DISPOSICION 3/2012

Buenos Aires, 31/7/2012.
Fecha de publicación: 07/08/2012.

VISTO el Expediente N° S04:0020164/2011 del registro de este Ministerio, la LEY DE PROTECCION DE LOS DATOS PERSONALES N° 25.326 y su Decreto Reglamentario N° 1558 del 29 de noviembre de 2001, modificado por su similar N° 1160 del 11 de agosto de 2010 y las Disposiciones Nros. 011 del 19 de septiembre de 2006 y 005 del 28 de mayo de 2008 de esta Dirección Nacional, y

CONSIDERANDO:

Que la Ley N° 25.326 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, así como también el acceso a la información que sobre los mismos se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la CONSTITUCION NACIONAL.

Que es facultad de esta Dirección Nacional diseñar los instrumentos que considere adecuados para la mejor protección de los datos personales y para el cumplimiento de sus funciones y atribuciones.

Que de conformidad con lo establecido en el artículo 29, incisos b) y e), de la Ley N° 25.326, se encuentran entre sus funciones y atribuciones, las de dictar las normas y reglamentaciones que se deben observar en el desarrollo de sus actividades y las de solicitar la información pertinente a las entidades públicas y privadas, en orden a proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos que se le requieran.

Que a su vez el artículo 31 de la Ley N° 25.326 prevé que la reglamentación determinará las condiciones y procedimientos para la aplicación de las sanciones allí previstas y que corresponda aplicar en casos de inobservancia de los preceptos contenidos en la Ley citada.

Que asimismo es responsabilidad del Organo de Control de la Ley N° 25.326 la realización de investigaciones e inspecciones, el requerimiento de información, antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales a los responsables o usuarios de archivos, como así también la de controlar la observancia de las normas sobre integridad y seguridad de esos datos por parte de los titulares o usuarios de archivos, registros o bancos de datos.

Que la experiencia recogida en el curso de la gestión llevada a cabo por esta Dirección Nacional en relación con la mencionada actividad, impone la necesidad de realizar modificaciones en los instrumentos de inspección implementados mediante la Disposición DNPDP N° 005/08.

Que en ese entendimiento y a fin de optimizar el procedimiento de inspección de los archivos, registros, bases o bancos de datos públicos y privados previstos en la Ley N° 25.326 y en la Disposición DNPDP N° 005/08, esta Dirección Nacional considera necesario reemplazar las NORMAS DE INSPECCION Y CONTROL DE LA DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES oportunamente aprobadas por la Disposición DNPDP N° 005/08 como Anexo I, por nuevos instrumentos bajo los nombres de “Formulario de Inspección” e “Instructivo del Formulario de Inspección”, obrantes en los Anexos I y II, respectivamente.

Que mediante dichos instrumentos se prevé otorgar mayor celeridad y eficacia a la actividad fiscalizadora, teniendo en miras facilitar a los inspeccionados los elementos de juicio necesarios para la observancia de los principios y requisitos de licitud que establece la Ley N° 25.326.

Que a fin de observar una mejor técnica legislativa que permita contener en un solo cuerpo normativo el régimen regulatorio de la actividad de contralor de los principios enunciados en la Ley N° 25.326 y otorgue mayor transparencia y seguridad en el tratamiento de datos personales a quienes resultan alcanzados por aquélla, se impone derogar la Disposición DNPDP N° 005/08 y aprobar el nuevo cuerpo dispositivo que conforma el procedimiento de fiscalización aludido precedentemente.

Que ello permitirá a esta Dirección Nacional efectuar las correcciones y recomendaciones que resulten necesarias para mejorar su gestión y proteger debidamente los derechos del titular del dato.

Que ha tomado la intervención de su competencia la DIRECCION GENERAL DE ASUNTOS JURIDICOS de este Ministerio.

Que la presente disposición se dicta en uso de las facultades contenidas en los artículos 29, inciso 1, apartados b) y e), de la Ley N° 25.326, 29, inciso 5, apartado a), del Anexo I del Decreto N° 1558/01 y 1°, inciso V), del Decreto N° 1160/10.

Por ello,

EL DIRECTOR NACIONAL
DE PROTECCION DE DATOS PERSONALES
DISPONE:

Artículo 1° — Apruébanse el "Formulario de Inspección" obrante en el Anexo I del presente acto y el "Instructivo del Formulario de Inspección" agregado como Anexo II.

Art. 2° — El ejercicio de la facultad de fiscalización que tiene asignada esta Dirección Nacional se desarrollará de oficio y cuando estime corresponder, si bien podrá tener causa en una petición o denuncia de un órgano del Estado Nacional, provincial, municipal o un particular.

Art. 3° — Las inspecciones y controles serán efectuados por un agente de la planta permanente de esta Dirección Nacional debidamente acreditado, quien revestirá el carácter de inspector y podrá estar acompañado por el personal técnico que sea designado a tal fin por el Director Nacional de Protección de Datos Personales a propuesta del titular del área requerida. En todos los casos y de considerarlo pertinente, el Director Nacional de Protección de Datos Personales podrá estar presente en la inspección.

Art. 4° — La iniciación de la inspección se instrumentará mediante decisión del Director Nacional de Protección de Datos Personales y será debidamente notificada al responsable de la base de datos sujeta a control con una antelación no inferior a DIEZ (10) días hábiles, salvo que se entienda que la previa notificación pueda afectar el resultado de la investigación, en cuyo caso deberá constar la pertinente justificación en el acto de apertura de la inspección. En caso de efectuarse notificación, la misma deberá ir acompañada por una copia de los textos correspondientes al "Formulario de Inspección" y su Instructivo, aprobados como Anexos I y II de la presente.

Art. 5° — La inspección consistirá en una o más visitas presenciales del inspector, en la que podrá acceder a la totalidad de los locales, equipos o programas de tratamiento de datos personales del responsable de la base de datos controlada. Dichas visitas se harán en días y horas hábiles administrativos, sin perjuicio de lo cual de oficio o a petición de parte podrán habilitarse aquellos que no lo fueren.

