CPCECABA Comisión de Sistemas de Registros, su integridad y autenticidad documental

Material entregado en la RCyT Caso Práctico de Revisión de la Ley 25326 Setiembre 2011

Programa de revisión

Objetivo: Aplicación de las Normas de Inspección y Control aprobadas por la Disp.5/2008 de la DNPDP (Punto 4 Metodología de la Inspección)en la resolución del Caso Práctico de revisión entregado en la RCyT Setiembre 2011

Programa de revisión	Si/No/ Parc./ N/A	Observ
4.1 Acreditaciones obligatorias del Responsable		
4.1.1 Verificar la acreditación de Personería		
4.1.2 Verificar el registro en la DNPDP		
4.2 Acreditaciones optativas		
Verificar la existencia de las siguientes Acreditaciones: 4.2.1 Anses 4.2.2 ART 4.2.3 Habilitación municipal 4.2.4 CUIT		
4.3 Legalidad y corrección de los datos objeto de tratamiento		
4.3.1 Licitud del tratamiento de datos personales		
4.3.1.1 Relevar y verificar con la inscripción en el Registro los Tipos de datos que se gestionan		
4.3.1.2 Relevar y verificar con la inscripción en el Registro la Finalidad del tratamiento, servicios que se prestan		
4.3.1.3 Relevar y verificar con la inscripción en el Registro el Origen y fuente de los datos, formas de recolección.		
4.3.1.3.1 Relevar y verificar los procesos de incorporación de datos a la base		
4.3.1.3.2 Mediante la selección de una muestra comprobar la existencia de consentimientos firmados a fin de verificar el consentimiento del titular para el tratamiento de sus datos		
4.3.1.4 Relevar y verificar el cumplimiento de lo establecido en el art 11 de la Ley (y reglamento) en cuanto a la Cesión de datos a terceros		
4.3.1.5 Relevar y verificar el cumplimiento de lo establecido en el art 12 de la Ley (y reglamento) en cuanto a Transferencia internacional de datos personales		
4.3.1.6 Relevar y verificar la aplicación de Mecanismos de disociación personal de acuerdo a lo establecido en el art 11 inc 6.		
4.3.1.7 Relevar y verificar el cumplimiento de lo establecido en el art 4 inc 7 de la Ley (y reglamento) en cuanto a la Destrucción de la información:		

4.3.1.7.1 Verificación de la Utilidad o pertenencia de la información registrada		
4.3.1.7.2 Periodicidad de la verificación		
4.3.1.7.3 Forma de destrucción		
4.3.2 Inscripciones vigentes en la DNPDP para los tratamiento de datos inspeccionados		
4.3.2 Verificar las inscripciones vigentes en la DNPDP para los tratamiento de datos inspeccionados, según art 21 de la Ley y reglamento		
4.3.3 Medidas de seguridad de la información		
4.3.3.1. Relevar y verificar el **cumplimiento de la Disposición DNPDP N°11/06**: **Medidas de seguridad Nivel Básico:** Contenido del Documento de Seguridad de Datos Personales de acuerdo a los establecido por la Disposición 11/2006 de la DNPDP:		
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 la rutinas de control de datos de los programas de ingreso de datos que minimicen la posibilidad de incorporar al sistema de información datos ilógicos, incorrectos o faltantes. Descripción de las acciones a seguir ante los errores detectados a efectos de su corrección.		
4. Registros de incidentes de seguridad		
5. Procedimientos para efectuar las copias de respaldo y de recuperación de datos		
6. Relación actualizada entre Sistemas de Información y usuarios de datos con autorización para su uso.		
7. Procedimientos de identificación y autenticación de los usuarios de datos autorizados para utilizar determinados sistemas de información		
8. Control de acceso de usuarios a datos y recursos necesarios para la realización de sus tareas para lo cual deben estar autorizados.		
9. Adoptar medidas de prevención a efectos de impedir amenazas de software malicioso (virus, troyanos, entre otros), que puedan afectar archivos con datos de carácter personal		
10. Procedimiento que garantice una adecuada gestión de soportes que contengan datos de carácter personal (identificación del tipo de información que contienen, almacenamiento en lugares de acceso restringido, autorización para su salida fuera del local en que están ubicados, destrucción de información en desuso, etc.)		
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 nivel Básico más las establecidas en los puntos 2,3,4 y 5 del Nivel Medio.		
Medidas de seguridad Nivel Medio		

CPCECABA Comisión de Sistemas de Registros, su integridad y autenticidad documental

