UNIVERSIDAD NACIONAL DE SALTA

Facultad de Ciencias Económicas, Jurídicas y Sociales

Cátedra: **SISTEMAS DE INFORMACION PARA LA GESTION – GESTION DE TI**

Unidad 6. Impacto ético, social y legal en la gestión de las tecnologías de información

Contenidos:
Impacto ético, social y legal de las tecnologías de información: problemas éticos y sociales relacionados con las tecnologías de información. Políticas de Información y aseguramiento de la calidad de datos. Impactos legales en los Sistemas de Información. **Impacto ético, social y legal en la gestión de la infraestructura.** Políticas de TI. Normativas actuales y mejores prácticas en la utilización de tecnologías de internet.

Objetivos específicos:

- Entender que aspectos éticos, sociales y políticos generan los SI
- Conocer conceptos básicos de responsabilidad legal

Bibliografía Básica:

- Sistemas de información gerencial / Laudon, Kenneth C. (2012) Sistemas de información gerencial [texto impreso] / Laudon, Kenneth C.; Laudon, Jane P.. - 12a. ed.. - México : Pearson Educación, 2012. SBN 978-607-32-0949-6. Nota de contenido : Cap 4. Aspectos éticos y sociales en los sistemas de información)

- Normas del contexto legal en Argentina aplicables para cada tema especifico en los sistemas de Información

Índice de Contenido

1. El sistema de protección de datos personales

Introducción

La protección de datos personales también conocido como habeas data (habeas traducido del latín significa “guarda”; data traducido del inglés significa “dato” o “información”) jurídicamente es una figura prevista en el articulo 43 de la constitución nacional que ha cobrado mayor relevancia como consecuencia del avance de la tecnología informática.
Desde un enfoque organizativo el sistema de protección de datos personales es un conjunto de normas, políticas, técnicas, procedimientos, etc. destinadas a asegurar un contexto de seguridad, privacidad e integridad.

Objetivos

- Asegurar un nivel adecuado al cumplimiento de las normas
- Ofrecer apoyo y asistencia a los interesados en el ejercicio de sus derechos
- Ofrecer vías adecuadas de recurso a quienes resulten perjudicados en el caso de que no se observen las normas

Definición

La protección integral de los datos personales garantiza el honor y la privacidad de la personas, como también el acceso a la información que sobre las mismas se registre.

Escenario Jurídico

El marco normativo vigente en nuestro país sobre protección de datos personales se compone de la siguiente forma:

CONSTITUCION NACIONAL

En su artículo 43 tenemos: *“toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística”*

LEY Nº 25.326

El 30 de Octubre de 2000 se promulga la ley 25326 de Protección de los datos personales por la cual se otorga al ciudadano común una facultad de control sobres sus datos personales mediante una serie de principios y derechos. Se establecen obligaciones de los responsables de archivos. Se detallan sanciones; controles y en especial la acción de protección de los datos personales.

DECRETO 1558/2001

Este decreto reglamenta la ley 25326.

RESOLUCIONES AAIP (DNPDP)

Comprende las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por la ley 25326. Son emitidas por la Agencia de Acceso a la Información Publica (Dirección Nacional de Datos Personales (DNPDP)) según el inciso b) del artículo 29 de la mencionada ley.

2. Glosario

A continuación, se transcribe el artículo 2 de la ley 25326 que establece a modo de glosario una serie de definiciones:

***"Datos personales**: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.*

***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.*

***Archivo, registro, base o banco de datos**: Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.*

***Tratamiento de datos**: Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.*

***Responsable de archivo, registro, base o banco de datos**: Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.*

***Datos informatizados**: Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.*

***Titular de los datos**: Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.*

***Usuario de datos**: Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.*

Disociación de datos*: Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable."*

3. Dirección Nacional de Protección de Datos Personales

La Agencia de Acceso a la Información Publica (Ex Dirección Nacional de Protección de Datos Personales) es el órgano descentralizado del Ministerio de Justicia y Derechos Humanos de la Nación para el control de la Ley de Protección de Datos Personales y el Registro Nacional "No llame".
Ejerce las funciones encomendadas por la ley y su decreto reglamentario con plena independencia.