Art. 6° — La inspección se desarrollará conforme lo disponen los puntos del "Formulario de Inspección" y el "Instructivo del Formulario de Inspección", en forma total o parcial según el alcance objetivo o causal del control y a las características del tratamiento de datos bajo inspección.

Art. 7° — En los casos en que las circunstancias fácticas y el tipo de tratamiento de datos así lo exijan, se podrá solicitar a los controlados la presentación de elementos adicionales que permitan fiscalizar el cumplimiento de las obligaciones y principios contenidos en la Ley N° 25.326 y su reglamentación, en el marco de las competencias asignadas a esta Dirección Nacional.

Art. 8° — Los actos de inspección constarán en un acta que será labrada por duplicado por el inspector y suscripta por el mismo, por los técnicos que lo acompañen, en su caso y por

el responsable de la base de datos controlada. El original se incorporará a las actuaciones que dieron origen a la inspección y el duplicado será entregado al responsable de la base de datos.

Art. 9° — En caso de que resultare necesario solicitar autorización judicial para acceder a locales, equipos o programas de tratamiento de datos, a fin de verificar infracciones al cumplimiento de la Ley N° 25.326, el inspector deberá elevar la respectiva petición al Director Nacional de Protección de Datos Personales, quien formulará el correspondiente requerimiento.

Art. 10. — Derógase la Disposición DNPDP N° 005 del 28 de mayo de 2008.

Art. 11. — Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese. — Juan A. Travieso.

ANEXO I

FORMULARIO DE INSPECCION

El presente documento tiene por objetivo facilitar la determinación de los distintos tratamientos de datos que realizan los responsables y verificar si los mismos se ajustan a los principios y requisitos de licitud que establece la Ley Nº 25.326, lo que permitirá a la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES efectuar las correcciones y recomendaciones que resulten necesarias para mejorar la gestión y la protección de los derechos del titular del dato.

A. IDENTIFICACION DEL RESPONSABLE:

1. NOMBRE DEL RESPONSABLE Y ACREDITACION DE PERSONERIA
2. NUMERO DE CUIT/CUIL/CDI DEL RESPONSABLE

B. DESARROLLO DE LA INSPECCION:

	NA	SI	NO
3. NUMERO DE REGISTRO ANTE LA DNPDP			
Observaciones:			
4. BANCOS DE DATOS INSCRIPTOS ANTE LA DNPDP			
Observaciones:			
5. POLITICA DE PRIVACIDAD			
Observaciones:			
5.a. Designa encargado de la Política de Privacidad			
Observaciones:			
5.b. Difunde y capacita respecto de la Política de Privacidad			
Observaciones:			
5.c. Incorpora el control de cumplimiento de la Política de Privacidad en sus procesos de auditoría			
Observaciones:			
6. CALIDAD DE LOS DATOS (artículo 4° Ley Nº 25.326)			
6.a. Determina la finalidad del tratamiento de los bancos de datos			
Observaciones:			
6.b. Determina la categoría de los datos admisibles en sus bancos de datos			
Observaciones:			
6.c. Trata datos sensibles (artículos 2° y 7° Ley Nº 25.326)			
Observaciones (en caso afirmativo, especificar razón de interés general fundada en ley que autorice su tratamiento y medidas de seguridad aplicadas a los mismos):			
6.d. Toma medidas para garantizar la calidad del dato objeto de tratamiento			
Observaciones:			
6.e. Verifica la utilidad de los datos en forma periódica			
Observaciones:			
7. RECOLECCION DE LOS DATOS (artículos 5° y 6° Ley Nº 25.326)			
7.a. Verifica el origen de los datos (fuentes) y su licitud			
Observaciones:			
7.b. Recolecta los datos conforme requisitos de la Ley (artículos 5°, 6°, 26 y 27 Ley Nº 25.326)			
Observaciones:			
7.c. Cumple en brindar el derecho de información al titular del dato (artículo 6° Ley Nº 25.326)			
Observaciones:			
7.d. Recaba el consentimiento del titular del dato (de ser exigible)			
Observaciones:			
8. CESION DE DATOS (artículo 11 Ley Nº 25.326)			
8.a. Determina los destinatarios de cesiones actuales o eventuales			
Observaciones:			
8.b. Posee el consentimiento previo del titular del dato (de ser exigible)			
Observaciones:			
9. CONFIDENCIALIDAD (artículo 10 Ley Nº 25.326)			
Posee convenios de confidencialidad firmados por los empleados, usuarios o terceros que accedan a la información registrada en la base de datos			
Observaciones:			
10. MEDIDAS DE SEGURIDAD (artículo 9° Ley Nº 25.326 y Disposición DNPDP Nº 11/06)			
Observaciones:			
10.a. NIVEL BASICO			
10.a.1. Posee documento de seguridad			
10.a.2. Asigna funciones y obligaciones del personal respecto al tratamiento de datos personales			
10.a.3. Documenta sus bancos de datos y los sistemas de información que los almacenan			
10.a.4. Establece medidas de control de calidad de la información a incorporar al banco de datos			
10.a.5. Registra y prevé medidas ante *incidentes de seguridad*			
10.a.6. Realiza copias de resguardo de la información periódicos			
10.a.7. Mantiene un control actualizado de los usuarios del sistema, autorizados mediante claves			
10.a.8. Gestiona adecuadamente las claves y las renueva periódicamente			
10.a.9. Prevé medidas para proteger la información de equipos desatendidos			
10.a.10. Establece protección permanente y actualizada contra accesos no autorizados, virus y software malicioso			
10.a.11. Prevé medidas técnicas para el correcto funcionamiento de los equipos (instalación, temperatura ambiente) o evitar su daño por elementos externos como el fuego, etc.			
10.a.12. Posee política de gestión de soportes de datos personales, sean en papel o cualquier otro dispositivo técnico (inventario, almacenamiento, procedimientos en caso de extracción, salidas o destrucción por desuso)			
10.b. NIVEL MEDIO Permita establecer el perfil de personalidad o conductas determinadas de las persona o resulte afectada por secreto legal específico o empresas privadas de servicios públicos.			
10.b.1. Designa responsable de Seguridad			
10.b.2. Incorpora el control de medidas de seguridad de datos personales en sus procesos de auditoría			
10.b.3. Impide la reiteración de intento de acceso no autorizado al sistema de Información			
10.b.4. Prevé medidas físicas para evitar el acceso indebido a la zona del centro de cómputos y depósito de soportes de almacenamiento de información			
10.b.5. Posee procedimiento de recuperación de la información de respaldo y tratamiento de la misma en caso de contingencia que ponga no operativo el o los equipos de procesamiento habituales			
10.b.6. Toma medidas de protección de los datos personales cuando son transmitidos por redes internas o externas a la empresa			
10.b.7. En caso de incidentes de seguridad de la información, autoriza e identifica la persona que recupero y/o modificó dicho datos			
10.b.8. Las pruebas de funcionamiento de los sistemas de información se realizan en paralelo al sistema real			
10.c. NIVEL CRITICO Contenga "datos sensibles" cuyo tratamiento no sea obligatorio o para fines meramente administrativos (ej. Administración del personal).			
10.c.1. Distribución de Soportes: Encripta los datos cuando se trasladen en soportes o se realicen copias de resguardo de la información			
10.c.2. Lleva registro de acceso al sistema de los operadores y administrador (log, usuario, fecha, hora, autorizado, denegado, tipo de operación realizada)			
10.c.3. Deposita copias de seguridad del sistema fuera de la localización habitual, en caja ignifuga y a prueba de gases o bien en una caja de seguridad bancaria, situadas a una distancia prudencial			
10.c.4. Encripta los datos de carácter personal que se trasmiten a través de redes de comunicación			
11. ACTIVIDADES DE PUBLICIDAD DIRECTA (artículo 27 Ley Nº 25.326)			
11.a. Utiliza sólo las categorías autorizadas (inciso 1º artículo 27 Ley 25.326 y Decreto)			
Observaciones:			
11.b. Recaba los datos de fuentes legítimas (inciso 1º artículo 27 Ley 25.326 y Decreto)			
Observaciones:			
11.c. Respeta derecho de acceso del titular del dato (inciso 2º artículo 27 Ley Nº 25.326)			
Observaciones:			
11.d. Respeta derecho de retiro o bloqueo del titular del dato (inciso 3º artículo 27 Ley Nº 25.326)			
Observaciones:			