Alcance: archivos, registros, bases y bancos de datos que contengan 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 las 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 (por ejemplo secreto bancario		
1.El Instructivo de seguridad deberá identificar al Responsable (u órgano específico) de seguridad		
2. Realización de auditorías (internas/externas) que verifiquen el cumplimiento de los procedimientos e instrucciones vigentes en materia de seguridad de datos personales Los informes de auditoría pertinentes serán presentados al Responsable del archivo a efectos de que se adopten las medidas correctivas que correspondan.		
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/ Registro de entradas y salidas de soportes informáticos		
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.		
Medias de seguridad de Nivel Crítico Archivos, registros, bases y bancos de datos que contengan datos personales, definidos como 'datos sensibles'. Excepciones: archivos, registros, bases y bancos de datos que deban efectuar el tratamiento de datos sensibles para fines administrativos o por obligación legal. No obstante, ello no excluye que igualmente deban contar con aquellas medidas de resguardo que sean necesarias y adecuadas al tipo de dato.		
1.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, cuándo 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 (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 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 externa, 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 esa información y de tratamiento de la misma en caso de contingencias que pongan no operativo el/los equipos de procesamiento habituales.		
4.Transmisión de datos: los datos de carácter personal que se transmitan a través de redes de comunicación, deberán serlo cifrados o utilizando cualquier otro mecanismo que impida su lectura y/o tratamiento por parte de personas no autorizadas Tratamiento: automatizado		
4.3.4 Política de privacidad y confidencialidad del responsable		
4.3.4.1.Verificar la existencia de una política de privacidad		
4.3.4.2 Relevar y verificar el grado de cumplimiento de la política de privacidad		
4.3.4.3 Relevar y verificar la publicidad y difusión de la política de privacidad		
4.3.4.4 Mediante la selección de una muestra comprobar la existencia de convenios de confidencialidad firmados por los empleados, usuarios o terceros que accedan a la información registrada en la base de datos		
4.3.4.5 Verificar que el responsable adopta los mecanismos para evaluar el cumplimiento de la política de privacidad y de los convenios de confidencialidad		
4.3.5 Casos especiales Cumplimiento de la normativa específica		
4.3.5.1.1 Datos relativos a la salud: Establecimiento sanitarios y profesionales de la salud Relevar y verificar el cumplimiento del art 8 de la Ley		
4.3.5.2 Tratamiento de datos por cuenta de terceros		
4.3.5.2.1.Verificar la existencia de Contrato de servicio firmado y adecuado (art 25 de la Ley)		
4.3.5.2.2 Verificar el contenido del Contrato y constatar que exprese el uso posterior de los datos una vez cumplido el contrato (conservación o destrucción)		
4.4 Idoneidad de los medios empleados en el tratamiento de los datos y gestiones anexas		
4.4.1 Materiales: instalaciones y medios de almacenamiento		
4.4.4.1 Relevar y verificar si son compartidas y exclusivas		
4.4.1.2 Relevar y verificar el grado de privacidad/seguridad en las operaciones		
4.4.2 Sistemas, software		
4.4.2.1. Relevar y verificar los medios de seguridad contra acciones no permitidas (por ejemplo, accesos no autorizados, software malicioso)		
4.4.3 Personal: Entrevistar al personal de las siguientes áreas a fin de determinar su calificación		

-Diseño de sistemas y gestión de sistemas - Atención de titulares y usuarios -Legales Relevar: -Conocimiento de responsabilidad vinculada al tratamiento de datos personales, los derechos de los titulares y las obligaciones de la Ley -Estudios y formación vinculados a la protección de los datos personales -Para los 2 últimos, capacidad de trato, actitud frente a terceros y capacidad de comunicación		
4.4.4 Procedimentales 4.4.4.1Derecho de acceso según art. 14 y 15 de la Ley (y reglamento) 4.4.4.2 Rectificación, Actualización, Supresión, Bloqueo según art. 16 de la Ley (y reglamento)		
4.4.4.1Derecho de acceso según art. 14 y 15 de la Ley Relevar y verificar los siguientes aspectos: -Personas a cargo, calificación -Recepción de solicitud (formas, lugar, horario) -Verificación de la identidad del solicitante -Elaboración de la respuesta, colección de la información, redacción, presentación (papel, archivo) -Entrega de la respuesta, formas y procedimiento (correo, mail, fax) -Registro del caso (ticket, archivo) -Seguimiento -Tiempo transcurrido entre la solicitud y la recepción de la respuesta.		
4.4.4.2 Rectificación, Actualización, Supresión, Bloqueo según art. 16 de la Ley (y reglamento) Relevar y verificar los siguientes aspectos: -Personas a cargo, calificación -Recepción de solicitud (formas, lugar, horario) -Verificación de la identidad del solicitante -Elaboración de la respuesta, colección de la información, redacción, presentación (papel, archivo) -Entrega de la respuesta, formas y procedimiento (correo, mail, fax) -Registro del caso (ticket, archivo) -Seguimiento -Tiempo transcurrido entre la solicitud y la recepción de la respuesta.		
4.5 Acatamiento de las disposiciones de la DNPDP **Disposiciones particulares acaecidas en sumarios tramitados ante la DNPDP en los que el responsable de la base de datos haya sido parte.**		