Registro Nacional de Base de Datos

Registro obligatorio de bases de datos públicas o privadas dispuesto en el inciso 1, articulo 21 de la Ley Nº 25.326. Creado por la Dirección Nacional de Protección de Datos Personales.

La obligación de registrarse alcanza a personas físicas o de existencia ideal privadas y públicas que sean titulares de bases de datos personales o realicen tratamiento de información personal

Base de datos sujetas a inscripción

Las bases de datos que deben inscribirse son las que excedan el uso exclusivamente personal y se destinen a dar informes.

4. Principios Generales

El capítulo 2 de la ley de protección de datos establece una serie de principios generales que deben considerar tantos los responsables como usuarios de datos personales al momento de realizar tratamientos manuales y/o informáticos de los mismos.

LICITUD BASE DE DATOS

El principio de la Licitud de las bases de datos se establece en el artículo 3: *"La formación de archivos de datos será lícita cuando se encuentren debidamente inscriptos, observando en su operación los principios que establece la presente ley y las reglamentaciones que se dicten en su consecuencia. Los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública."*

CALIDAD DE LOS DATOS

El principio de la Calidad de los datos se establece en el artículo 4:

"1. Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.

2. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley.

3. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.

4. Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario.

5. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la presente ley.

6. Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.

7. Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados."

CONSENTIMIENTO

El principio del Consentimiento se establece en el artículo 5:

"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 a 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."

INFORMACIÓN

El principio de Información se establece en el artículo 6:

"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."

CATEGORÍA DE DATOS

El principio de Categoría de datos se establece en el artículo 7:

"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."

DATOS RELATIVOS A LA SALUD

El principio Datos relativos a la salud se establece en el artículo 8:

"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."

DEBER DE CONFIDENCIALIDAD

El principio Deber de confidencialidad se establece en el artículo 10:

"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 aun 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."

CESIÓN

El principio de Cesión se establece en el artículo 11:

"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."

TRANSFERENCIA INTERNACIONAL

El principio de Transferencia internacional se establece en el artículo 12:

"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.

2. La prohibición no regirá en los siguientes supuestos:

a) Colaboración judicial internacional;

b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto se realice en los términos del inciso e) del artículo anterior;

c) Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable;

d) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte;

e) Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico."

5. Seguridad de los datos

El principio de Seguridad de los datos merece un apartado propio porque se trata de un aspecto relevante y crítico para el logro de ese contexto de seguridad, privacidad e integridad.

El artículo 9 establece:

"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."

Estas medidas técnicas y organizativas fueron normadas por la Dirección Nacional de Protección de datos personales a través de la resolución 47/2018 que aprueba las "Medidas de seguridad recomendadas para el tratamiento y conservación de los datos personales en medios informatizados y no informatizados".

Medidas de seguridad recomendadas para el tratamiento y conservación de los datos personales en medios informatizados

En Anexo I se establece:

De modo referencial y con el objetivo de facilitar el cumplimiento de la Ley N° 25.326 de Protección de los Datos Personales, se establecen las medidas de seguridad recomendadas para la administración, planificación, control y mejora continua de la seguridad de la información.

Los procesos señalados reúnen el conjunto de tareas y especialidades que las entidades pueden poseer, con estas u otras denominaciones y en la composición orgánica que mejor satisfaga sus intereses y funcionamiento.

A - Recolección de datos

Relacionado con los procesos necesarios para asegurar la completitud e integridad de los datos, minimizar los errores e implementar las medidas técnicas con el objeto de asegurar la confidencialidad y limitar el acceso durante la recolección.

