C.P.C.E.C.A.B.A.

Ejercicio práctico de revisión del cumplimiento de la Ley 25.326 de Protección de Datos Personales

Dra. Graciela Braga

Dra. Silvia Iglesias

Introducción a Ley 25.326 Jerarquía Legal

Introducción a Ley 25.326
Titulares y Definición de Datos Alcanzados

Titulares Datos

Contenidos y Almacenados

Introducción a Ley 25.326
Tipos de Datos

Básicos	• Nombre y apellido, documento de identidad, identificación tributaria o previsional, ocupación, domicilio y fecha de nacimiento
Intermedios	• Son los que superan a los básicos y no son sensibles. • Ejemplo TE, remuneración, estado civil, patrimonio
Sensibles	• Los que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a las salud o a la vida sexual

Introducción a Ley 25326
La Base es Legal si:

- **Están inscriptas y renovadas Art.3, 21, 22, 23, 24**
- **Si se le provee seguridad Art.9**
- **Si se informa el titular el tratamiento y destino de los datos y no se los usa para otros fines Art. 6**
- **Si se solicito el consentimiento para el tratamiento Art. 5**
- **Si se informo si serán cedidos o transferidos Art. 6**
- **Si se da Acceso a todos sus datos almacenados en las entidades a los titulares Art. 14**
- **Si se les permite la rectificación y actualización de sus datos Art.16**
- **Si se les permite la supresión de sus datos en la bases de las entidades Art.16**

El Rol del Profesional en Cs. Económicas Obligaciones de los Responsables

Calidad de los Datos Art. 4

- Confidencialidad
- Disponibilidad
- Integridad
- Trazabilidad

El Rol del Profesional en Cs. Económicas Disposición 11/06 DNPDP

Todos los niveles

datos en papel y/o informatizados

- Organigrama
- Manual de Funciones y Responsabilidades
- Registros documentados de todos los procesos y procedimientos de: Tratamiento de los D. P. - Eventos de Seguridad y su Solución - Control de Accesos - Validación de los D. P.- Alta, Baja, Modificacón y Consulta de los D.P.- Soportes de información - Copias de respaldo y su recupero -Forma de trabajo en las pruebas de Software - Control de malware (software malicioso)

El rol del Profesional en Cs. Económicas Disposición 11/06 DNPDP

Nivel Intermedio y Sensible datos en papel y/o informatizados

- Responsable de Seguridad de los Datos Personales
- Auditorías de Cumplimientos de la Seguridad (interna o externa)
- Registros más detallados en los procedimientos, límites en los accesos, mayor tiempo de guarda e identificaicon de personas y soportes, en el uso de soportes, en las copias de seguridad
- Procesos y procedimientos de seguridad en las comunicaciones (transporte seguro)

Qué y cómo inspecciona la DNDP

La inspección consiste en:

Un formulario con el detalle de documentos y controles para preparar la auditoría enviado 10 días antes

Entrevistas al personal responsable y usuarios de datos personales

Revisión de contratos y consentimientos informados
Revisión de los procesos de tratamiento de datos informatizados y manuales, incluida la comercialización

Revisión de la seguridad de datos según Disp. 11/06 DNPDP

Revisión de los Procesos que garanticen el Acceso, Modificación y Supresión de Datos Personales por los Titulares de datos

Qué y cómo inspecciona la DNDP

Evalúan:

Capacitación de los Responsables de Bases

Legalidad y corrección de los datos objeto de tratamiento(Licitud de los datos, Registro en la DNPDP, Medidas de Seguridad, Política de Privacidad)

Idoneidad de los medios empleados en el tratamiento de los datos y en gestiones anexas (Materiales, Sistemas y Software. Personal, Procedimientos de derecho de acceso, atención de reclamos, corrección de errores, comunicación)

Acatamiento de las disposiciones de la DNPDP

Las Sanciones Judiciales y Administrativas
Acciones Judiciales

De Habeas Data	• Por vulnerarse el derecho de acceso
De Derechos Personales	• Por derechos personales en el fuero civil • Por derechos del consumidor

Las Sanciones Judiciales y Administrativas

Leves: Incumplimiento	• **Hasta 2 Apercibimientos** • **y/o multa de: $ 1.000 a 3.000**
Graves: Incumplimiento persistente	• **Hasta 4 Apercibimientos** • **Suspensión de 1 a 30 días** • **y/o multa de: $ 3.001 a 50.000**
Muy Graves: Reiterados incumplimietos y obstaculizar	• **Hasta 6 Apercibimientos** • **Suspensión de 31 a 365 días** • **Clausura o Cancelación del banco de datos** • **y/o multa de: $ 50.001 a 100.000**