12. TRANSFERENCIA INTERNACIONAL (artículo 12 Ley Nº 25.326)			
Observaciones:			
12.a. La realiza mediante contrato de transferencia Internacional			
Observaciones (en caso de contar con la aprobación de esta Dirección Nacional, consignar dicha circunstancia):			
12.b. La realiza mediante consentimiento del titular del dato			
Observaciones:			
13. TRATAMIENTO DE DATOS POR CUENTA DE TERCEROS (artículo 25 Ley Nº 25.326)			
13.a. Posee contrato de servicios de tratamiento por parte de terceros			
Observaciones:			
13.b. Determina la finalidad del tratamiento			
Observaciones:			
13.c. Determina medidas de seguridad y confidencialidad			
Observaciones:			
13.d. Determina el plazo de conservación de los datos			
Observaciones:			
14. DERECHOS DEL TITULAR DEL DATO (articulos 14, 15 y 16 Ley Nº 25.326)			
14.a. Establece procedimientos y plazos de ley para el derecho de acceso			
Observaciones:			
14.b. Establece procedimientos y plazos de ley para el derecho de rectificación			
Observaciones:			
15. CAPACITACION			
15.a. Verifica capacitación a nivel general de la empresa			
Observaciones:			
15.b. Verifica capacitación específica del área de sistemas			
Observaciones:			
15.c. Verifica capacitación específica del área atención al público/clientes			
Observaciones:			
15.d. Verifica capacitación específica del área recursos humanos			
Observaciones:			
16. ACATAMIENTO DE LAS DISPOSICIONES DE LA DNPDP			
16.a. Constata correcto acatamiento Disposiciones de la DNPDP			
Observaciones:			
16.b. Verifica acatamiento de disposiciones particulares acaecidas en sumarios tramitados ante la DNPDP en los que el responsable de la base de datos haya sido parte			
Observaciones:			

C. CASOS ESPECIALES:

17. ESTABLECIMIENTOS SANITARIOS Y MEDICOS (artículos 7° y 8° Ley Nº 25.326)			
Toma medidas que garanticen el secreto profesional			
Observaciones:			
18. INVESTIGACIONES CLINICAS, FARMACOLOGICAS Y FARMACOGENETICAS (artículos 7° y 8° Ley Nº 25.326)			
Utiliza modelos de consentimiento informado aprobado por la DNPDP			
Observaciones:			
19. EMPRESAS DE INFORMES CREDITICIOS (artículo 26 Ley Nº 25.326)			
19.a. Utiliza sólo las categorías autorizadas (incisos 1 y 2)			
Observaciones:			
19.b. Recaba los datos de fuentes legítimas (incisos 1 y 2)			
Observaciones:			
19.c. Respeta derecho de acceso del titular del dato (inciso 3)			
Observaciones:			
19.d. Aplica los plazos de caducidad del dato (inciso 4)			
Observaciones:			
19.e. Controla existencia de interés legítimo del cesionario (inciso 5)			
Observaciones:			

INSTRUCTIVO DEL FORMULARIO DE INSPECCION

Objetivos

El Formulario de Inspección es un instrumento coadyuvante de las finalidades de toda inspección:

— Concientizar a los responsables o titulares de los bancos de datos, sobre los alcances y aplicación a su actividad de la LEY DE PROTECCION DE LOS DATOS PERSONALES Nº 25.326.

— Determinar el efectivo cumplimiento de la Ley por parte del responsable y realizar las recomendaciones necesarias para la mejor protección de los datos personales.

— De detectarse infracciones: otorgar plazo de subsanación y/o aplicar sanción —previo sumario— conforme a la Disposición DNPDP Nº 7/2005, según la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES considere pertinente.

Metodología

El Formulario de Inspección se completará previo a la visita de inspección (por parte del responsable) y/o al momento de la visita (por parte del inspector), de lo que se dejará constancia en el Acta de Inspección.

