326.pdf), siendo la Dirección Nacional de Protección de Datos Personales, del Ministerio de Justicia, Seguridad y Derechos Humanos, el Organo de control de la citada norma legal(http://www.jus.gov.ar/datospersonales/).

Se pueden definir **perfiles** como Jefe o Secretaria, si la firma los posee, y asignar a cada perfil, obligaciones y "privilegios". Puede haber varios empleados bajo un mismo perfil.

Jefe, Socio Gerente, Presidente o dueño del estudio, fábrica, comercio.

Obligaciones: titular de la empresa máximo responsable, asignación de responsabilidades a subalternos, tareas, limitaciones.

Secretaria

Obligaciones: mantener agendas actualizadas, asignar turnos, facturar, cobrar, otras especificar**.**

Empleado Administrativo

Obligaciones:

• Operar el sistema, contabilizar, solicitar compras, emitir facturas, cobrar, liquidar sueldos.

• Mantener la información segura realizando backups, contabilizar y almacenar los backups bajo llave, mantener el área de administración cerrada, correr rutinas de actualización de antivirus.

• otras especificar.

Proveedor externo y service de sistemas (Consignar nombre y CUIT)

Obligaciones:

• Mantener los sistemas de información funcionando correctamente manteniendo la integridad de los datos personales.

- Acceder a toda la información que la empresa guarda en sus sistemas.

- Otras especificar

2- Descripción de los archivos con datos personales y los sistemas que los tratan

Listado de clientes, listado de proveedores, listado de personal, otros especificar.

Se utiliza programa de gestión administrativa marca y versión especificar.

Sistema operativo marca y versión especificar.

3- Descripción de las rutinas de control de datos y acciones a seguir ante errores.

Se instruye al personal involucrado para percibir las posibles inconsistencias u errores y corregirlos en el momento en el que tomen cuenta si el sistema lo permite, o den aviso al idóneo con la posibilidad de corregirlos.

4- Registros de incidentes de seguridad. Notificación, gestión y respuesta.

Se crea en el programa de email una carpeta DNPDP, y luego se pasan a ella todos los emails referidos a protección de datos personales.

Cuando ocurre algo que se considere un incidente de seguridad se redactan uno o más emails describiendo lo sucedido y las acciones tomadas para su solución y se los envía a otra cuenta.

Quedan de este modo registradas en esos emails, las fechas y horas, las características, y la solución del incidente.

También se puede llevar registro de incidentes en un capítulo de un Cuaderno de Informes de Sistemas donde se reportan todos los acontecimientos referidos a la Protección de Datos Personales, que se guarda bajo llave en el escritorio de Secretaria.

5- Procedimiento para efectuar las copias de respaldo y recuperación de datos (Backups)

Se copian las carpetas Documentos y …(especificar otras)… a dos CD-ROM, y se verifica el correcto copiado con la rutina del programa de copiado, y también leyéndolos.

Se consigna en la superficie de los CDs la fecha, y las carpetas que se han copiado en él.

Se guarda un CD bajo llave en un mueble de la oficina de administración y otro es llevado al domicilio particular del dueño de la firma.

6- Relación actualizada entre los Sistemas de Información y Usuarios de datos.

Los Usuarios de datos son todos aquellos quienes utilizan los datos que almacena la firma: los empleados administrativos, secretarias, vendedores, etc.

No siempre cualquier empleado puede acceder a cualquier dato o función, el privilegio para acceder a tales o cuales datos o funciones se otorgan a cada perfil: "Jefe", "Secretaria", "Administrativo 1º", "Administrativo 2º", etc.

Esta Relación entre los Sistemas y Usuarios, es congruente con los "privilegios" de cada perfil.

Jefe, Socio Gerente, Presidente o dueño del estudio, fábrica, comercio.

SI Acceso a: toda la información de la compañía.

Secretaria

SI Acceso a: Todo menos lo especificado en NO.

NO Acceso a: legajos de personal, otras especificar.

Administrativo (engloba a todos los administrativos en general).

SI Acceso a: particularizado para cada subperfil.

NO Acceso a: particularizado para cada subperfil.

Administrativo 1º General, Personal

SI Acceso a: información de clientes, proveedores, personal, Internet, otras especificar

NO Acceso a: agenda personal de Jefe, otras especificar.

Administrativo 2º Compras, Ventas

SI Acceso a: información de clientes, proveedores, Internet, otras especificar

NO Acceso a: agenda personal de Jefe, legajos de personal, otras especificar

Proveedor de sistemas informáticos, o de archivo de documentación o datos.

SI Acceso a: toda la información de la compañía con limitaciones y obligaciones descriptas en contrato de servicio y/o la "Obligación de confidencialidad".

7- Procedimientos de identificación y autenticación de los Usuarios de datos.

El sistema posee "Cuentas de Usuario" únicas, que se asignan a cada persona que accede a él.

Cada cuenta posee una "password" secreta, sólo conocida por el usuario, que es requerida para autenticarse y acceder al sistema.

La password posee no menos de ocho caracteres y debe ser cambiada por el usuario cada 30 días ya que caduca automáticamente.

8- Control de acceso de Usuarios de datos.

De acuerdo a su "perfil" se asignan a los Usuarios llaves de las puertas de ingreso a cada sector de la firma.

Se asignan muebles y cajoneras con llaves particulares para cada Usuario.

En el sistema informático cada Usuario posee una cuenta con su "password", y con sus particulares "privilegios" de acceso a determinada información.

9- Medidas de prevención frente a amenazas de software malicioso.

El sistema operativo posee un "Módulo de Seguridad" con Firewall para evitar el acceso no deseado de intrusos a través de la red Internet, y programa Antivirus residente en memoria que limita el ingreso de virus a través de redes, disquetes, CDs u otros dispositivos de ingreso.

Este "Módulo de Seguridad" cuenta con una solicitud periódica y automática de actualización, que se lleva a cabo cada vez que ocurre.

10- Procedimiento que garantice la adecuada Gestión de los Soportes de datos.

Los soportes de datos de respaldo, ej. CD-ROMs de Backup, se etiquetan indicando, fecha, y contenidos en general.

Se asienta el backup en un capítulo que contiene el Cuaderno de Informes de Sistemas, donde copian lo escrito en la etiqueta del CD.

Se redacta un email con idéntico contenido, se lo envía a otra cuenta y se lo pasa a la carpeta DNPDP previamente creada.

Se guarda un CD bajo llave en un mueble de la oficina de administración y otro es llevado al domicilio particular del dueño de la firma.

Cuando la información de un soporte de datos ya no sea útil y haya prescripto, se procederá a su destrucción, rayando su superficie y partiéndolo en pedazos antes de tirarlo a la basura.

Se realizan el asiento de la operación en el Cuaderno de Informes de Sistemas, y en el email.

Firma	Firma
Responsable de los Datos Personales	Responsable de Seguridad
DNI – CUIT	DNI – CUIT - CUIL