INTRODUCCIÓN AL PROCESO DE REVISIÓN DEL CUMPLIMIENTO NORMATIVO

CUALES SON LOS BENEFICIOS DE LA REVISIÓN PARA NUESTROS CLIENTES

Demuestra (o no) razonable cumplimiento de leyes y disposiciones

Mejora el cumplimiento de normas internas

Incrementa concientización y capacitación del personal

Provee información para planificar las inspecciones de la DNPDP

Mejora la satisfacción de los titulares de los datos reduciendo errores que originen quejas

FTE: GTAG4-IIA

PROCESO DE REVISIÓN DEL CUMPLIMIENTO NORMATIVO

Objetivo es similar al planteado por la DNPDP en su proceso 'Inspección y Control' :

Evaluar el grado de cumplimiento de lo prescripto por la Ley 25.326.

Realizar recomendaciones para el mejor desempeño del responsable dentro del marco legal.

→ Base adecuada para ejecutar el proceso de revisión.

PLANEAMIENTO: *Obtener documentación*

Misión, objetivos y procesos de negocios

Tipo de datos recolectados y usados en cada proceso de negocio (propios y tercerizados)

Legislación/disposiciones aplicables a 'esta' organización, que puede incluir los requerimientos de privacidad.

Estructura organizacional, incluyendo roles y responsabilidades del personal que interviene en el tratamiento de los datos personales, acuerdos de confidencialidad. Capacitación.

Formularios de inscripción y renovación

Manual de seguridad

Política de privacidad de la entidad

En caso de corresponder, formulario de auditoría/revisiones anteriores (de privacidad o seguridad de la información)

Tercerizados: contratos, formularios de inscrip./renovación

PLANEAMIENTO: *Analizar documentación para obtener conocimiento*

Evaluación de riesgo realizada por la organización (tanto sobre privacidad como sobre seguridad de los sistemas y seguridad física)

Gestión de la privacidad, controles administrativos y técnicos implementados para cumplimiento normativo

Responsabilidades por el uso de la información por parte del personal/terceros

Aseguramiento de Confidencialidad, integridad, disponibilidad y trazabilidad de los datos (propia y de terceros)

Cumplimiento de los derechos de los titulares de los datos

PLANEAMIENTO: *Realizar Análisis de impacto de no cumplimiento normativo para definir alcance y procedimientos de auditoría*

Indicadores:

Inexistencia de base legal/ consentimiento para la recolección de los datos

Falta de revisión de la adecuación y la exactitud de los datos

Falta de una clara definición del propósito de la recolección de datos

Utilización de los Datos personales para otros propósitos que los inicialmente previstos

Inadecuada/Inexistente protección de los datos personales contra modificación, pérdida o exposición

Falta de transparencia en las políticas, prácticas o modos de procesamiento de los datos personales

Imposibilidad práctica de acceso a los datos por parte de sus titulares

FTE: GTAG4-IIA

EJECUCIÓN

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.		

EJECUCION

La normativa de la DNPDP es insuficiente, deben utilizarse buenas practicas internacionales de Seguridad de la Información y armar los papeles de trabajo en base a la normativa legal y estas buenas practicas. No alcanza como papel de trabajo la planilla de inspecciones

INFORME DE AUDITORIA

Medidas de seguridad Nivel Medio/Critico

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.

REPORTE: ELABORACION DE LA CONCLUSION

INICIAL	Actividades ad hoc, con: • Inexistencia de políticas, reglas o procedimientos • Actividades de bajo nivel eventuales, no coordinadas • Redundancias y falta de equipo de trabajos y compromiso
REPETIBLE	Política de privacidad definida con: • Algún compromiso de la Dirección • Concientización y compromiso general • Planes específicos en áreas de riesgo alto
DEFINIDO	Política y organización de la privacidad implementada, con: • Evaluación de riesgo realizada • Prioridades establecidas y recursos asignados en consecuencia • Actividades para coordinar e implementar controles efectivos
ADMINISTRADO	Gestión de privacidad efectiva y consistente, con: • Temprana consideración de privacidad en desarrollo de sistemas y procesos • Privacidad integrada en las funciones y en los objetivos de desempeño • Monitoreo a nivel organizacional y funcional • Revisión periódica basada en riesgos
OPTIMIZADO	Mejoramiento continuo de políticas, prácticas y controles de privacidad con: • Análisis del impacto sobre la privacidad que ocasionaría los cambios • Recursos exclusivamente dedicados al logro de los objetivos de privacidad • Alto nivel de integración funcional y trabajo en equipo para alcanzar los objetivos de privacidad

RESOLUCIÓN DEL EJERCICIO
PUESTA EN COMUN
CONCLUSIONES