Instrucciones para su llenado

En cada punto de consulta (del 1 al 19) se deberá indicar si el mismo no resulta aplicable al inspeccionado, bastando para ello hacer una cruz en la columna indicada como “NA” (No Aplicable).

En caso de resultar aplicable se deberá marcar con una cruz si el banco de datos cumple o no con dicho punto, marcando con una cruz en la columna “SI” o en la columna “No”, según corresponda.

En el campo “Observaciones” se incluirán todas las aclaraciones que se consideren pertinentes para el mejor cumplimiento de los objetivos de la inspección.

A. IDENTIFICACION DEL RESPONSABLE

1. NOMBRE DEL RESPONSABLE Y ACREDITACION DE PERSONERIA

Se verificará quién es el responsable de las bases de datos. Cuando sean personas jurídicas, se deberá solicitar el poder o acreditación de personería del representante legal.

2. NUMERO DE C.U.I.T./C.U.I.L./C.D.I. DEL RESPONSABLE

Verificar el Número de C.U.I.T./C.U.I.L./C.D.I. del responsable de la empresa.

B. DESARROLLO DE LA INSPECCION

3. NUMERO DE REGISTRO ANTE LA DNPDP

Se deberá colocar el N° de Registro asignado por la DNPDP a la empresa inspeccionada.

Cita Normativa (Ley Nº 25.326):

“ARTICULO 3°.- (Archivo de datos - Licitud) - La formación de archivo de datos será licita cuando se encuentren debidamente inscriptos…”.

“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…”.

4. BANCO DE DATOS INSCRIPTOS ANTE LA DNPDP

Se deberán indicar las bases de datos inscriptas en el Registro Nacional de Bases de Datos de la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES. Las mismas se encuentran especificadas en el Formulario de Inscripción.

5. POLITICAS DE PRIVACIDAD

Se verificará si tiene una política de privacidad acorde a lo dispuesto por la Ley Nº 25.326 y que la misma desarrolle cuanto menos los temas que se exponen a continuación:

Lineamientos básicos para una política de Protección de Datos Personales.

1. Definición del Objeto de la política de Protección de Datos Personales (objeto tutelado, como por ejemplo, los artículos 1° y 2° de la Ley Nº 25.326 y sus principios), alcance corporativo (a quienes resulta exigible la política) y su compatibilidad y/o relación con las políticas de protección de la información comercial o cualquier otra política que entre en conjunción con la protección de datos personales.

2. Definición de términos de la política (acordes con la Ley Nº 25.326).

3. Principios de protección de datos personales de la política aplicables a la empresa (acordes con la Ley Nº 25.326, artículos 3°, 4°, 5°, 6°, 7° y 11).

4. Confidencialidad de los datos personales (artículo 10 de la Ley Nº 25.326), con referencia a los convenios de confidencialidad del personal y terceros que presten servicios, etc. (todo que entre en contacto con los datos personales de la institución).

5. Seguridad de los datos personales, aplicación de la Disposición DNPDP Nº 11/06 (manual de seguridad).

6. Transferencia Internacional de datos personales (aplicando el artículo 12 de la Ley Nº 25.326 y Decreto N° 1558/01).

7. Publicidad directa (artículo 27 de la Ley Nº 25.326 y Decreto N° 1558/01), Disposiciones DNPDP Nros. 10/08 y 4/09.

8. Prestaciones de servicios de tratamiento de datos por cuenta de terceros (artículo 25 de la Ley Nº 25.326 y Decreto N° 1558/01).

9. Derechos de los titulares de los datos (personal, clientes y proveedores), y procedimientos para responder a su ejercicio (derechos de acceso, rectificación, supresión, etc., artículos 14, 15 y 16 de la Ley Nº 25.326).

10. Designación de un Encargado de Protección de Datos por parte del Directorio (a cargo de velar por la correcta y efectiva aplicación de la presente política y su relación con el órgano de control).

11. Implementación y ejecución de la política en la empresa.

12. Capacitación. Areas Sistemas - Jurídicas - Atención Público.

13. Auditoría sobre su cumplimiento. Notificación de incidentes.

14. Determinación de responsabilidades en caso de incumplimiento.

5.a. Designa encargado de la Política de Privacidad.

Se deberá indicar si el responsable del Banco de Datos ha designado un encargado de la Política de Privacidad que tenga a su cargo velar por el adecuado cumplimiento de la misma.

5.b. Difunde y capacita respecto de la Política de Privacidad.

Se verificará si dentro de la organización se difunde la Política de Privacidad y se capacita al personal de la misma para su correcta implementación.

5.c. Incorpora el control de cumplimiento de la política de privacidad en sus procesos de auditoría.

Se deberá verificar si existen mecanismos de control o auditorías internas que evalúen el cumplimiento de lo establecido en las políticas de protección de datos personales.

6. Calidad de los datos (artículo 4° de la Ley Nº 25.326)

6.a. Determina la finalidad del tratamiento de los bancos de datos.

Debe verificarse que los bancos de datos posean una finalidad definida por el Responsable en sus políticas. Se recomienda verificar lo denunciado en el Formulario de Inscripción en el Registro Nacional de Bases de Datos (punto 2 del FA.01).

Cita Normativa (Ley Nº 25.326):

"ARTICULO 3°.- …Los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública."

"ARTICULO 4°.- inciso 3°: Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención."

6.b. Determina la categoría de los datos admisibles en sus bancos de datos

Se deberá verificar si el responsable determina y cumple con la categoría de datos admisible conforme a la finalidad del tratamiento previsto. Al respecto, se recomienda ver lo denunciado en el Formulario de Inscripción en el Registro Nacional de Bases de Datos (punto 3 del FA01: Naturaleza dato. Datos Sensibles, Datos relativos a Antecedentes penales o contravencionales. Especificar los tipos de datos personales que trata).

Cita Normativa (Ley Nº 25.326):

"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 con el ámbito y finalidad para los que se hubieren obtenido."

"ARTICULO 21.- (Registro de archivos de datos. Inscripción). …3) Ningún usuario de datos podrá poseer datos personales de naturaleza distinta a los declarados en el registro."