A - Recolección de datos	Descripción
A.1. INTEGRIDAD	
A.1.1. ASEGURAR COMPLETITUD	Verificar que campos que componen formulario de recolección de datos permitan ingreso completo de dato requerido
A.1.2. MINIMIZAR ERRORES DE INGRESO	Indicar en forma clara y concreta el tipo de información a ingresar y su formato
A.1.3. ASEGURAR INTEGRIDAD	Verificar exactitud dato ingresado en caso de que el tipo de registro lo permita
A.2. CONFIDENCIALIDAD	

A - Recolección de datos	Descripción
A.2.1. ASEGURAR CONFIDENCIALIDAD DURANTE RECOLECCION	Cifrar comunicación cliente-servidor durante recolección
A.2.2. LIMITAR ACCESO A RECOLECCION DATOS	Limitar cache del formulario en el cliente. Limitar carga de dato en el cliente a una sola sesión de usuario
A.2.3. LIMITAR ACCESO NO AUTORIZADO DURANTE RECOPILACION	Utilizar certificados digitales seguros y validados por entidades autorizadas(CA). Cifrar comunicación durante traslado desde el servidor de aplicación hacia la base de datos

B - Control de acceso

Relacionado con la implementación de medidas de seguridad, mecanismos de autenticación, segregación de roles y funciones, y demás características del acceso a los sistemas para la protección de la identidad y la privacidad.

B - Control de acceso	Descripción
B.1. IDENTIFICACION DE ACTIVOS	
B.1.1. IDENTIFICAR ACTIVOS	Elaborar inventario de activos informáticos que almacenen o gestionen datos personales
B.1.2. DEFINIR RESPONSABLES Y RESPONSABILIDADES	Definir propietarios de activos informáticos que almacenen o gestionen datos personales. Notificar a los propietarios. Especificar a los propietarios autorizaciones de acceso (tipo de acceso y validez)
B.1.3. VERIFICAR APLICACIÓN DE CONTROLES	Elaborar procedimientos de 1) actualización periódica del inventario: 2) verificación de autorizaciones: 3) para nuevos activos informáticos, definiendo responsable asignado y autorizaciones.
B.2. ACCESO A LOS DATOS	
B.2.1. GESTIONAR ACCESOS A SISTEMAS	Elaborar documento interno que defina controles de acceso a cada sistema. Definir e identificar aquellos superusuarios (administradores) puedan evadir controles de acceso definidos para el propietario. Controlar y monitorear a superusuarios (registrar acceso y actividad)
B.2.2. ASIGNAR PERMISOS	Disponer de notificación concreta y formal de responsabilidades asumidas por cada usuario que acceda internamente a los sistemas (notificación fehaciente)
B.2.3. VERIFICAR IDENTIFICACION Y AUTORIZACION	Disponer de sistema que identifique inequívocamente a cada usuario. Establecer política de contraseñas seguras. Disponer de registro de acceso a los sistemas: de uso de sistemas. Procedimiento de alta, baja y

B - Control de acceso	Descripción
	modificación de usuarios. Limitar acceso de superusuarios a datos personales o establecer seguimiento de actividad. Asegurar política de contraseñas seguras en todos los sistemas. Evitar usuarios genéricos.
B.2.4. CONTROLAR ACCESO FISICO AL CENTRO DE DATOS	Disponer control de acceso físico al centro de datos. Elaborar procedimiento de control de acceso físico. Disponer de registro de accesos físicos (identificando día, hora, ingresantes y motivo). Asegurar sistema de registro del control de acceso.
B.2.5. MONITOREAR ACTIVIDADES	Definir procedimiento de limpieza de cuentas inactivas con privilegios de acceso. Limitar acceso interno a sistemas con un mismo usuario a una sola sesión concurrente. Monitorear y controlar cuentas de usuario que dispongan de privilegios especiales, identificarlas en forma diferencial. Identificar y analizar intentos de autenticación fallidos.

C - Control de cambios

Relacionado con la implementación de los procesos para identificar fehacientemente a toda persona que acceda a realizar cambios en los entornos productivos que contengan datos personales, garantizando su identificación, autenticación y autorización correspondiente.

C - Control de cambios	Descripción
C.1.1. ASEGURAR CAMBIOS	Verificar que cambios en entornos productivos mantengan y aseguren integridad de datos. Asegurar durante proceso de cambio medidas de recolección de datos y control de acceso. Disponer de registro de verificaciones y/o de pruebas realizadas para asegurar integridad, disponibilidad y confidencialidad de datos. Disponer de responsable de control de entornos productivos. Disponer de procedimiento de control de cambio en entorno productivo.