6.c. Trata datos sensibles (artículos 2° y 7° de la Ley Nº 25.326)

Debe indicarse si el banco de datos trata datos sensibles y en caso afirmativo indicar la norma que autoriza dicho tratamiento y las medidas de seguridad que se aplican a los mismos (Nivel Crítico, salvo que se traten para fines administrativos —ej.: administración de personal— u obligación legal —ej.: examen preocupacional—).

Cita Normativa (Ley Nº 25.326):

"ARTICULO 2°.- (Definiciones). A los fines de la presente ley se entiende por: …— 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."

"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."

6.d. Toma medidas para garantizar la calidad del dato objeto de tratamiento

Verificar la existencia de procesos y medidas de control a fin de mantener la calidad de la información exigible según la finalidad del tratamiento, de manera tal que garanticen que los datos sean ciertos, adecuados, pertinentes, no excesivos, exactos y completos.

Cita Normativa (Ley Nº 25.326):

"ARTICULO 4°.- (Calidad de los datos). 1. Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, en relación con el ámbito y finalidad para los que se hubieren obtenido. …4. Los datos deben ser exactos y actualizarse en los casos de que ello fuera necesario. 5. Los datos total o parcialmente inexactos o incompletos deben ser suprimidos o sustituidos o en su caso completados por el responsable de la base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información."

6.e. Verifica la utilidad de los datos en forma periódica

Se deberá verificar la existencia de mecanismos a fin de mantener la utilidad de los datos almacenados acordes con la finalidad del tratamiento. Cuanto menos, se debería verificar la utilidad del dato una vez al año al momento de renovar la inscripción en el Registro Nacional de Bases de Datos.

Se deberá establecer un procedimiento de destrucción de los datos que han perdido su utilidad, sea en los sistemas como en soporte papel o cualquier otro dispositivo técnico de almacenamiento (cintas de backup, discos, etc.).

Cita Normativa (Ley Nº 25.326)

"ARTICULO 4°.- (Calidad de los datos). …7. Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados."

7. RECOLECCION DE LOS DATOS (artículos 5° y 6° de la Ley N° 25.326)

Se verificará la licitud de la recolección de datos que realiza el responsable, particularmente se verificará en los formularios de recolección el cumplimiento del derecho de información al titular del dato que dispone el artículo 6° de la Ley N° 25.326 y la Disposición DNPDP Nº 10/2008.

Cita Normativa (Ley Nº 25.326)

"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 con 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. Se verificará si se informa al titular del dato en forma expresa y clara, la finalidad para la que serán tratados y quiénes pueden ser sus destinatarios."

7.a. Verifica el origen de los datos (fuentes) y su licitud.

Debe determinarse si el responsable obtiene los datos de fuente lícita (ej.: formularios suscriptos por el mismo titular del dato —personal o clientes—, o fuente de acceso público irrestricto como ser la AFIP —proveedores—).

7.b. Recolecta los datos conforme requisitos de la ley (artículos 5°, 6°, 26 y 27 de la Ley Nº 25.326)

Verificar si pide el consentimiento del titular del dato (en caso de ser exigible) y respeta la finalidad que motivó su recolección inicial (en caso de datos obtenidos por cesión de terceros).

7.c. Cumple en brindar el derecho de información al titular del dato (artículo 6° de la Ley Nº 25.326)

Verificar si los formularios de recolección cumplen con lo dispuesto por el artículo 6° de la Ley Nº 25.326 y la Disposición DNPDP N° 10/2008.

7.d. Recaba el consentimiento del titular del dato (de ser exigible).

En caso de ser exigible, verificar la existencia del consentimiento por escrito, o medio que lo equipare, del titular del dato.

8. CESION DE DATOS (artículo 11 de la Ley N° 25.326)

Se verificará si el responsable realiza cesión de datos personales en los términos del artículo 11 de la Ley Nº 25.326.

Cita Normativa (Ley Nº 25.326)

"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."

8.a. Determina los destinatarios de cesiones actuales o eventuales

Se deberá verificar si el responsable tiene prevista la cesión de datos personales a actuales o eventuales cesionarios indicando los elementos que permitan identificarlos.

8.b. Posee el consentimiento previo del titular del dato (de ser exigible)

En caso de ser exigible, se deberá verificar la existencia del consentimiento expreso previo informado, por escrito o medio que lo equipare, para la cesión prevista.

9. CONFIDENCIALIDAD (artículo 10 de la Ley N° 25.326)

Se deberá verificar si el inspeccionado posee convenios de confidencialidad firmados por los empleados, usuarios o terceros que accedan a la información registrada en la base de datos.

Cita Normativa (Ley Nº 25.326)

"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 aún 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."

10. MEDIDAS DE SEGURIDAD (artículo 9° de la Ley Nº 25.326 y Disposición DNPDP Nº 11/06)

Se verificará la correcta implementación de las medidas de seguridad dispuestas por el artículo 9º de la Ley Nº 25.326 y la Disposición DNPDP Nº 11/2006. Se comprobará la existencia de las medidas de seguridad en los sistemas, la red interna, puestos de acceso y servidores (centro de cómputos). En momento alguno el equipo de inspección ingresará a los sistemas, sino que solicitará al responsable que exhiba la existencia de dichas medidas.

Cita Normativa (Ley Nº 25.326)

"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."

La Disposición DNPDP Nº 11/06 establece TRES (3) niveles de seguridad: BASICO, MEDIO y CRITICO. Para cada uno de los niveles mencionados se han previsto distintas medidas de seguridad que el responsable debe aplicar a sus bancos de datos según el nivel en que califiquen.

10.a. NIVEL BASICO

10.a.1. Posee documento de seguridad.

Se verificará si posee documento de seguridad, que puede consistir en un manual integral o un conjunto de normas que cumpla con los requisitos de la Disposición DNPDP Nº 11/06 (Ver modelo de manual en la Disposición DNPDP Nº 9/08).

10.a.2. Asigna funciones y obligaciones del personal respecto al tratamiento de datos personales.

Verificar si se ha diseñado y otorgado funciones, niveles de acceso y procedimientos del personal respecto del tratamiento de los datos, lo que incluye la firma de compromisos de confidencialidad (artículo 10 de la Ley Nº 25.326).

10.a.3. Documenta sus bancos de datos y los sistemas de información que los almacenan.

Controlar que se encuentren documentadas las distintas bases de datos de titularidad del responsable, y los sistemas de información que utiliza para su tratamiento (ej.: base de datos del personal, clientes, proveedores, agenda).

10.a.4. Establece medidas de control de calidad de la información a incorporar al Banco de Datos.

Debe preverse la instrucción del personal y/o diseñarse sistemas o procedimientos de control para garantizar que la información a incorporar sea correcta y congruente (ej.: datos numéricos en campos numéricos, no números en campos destinados a nombres, etc.).

10.a.5. Registra y prevé medidas ante incidentes de seguridad.

Debe verificarse la existencia de un registro de incidentes de seguridad y las medidas adoptadas para su solución y evitar reincidencias.

10.a.6. Realiza copias de resguardo de la información periódicas.

Debe preverse la realización de copias de resguardo de la información ("backups") en forma periódica y depositarse en lugar seguro.

10.a.7. Mantiene un control actualizado de los usuarios del sistema autorizados mediante claves.

Debe existir una política de actualización de los usuarios.

10.a.8. Gestiona adecuadamente las claves y las renueva periódicamente.

Debe existir una política de contraseñas por medio de la cual se obligue a los usuarios a renovar sus claves y registrar las mismas en lugar seguro.

10.a.9. Prevé medidas para proteger la información de equipos desatendidos.

Cuando el usuario desatienda el equipo durante un tiempo prudencial se debe requerir el reingreso de clave.

10.a.10. Establece protección permanente y actualizada contra accesos no autorizados, virus y software malicioso.

Debe preverse la actualización de dichas medidas de protección.

10.a.11. Prevé medidas técnicas para el correcto funcionamiento de los equipos (instalación, temperatura ambiente) o evitar su daño por elementos externos como el fuego, etc.

En caso de nivel medio, debe verificarse la existencia de las siguientes medidas sobre el centro de cómputos: Area Segura: Evitar acceso físico no autorizado. Perímetro de Seguridad: Paredes y Puerta de Acceso controladas. Protección Física: Area ignífuga, matafuegos, inundaciones, explosiones. Protección de Energía: Falla eléctrica, ups o generadores que mantengan el suministro eléctrico para proteger las bases de datos, temperatura ambiente.

10.a.12. Posee política de gestión de soportes de datos personales, sean en papel o cualquier otro dispositivo técnico (inventario; almacenamiento; procedimientos en caso de extracción, salidas o destrucción por desuso).

Debe preverse un registro y procedimiento respecto de los soportes de resguardo de la información (ej.: CDs), identificándolos y depositándolos en lugar seguro. Verificar, asimismo, la existencia de un procedimiento de destrucción seguro de dichos soportes previo a su descarte.

10.b. NIVEL MEDIO

Permita establecer el perfil de personalidad o conductas determinadas de las persona o resulte afectada por secreto legal específico o empresas privadas de servicios públicos.

10.b.1. Designa responsable de Seguridad.

Deberá existir un responsable de la Seguridad de Información.

10.b.2. Incorpora el control de medidas de seguridad de datos personales en sus procesos de auditoría.

Se deberá incorporar en los procedimientos de las auditorías el control de las medidas de seguridad para la protección de los datos personales.

10.b.3. Impide la reiteración de intento de acceso no autorizado al sistema de Información.

Debe preverse que ante la reiteración de intentos fallidos de acceso se bloquee al usuario.

10.b.4. Prevé medidas físicas para evitar el acceso indebido a la zona del centro de cómputos y depósito de soportes de almacenamiento de información.

Debe verificarse la existencia de medidas de seguridad para controlar y registrar el acceso a dichos ámbitos.

10.b.5. Posee procedimiento de recuperación de la información de respaldo y tratamiento de la misma en caso de contingencia que ponga no operativo el o los equipos de procesamiento habituales.

Deben preverse mecanismos de recuperación de la información de respaldo ("backups") en los casos de caídas del sistema y un plan de contingencia.

10.b.6. Toma medidas de protección de los datos personales cuando son transmitidos por redes internas o externas a la empresa.

Debe verificarse la existencia de medidas de seguridad adecuadas para la protección de la información al momento de ser transmitida por redes internas y/o externas.

10.b.7. En caso de incidentes de seguridad de la información, autoriza e identifica la persona que recuperó y/o modificó dicho datos.

Debe preverse la registración de las personas que realicen tareas de recuperación de la información, identificando las tareas desarrolladas por las mismas.

10.b.8. Las pruebas de funcionamiento de los sistemas de información se realizan en paralelo al sistema real.

En los casos que se realicen pruebas de funcionamiento de los sistemas de información y/o modificación de los existentes, debe realizarse en paralelo y protegiendo la confidencialidad de la información.

10.c. NIVEL CRITICO

Contenga "datos sensibles" cuyo tratamiento no sea obligatorio o para fines meramente administrativos (ej.: Administración del personal).

10.c.1. Distribución de Soportes: Encripta los datos cuando se trasladen en soportes o se realicen copias de resguardo de la información.

10.c.2. Lleva registro de acceso al sistema de los operadores y administrador (log, usuario, fecha, hora, autorizado, denegado, tipo de operación realizada).

10.c.3. Deposita copias de seguridad del sistema fuera de la localización habitual, en caja ignífuga y a prueba de gases o bien en una caja de seguridad bancaria, situadas a una distancia prudencial.

10.c.4. Encripta los datos de carácter personal que se trasmiten a través de redes de comunicación.

11. ACTIVIDADES DE PUBLICIDAD DIRECTA (artículo 27 de la Ley Nº 25.326)

Cita Normativa (Ley Nº 25.326):

"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."

"Decreto N° 1558/2001: 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. …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."

11.a. Utiliza sólo las categorías autorizadas (inciso 1. Artículo 27 de la Ley Nº 25.326 y Decreto)

Se deberá verificar que sólo utilizan datos aptos para establecer perfiles publicitarios y realizar la oferta prevista.