D - Respaldo y recuperación

Destinado a la implementación de los procesos de respaldo que permitan una correcta recuperación ante un incidente que impida el acceso a la información originalmente almacenada, definiendo prácticas de seguridad, difusión, entrenamiento y capacitación, para el desarrollo de tareas preventivas y correctivas de los incidentes de seguridad.

D - Respaldo y recuperación	Descripción
D.1. COPIAS DE RESPALDO Y PROCESO DE RECUPERACION	
D.1.1. ASEGURAR PROCESO FORMAL DE RESPALDO Y RECUPERACION	Disponer de procedimiento resguardo de información donde se identifique: que tipo de información se resguardara; que medio físico se utilizara; cantidad de copias de resguardo que se realizaran; periodicidad de ejecuciones de copias de resguardo; descripción del proceso de realización de copias de resguardo; tiempo de almacenamiento copias; responsable realizar copias; definir y verificar procedimiento prueba de recuperación. Disponer de registro de pruebas de recuperaciones realizadas identificando: tipo de información recuperada; lugar y fecha de pruebas; resultados de pruebas de recuperación; responsable de pruebas; personal interviniente en pruebas; notificación al responsable de datos; inventario de copias, ubicación real y medio físico donde se encuentra.
D.1.2. ASEGURAR CONTROL DE ACCESO EN LOS MEDIOS	Aplicar medidas de control de acceso a copias de resguardo. Cifrar copias. Asegurar entorno de prueba de recuperación. Eliminar en forma segura información recuperada durante pruebas una vez verificada su exactitud. Disponer medidas contra incendio o inundaciones en el sitio de almacenamiento de copias de resguardo. Almacenar copias en lugar diferente al entorno productivo. Disponer procedimiento de registro y control de transito para traslado. Asegurar entorno de prueba de recuperación.

E - Gestión de vulnerabilidades

Destinado a la implementación de procesos continuos de revisión que permitan identificar, analizar, evaluar y corregir todas las vulnerabilidades posibles de los sistemas informatizados que traten información, aplicando técnicas de control de la integridad, registro, trazabilidad y verificación.

E - Gestión de vulnerabilidades	Descripción
E.1. GESTION DE VULNERABILIDADES	
E.1.1. PREVENIR INCIDENTES DE SEGURIDAD DESDE EL DISEÑO	Considerar y analizar posibles amenazas en los sistemas informatizados. Disponer mapa conceptual que permita conocer flujo de información entre sistemas informatizados. Establecer documento de seguridad que indique medidas de seguridad adoptadas para los sistemas de información.
E.1.2. ASEGURAR PROTECCION	Fijar controles de seguridad para aplicaciones

E - Gestión de vulnerabilidades	Descripción
ADECUADA	que procesen datos personales, entre ellos: segmentación de roles y perfiles; autenticación segura; gestión de sesiones (control de acceso). Gestión mensajes de error en aplicaciones. Implementar reglas y controles de seguridad en servidores conectados a una red externa y almacenen o gestionen datos personales, programando alertas ante posibles ataques. Segmentar en forma física o lógica la red de la entidad, separando áreas publicas de privadas. Separar ambientes de producción, QA, prueba y desarrollo. Implementar controles para prevenir virus informáticos en los servidores y estaciones de trabajo que almacenen o gestionen datos personales. Implementar controles para prevenir ataques en estaciones de trabajo que gestionen datos personales. Establecer y ejecutar procedimiento de actualización periódica de software/hardware de todo el equipamiento. Definir responsable del cumplimiento de las medidas de seguridad. Filtros de inyección de códigos en base de datos, en aplicaciones. Implementar controles para detectar intrusiones en la red; fuga de información en estaciones de trabajo que tengan acceso al tratamiento de datos personales.
E.1.3. DETECTAR POSIBLES INCIDENTES DE SEGURIDAD	Disponer de sistema de auditoria de incidentes implementando sistema de registro que permita seguimiento ante eventos o acciones de un posible incidente (sistema de logs). Sincronizar todos los servidores / equipamiento con un servidor de horario público para asegurar una correcta trazabilidad en caso de realizar una auditoría. Implementar proceso de denuncia que permita que usuarios alerten eventos de seguridad. Disponer sistema de gestión de incidentes capaz de mostrar fecha de registro, documentación relevante, personas involucradas, activos afectados.
E.1.4. GARANTIZAR MEDIDAS EFICACES Y PERDURABLES	Implementar periódicamente procesos de auditoria interna para verificar cumplimiento de lo anterior, exportando informes y resguardándolos. Realizar auditorías externas a fin de evaluar seguridad de sistemas internos.