11.b. Recaba los datos de fuentes legítimas (inciso 1. Artículo 27 de la Ley Nº 25.326 y Decreto)

Verificar el origen y/o forma de recolección de los datos destinados a publicidad directa, particularmente que se hayan recolectado para dicha finalidad, brindando la adecuada información al titular del dato a dicho momento.

11.c. Respeta derecho de acceso del titular del dato (inciso 2. Artículo 27 de la Ley Nº 25.326 y Decreto).

Verificar que prevean y otorguen derecho de acceso al titular del dato sin cargo alguno, cumpliendo al momento de su recolección con la Disposición DNPDP Nº 10/2008.

11.d. Respeta derecho de retiro o bloqueo del titular del dato (inciso 3. Artículo 27 de la Ley Nº 25.326 y Decreto)

Verificar si prevé mecanismos eficaces para el ejercicio del derecho de retiro o bloqueo del titular del dato, y si cumple al momento del envío del mensaje de publicidad con las Disposiciones DNPDP Nros. 10/08 y 4/09.

Disposición DNPDP Nº 10/08

— "El titular de los datos personales tiene la facultad de ejercer el derecho de acceso a los mismos en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto conforme lo establecido en el artículo 14, inciso 3 .de la Ley Nº 25.326."

— "La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, Organo de Control de la Ley Nº 25.326, tiene la atribución de atender las denuncias y reclamos que se interpongan con relación al incumplimiento de las normas sobre protección de datos personales."

Disposición DNPDP Nº 4/09

— "Un aviso que informe al titular del dato sobre los derechos de retiro o bloqueo total o parcial, de su nombre de la base de datos, el mecanismo que se ha previsto para su ejercicio, con más la transcripción del artículo 27, inciso 3, de la Ley Nº 25.326 y el párrafo tercero del artículo 27 del Anexo I del Decreto Nº 1558/01."

— "Establécese que cuando se efectúen envíos de comunicaciones de publicidad directa no requeridas o consentidas previamente por el titular del dato personal, deberá advertirse en forma destacada que se trata de una publicidad. En caso de realizarse dicha comunicación a través de un correo electrónico deberá insertarse en su encabezado el término único 'publicidad'."

12. TRANSFERENCIA INTERNACIONAL (artículo 12 de la Ley N° 25.326)

Deberá verificarse si el inspeccionado realiza transferencias de datos a terceros países. Si los países destinatarios poseen legislación adecuada bastará con indicar en SI y aclarar dicha circunstancia en el campo Observaciones. En caso que el país destinatario no tenga legislación adecuada será exigible un contrato de transferencia internacional o el consentimiento del titular del dato, lo que se consulta en los puntos siguientes.

Cita Normativa (Ley Nº 25.326)

"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."

12.a. La realiza mediante contrato de transferencia Internacional

En caso que alguno de los países destinatarios de la transferencia internacional no posea legislación adecuada, debe verificarse si la misma se realiza mediante contrato de transferencia internacional que traspole adecuadamente la Ley Nº 25.326 y obligue a su cumplimiento a todas las partes intervinientes. En caso que dicho contrato se encuentre aprobado por la DNPDP, debe consignarse dicha circunstancia.

12.b. La realiza mediante consentimiento del titular del dato

En caso que alguno de los países destinatarios de la transferencia internacional no posea legislación adecuada, debe verificarse si la misma se realiza con el previo consentimiento del titular del dato.

13. TRATAMIENTO DE DATOS POR CUENTA DE TERCEROS (artículo 25 de la Ley Nº 25.326)

Verificar si el responsable del banco de datos contrata el servicio de tratamiento de sus datos con terceras personas, sea para almacenamiento o procesamiento, total o parcial.

Cita Normativa (Ley Nº 25.326).

"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."

13.a. Posee contrato de servicios de tratamiento por parte de terceros

En caso de contratar el tratamiento de sus datos por terceros, se verificará si posee un contrato que contenga los requisitos del artículo 25 de la Ley Nº 25.326 y el Decreto Nº 1558/2001: a) Cláusulas que dispongan el tratamiento bajo exclusivas instrucciones impartidas por el responsable; b) Medidas de seguridad y confidencialidad acordes con los artículos 9° y 10 de la Ley Nº 25.326 y Disposición DNPDP Nº 11/06; c) Finalidad exclusiva del tratamiento a las previstas contractualmente; d) Prohibición de cesión a terceros no prevista contractualmente, ni aun para su conservación; e) Destrucción de los datos una vez finalizado el contrato, salvo autorización para conservarlos hasta DOS (2) años después de finalizado en caso de preverse nuevas contrataciones. Se verifica a continuación el cumplimiento de dichos requisitos.

13.b. Determina la finalidad de tratamiento

Verificar que se determine contractualmente la finalidad del tratamiento de datos personales.

13.c. Determina medidas de seguridad y confidencialidad

Verificar que existan cláusulas de seguridad y confidencialidad acordes con la normativa aplicable.

13.d. Determina el plazo de conservación de los datos

Verificar que el contrato tenga previsto la destrucción y/o devolución de los datos en poder del prestador del servicio una vez finalizado el mismo.

14. DERECHOS DEL TITULAR DEL DATO (artículos 14, 15 y 16 de la Ley Nº 25.326)

14.a. Establece procedimientos y plazos de ley para el derecho de acceso

Se debe verificar la existencia de un procedimiento que contenga los siguientes puntos: 1. Designación de personal a cargo capacitado para recepcionar el pedido del titular del dato. 2. Verificación de la identidad del titular del dato solicitante (D.N.I.). 3. Registro de la solicitud. 4. Procedimiento para la elaboración de la respuesta. 5. Registro de la respuesta y su entrega al solicitante. 6. Plazo previsto para cumplir con el pedido.

Cita Normativa (Ley Nº 25.326).

"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."

14.b. Establece procedimientos y plazos de ley para el derecho de rectificación

A los fines de verificar el cumplimiento por parte del responsable de los derechos de rectificación, supresión y/o confidencialidad del titular del dato, se debe verificar la existencia de un procedimiento que contenga los siguientes puntos: 1. Designación de personal a cargo capacitado para recepcionar el pedido del titular del dato. 2. Verificación de la identidad del titular del dato solicitante (D.N.I.). 3. Registro de la solicitud. 4. Procedimiento para la elaboración de la respuesta. 5. Registro de la respuesta y su entrega al solicitante. 6. Plazo previsto para cumplir con el pedido.