F - Destrucción de la información

Relacionado con la implementación de los procesos de eliminación de datos, asegurando que el contenido confidencial sea debidamente destruido, utilizando métodos de borrado seguro y aplicando un control eficaz del proceso.

F - Destrucción de la información	Descripción
F.1. ASEGURAR DESTRUCCION INFORMACION	
F.1.1. ESTABLECER FORMATO/MODELO DE DESTRUCCION	Fijar procedimiento destrucción de datos en donde se identifique: tipo de información a destruir; medio que contiene la información; responsable de la destrucción; descripción del proceso y método de destrucción utilizado.
F.1.2. ESTABLECER MECANISMOS SEGUROS DE ELIMINACION	Fijar procedimiento destrucción físico o lógico de datos que asegure el borrado total de la información sin posibilidad de recuperación de la misma cumpliendo tres premisas: 1) irreversibilidad; 2) seguridad; 3) confidencialidad.
F.1.3. DESIGNAR RESPONSABLE DE DESTRUCCION	Fijar persona autorizada para la destrucción y documentar su autorización.
F.1.4. MONITOREAR PROCESO	Disponer de inventario que identifique medios destruidos
F.1.5. DESCARTE MEDIOS MAGNETICOS	Implementar proceso de destrucción lógico de reescritura continua, de modo que los datos originales no puedan ser recuperados, pudiendo reutilizar el medio magnético. En caso de no poder realizar el proceso de destrucción lógico, implementar proceso de destrucción física utilizando técnicas de desmagnetización, desintegración, incineración, pulverización, trituración o fundición.

G - Incidentes de seguridad

Relativo al tratamiento de los eventos y consecuentes incidentes de seguridad que puedan afectar los datos personales, su detección, evaluación, contención y respuesta, como así también las actividades de escalamiento y corrección del entorno técnico y operativo.

G - Incidentes de seguridad	Descripción
G.1. NOTIFICACION ANTE INCIDENTES DE SEGURIDAD	
G.1.1. ESTABLECER RESPONSABILIDADES Y PROCEDIMIENTOS	Elaborar procedimiento de gestión ante incidentes de seguridad. Establecer responsable de comunicación.
G.1.2. ELABORAR INFORMES	Elaborar informe del incidente de seguridad que tenga contenido mínimo: 1) naturaleza de la

	violación; 2) categoría de dato personal afectado; 3) identificación usuarios afectados; 4) medidas adoptadas por responsable para mitigar incidente; 5) medidas aplicadas para evitar futuros incidentes
G.1.3. ENVIAR NOTIFICACION	Enviar notificación anexando informe a Av. Julio Roca 710, CABA, CP: 1067ABP. Email: incidente.seguridad@aaip.gob.ar

H - Entornos de Desarrollo

Relativo a la definición de los entornos de desarrollo de los sistemas de información, sean propios o de terceros.

H - Entornos de Desarrollo	Descripción
H.1. SEGURIDAD EN ENTORNO DE DESARROLLO	
H.1.1. IMPLEMENTAR POLITICA DE DESARROLLO SEGURO	Utilizar técnicas de enmascaramiento o disociación de la información en entorno de desarrollo, prueba y QA. En caso de no cumplir este punto y utilizar datos personales en entornos de desarrollo, prueba y QA, deberá considerarse y aplicar todas las medidas de los puntos A, B, C, D, E, F, G,

Medidas de seguridad recomendadas para el tratamiento y conservación de los datos personales en medios no informatizados

El anexo II establece:

De modo referencial y con el objetivo de facilitar el cumplimiento de la Ley N° 25.326 de Protección de los Datos Personales, se establecen las medidas de seguridad recomendadas para la administración, planificación, control y mejora continua de la seguridad de la información.

A - Recolección de datos

Relacionado con los procesos necesarios para asegurar la completitud e integridad de los datos minimizando los errores.

A - Recolección de datos	Descripción
A.1. INTEGRIDAD	
A.1.1. ASEGURAR COMPLETITUD	Verificar que campos que componen formulario de recolección de datos permitan ingreso completo de dato requerido
A.1.2. MINIMIZAR ERRORES DE INGRESO	Indicar en forma clara y concreta el tipo de información a ingresar y su formato

B - Control de acceso

Relacionado con la implementación de medidas de seguridad para la protección de la identidad y la privacidad.

B - Control de acceso	Descripción
B.1. IDENTIFICACION DE ACTIVOS	
B.1.1. IDENTIFICAR ACTIVOS	Elaborar inventario de activos informáticos que almacenen o gestionen datos personales
B.1.2. DEFINIR RESPONSABLES Y RESPONSABILIDADES	Definir propietarios de activos informáticos que almacenen o gestionen datos personales. Notificar a los propietarios. Especificar a los propietarios autorizaciones de acceso (tipo de acceso y validez)
B.1.3. VERIFICAR APLICACIÓN DE CONTROLES	Elaborar procedimientos de 1) actualización periódica del inventario: 2) verificación de autorizaciones: 3) para nuevos activos informáticos, definiendo responsable asignado y autorizaciones.
B.2. ACCESO A LOS DATOS	
B.2.1. GESTIONAR ACCESOS A SISTEMAS	Elaborar documento interno que defina controles de acceso a cada sistema. Definir e identificar aquellos superusuarios (administradores) puedan evadir controles de acceso definidos para el propietario. Controlar y monitorear a superusuarios (registrar acceso y actividad)
B.2.2. ASIGNAR PERMISOS	Disponer de notificación concreta y formal de responsabilidades asumidas por cada usuario que acceda internamente a los sistemas (notificación fehaciente)
B.2.3. VERIFICAR IDENTIFICACION Y AUTORIZACION	Disponer de sistema que identifique inequívocamente a cada usuario. Establer política de contraseñas seguras. Disponer de registro de acceso a los sistemas: de uso de sistemas. Procedimiento de alta, baja y modificación de usuarios. Limitar acceso de superusuarios a datos personales o establecer seguimiento de actividad. Asegurar política de contraseñas seguras en todos los sistemas. Evitar usuarios genéricos.
B.2.4. CONTROLAR ACCESO FISICO AL CENTRO DE DATOS	Disponer control de acceso físico al centro de datos. Elaborar procedimiento de control de acceso físico. Disponer de registro de accesos físicos (identificando día, hora, ingresantes y motivo). Asegurar sistema de registro del control de acceso.
B.3. COPIA O REPRODUCCION	
B.3.1. CONTROLAR COPIAS REPRODUUCCION	Asegurar control del responsable autorizado en la generación de copias o la reproducción de documentos

B - Control de acceso	Descripción
B.4. TRASLADO DOCUMENTACION	
B.4.1. CONTROLAR TRASLADO	Adoptar medidas de seguridad a fin de asegurar confidencialidad e impedir la sustracción, pérdida, manipulación o accesos indebido de la información objeto de traslado.
B.4.2. ASEGURAR ELIMINACION	Asegurar medidas de destrucción de la información (punto D) en la eliminación de las copias o reproducciones desechadas para evitar acceso a la información contenida en las mismas o su recuperación posterior.

C - Conservación de la información

Relacionado con la implementación de las medidas de control de ventilación, iluminación y demás condiciones que garanticen la integridad física y funcional de la información.

C. CONSERVACION DE LA DOCUMENTACION	Descripción
C.1. CONTROL CONDICIONES AMBIENTALES	
C.1.1. CONDICIONES AMBIENTALES	Implementar medidas para evitar la incidencia de luz directa sobre documentación y archivos. Asegurar el control de las instalaciones eléctricas en el local de depósito. Implementar medidas para controlar condiciones de temperatura y humedad en el local de depósito.
C.2. CONTROL DE INCENDIOS E INUNDACIONES	
C.2.1. INCENDIOS E INUNDACIONES	Disponer medidas de protección contra incendios o inundaciones en el local de depósito.