Cita Normativa (Ley Nº 25.326).

"ARTICULO 16.- (Derecho de rectificación, actualización o supresión). 1. Toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos. 2. El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad. 3. El incumplimiento de esta obligación dentro del término acordado en el inciso precedente, habilitará al interesado a promover sin más la acción de protección de los datos personales o de hábeas data prevista en la presente ley. 4. En el supuesto de cesión, o transferencia de datos, el responsable o usuario del banco de datos debe notificar la rectificación o supresión al cesionario dentro del quinto día hábil de efectuado el tratamiento del dato. 5. La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos. 6. Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá o bien bloquear el archivo, o consignar al proveer información relativa al mismo la circunstancia de que se encuentra sometida a revisión. 7. Los datos personales deben ser conservados durante los plazos previstos en las disposiciones aplicables o en su caso, en las contractuales entre el responsable o usuario del banco de datos y el titular de los datos."

15. CAPACITACION

Debe verificarse el compromiso del responsable para con la capacitación de las distintas áreas que participan en el tratamiento de datos personales, como ser los estudios, cursos de actualización, divulgación interna, confección de manuales e instructivos, capacitación del personal, etc.

Actividades desarrolladas	General Empresa	Sistemas	Atención Público	RRHH
Estudios vinculados a la protección de datos personales				
Cursos de actualización				
Divulgación Interna				
Confección de manuales e instructivos				
Capacitación del personal				

16. ACATAMIENTO DE LAS DISPOSICIONES DE LA DNPDP

Se verificará el cumplimiento por parte del responsable de las distintas disposiciones de la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES.

16.a. Constata correcto acatamiento Disposiciones de la DNPDP

Se indicará el correcto acatamiento del responsable de las Disposiciones que con carácter general ha dispuesto la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES y que sean aplicables a la actividad del inspeccionado.

16.b. Verifica acatamiento de disposiciones particulares acaecidas en sumarios tramitados ante la DNPDP en los que el responsable de la base de datos haya sido parte.

Se verificará el acatamiento del responsable de las disposiciones particulares que con motivo de algún sumario, inspección o cualquier otro trámite administrativo, le haya formulado la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES.

C. CASOS ESPECIALES

17. ESTABLECIMIENTOS SANITARIOS Y MEDICOS (artículos 7° y 8° de la Ley Nº 25.326)

Toma medidas que garanticen el secreto profesional

Se verificará que el responsable tome medidas que garanticen el secreto profesional, firmando los convenios de confidencialidad necesarios, en particular con el personal administrativo y auxiliar que tome conocimiento de datos afectados por dicho secreto, y prohibiendo el acceso a personas no autorizadas por la normativa específica.

Cita Normativa (Ley Nº 25.326):

"ARTICULO 8°.- (Datos relativos a la salud). Los establecimientos sanitarios públicos o privados y los profesionales vinculados a la ciencia de la salud puede recolectar y tratar los datos personales relativos a la salud física y mental de los pacientes respetando los principios del secreto profesional.

Secreto Profesional: arts. 11 y 19, inc. 3º, Ley Nº 17.132, y Código de Etica de la Confederación Médica Argentina de 1955)."

18. INVESTIGACIONES CLINICAS, FARMACOLOGICAS Y FARMACOGENETICAS (artículos 7° y 8° de la Ley Nº 25.326)

Utiliza modelos de consentimiento informado aprobado por la DNPDP

Se verificará si el responsable ha realizado el trámite de homologación del consentimiento informado ante la DNPDP.

19. EMPRESAS DE INFORMES CREDITICIOS (artículo 26 de la Ley Nº 25.326)

19.a. Utiliza sólo las categorías autorizadas (incisos 1. y 2. artículo 26 de la Ley Nº 25.326)

Para los casos de responsables que realizan tratamientos de datos para la finalidad de brindar informes crediticios a terceros, debe verificarse que sólo traten datos de la categoría admitida por el artículo 26 de la Ley Nº 25.326, incisos 1. y 2.: Datos de carácter patrimonial relativos a la solvencia y el crédito y al cumplimiento de obligaciones patrimoniales.

Cita Normativa (Ley Nº 25.326):

"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."

19.b. Recaba los datos de fuentes legítimas (incisos 1. y 2. artículo 26 de la Ley Nº 25.326)

Debe verificarse que los datos se recolecten de fuentes autorizadas por la ley (incisos 1. y 2. de la Ley Nº 25.326), esto es, de fuentes de acceso público o facilitados por el acreedor.

Cita Normativa (Ley Nº 25.326):

"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."

19.c. Respeta derecho de acceso del titular del dato (inciso 3. artículo 26 de la Ley Nº 25.326)

Verificar si se respeta el derecho de acceso a la información del titular del dato, indicándole de los últimos SEIS (6) meses la información transmitida y sus destinatarios (nombre y domicilio), en forma gratuita.

Cita Normativa (Ley Nº 25.326):

"ARTICULO 26.- (Prestación de servicios de información crediticia) …3. A solicitud del titular de los datos, el responsable o usuario del banco de datos, le comunicará las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y domicilio del cesionario en el supuesto de tratarse de datos obtenidos por cesión."

19.d. Aplica los plazos de caducidad del dato (inciso 4. artículo 26 de la Ley Nº 25.326)

Verificar la aplicación a sus informes de los plazos de caducidad del dato crediticio, aplicando el derecho al olvido en los términos del artículo 26, inciso 4., de la Ley Nº 25.326.

Cita Normativa (Ley Nº 25.326):

"ARTICULO 26.- (Prestación de servicios de información crediticia) …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 hacer constar dicho hecho."

19.e. Controla existencia de interés legítimo del cesionario (inciso 5)

Debe controlarse si al momento de ceder informes a terceros, el responsable instrumenta las medidas necesarias para verificar la existencia del interés legitimo del cesionario.

Cita Normativa (Ley Nº 25.326):

"ARTICULO 26.- (Prestación de servicios de información crediticia) …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."