D - Destrucción de la información

Relacionado con la implementación de los procesos de eliminación de datos, asegurando que el contenido confidencial sea debidamente destruido, utilizando métodos de destrucción seguros y aplicando un control eficaz.

D - Destrucción de la información	Descripción
D.1. ASEGURAR DESTRUCCION INFORMACION	
D.1.1. ESTABLECER FORMATO/MODELO DE DESTRUCCION	Fijar procedimiento destrucción de datos en donde se identifique: tipo de información a destruir; medio que contiene la información;

D - Destrucción de la información	Descripción
	responsable de la destrucción; descripción del proceso y método de destrucción utilizado.
D.1.2. ESTABLECER MECANISMOS SEGUROS DE ELIMINACION	Fijar procedimiento destrucción físico o lógico de datos que asegure el borrado total de la información sin posibilidad de recuperación de la misma cumpliendo tres premisas: 1) irreversibilidad; 2) seguridad; 3) confidencialidad.
D.1.3. DESIGNAR RESPONSABLE DE DESTRUCCION	Fijar persona autorizada para la destrucción y documentar su autorización.
D.1.4. MONITOREAR PROCESO	Disponer de inventario que identifique medios destruidos
D.1.5. DESCARTE DE ARCHIVOS	Implementar proceso de destrucción física utilizando técnicas de desintegración, incineración, pulverización, trituración o fundición.

E - Incidentes de seguridad

Relativo al tratamiento de los eventos y consecuentes incidentes de seguridad, que puedan afectar los datos personales, su detección, evaluación, contención y tratamiento.

E - Incidentes de seguridad	Descripción
E.1. NOTIFICACION ANTE INCIDENTES DE SEGURIDAD	
E.1.1. ESTABLECER RESPONSABILIDADES Y PROCEDIMIENTOS	Elaborar procedimiento de gestión ante incidentes de seguridad. Establecer responsable de comunicación.
E.1.2. ELABORAR INFORMES	Elaborar informe del incidente de seguridad que tenga contenido mínimo: 1) naturaleza de la violación; 2) categoría de dato personal afectado; 3) identificación usuarios afectados; 4) medidas adoptadas por responsable para mitigar incidente; 5) medidas aplicadas para evitar futuros incidentes
E.1.3. ENVIAR NOTIFICACION	Enviar notificación anexando informe a Av. Julio Roca 710, CABA, CP: 1067ABP. Email: incidente.seguridad@aaip.gob.ar

6. Derechos de los titulares de datos

Como motor principal de la norma, la ley de protección de datos contempla en su capítulo 3 los derechos que le caben a los titulares de datos.

DERECHO DE INFORMACIÓN

El artículo 13 establece el Derecho de información de la siguiente manera:

"Toda persona puede solicitar información al organismo de control relativa a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables. El registro que se lleve al efecto será de consulta pública y gratuita."

DERECHO DE ACCESO

El artículo 14 establece el Derecho de acceso de la siguiente manera:

"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."

DERECHO DE CONTENIDO DE LA INFORMACION

El artículo 15 establece el Derecho de acceso de la siguiente manera:

"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."

DERECHO DE RECTIFICACIÓN, ACTUALIZACIÓN O SUPRESIÓN

El artículo 16 establece el Derecho de rectificación, actualización o supresión en los siguientes términos:

"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."

EXCEPCIONES

El articulo 17 contempla una serie de excepciones a los derechos de acceso, rectificación o supresión de datos. Ellas son:

"1. Los responsables o usuarios de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación o la supresión en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros.

2. La información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser fundada y notificada al afectado.

3. Sin perjuicio de lo establecido en los incisos anteriores, se deberá brindar acceso a los registros en cuestión en la oportunidad en que el afectado tenga que ejercer su derecho de defensa."

GRATUIDAD

El artículo 19 establece que "*la rectificación, actualización o supresión de datos personales inexactos o incompletos que obren en registros públicos o privados se efectuará sin cargo alguno para el interesado."*

7. Acción de protección de datos personales

El capítulo 7 de la ley de protección de datos personales regula la procedencia, la legitimación activa y pasiva de la acción de habeas data a saber:

Procedencia según el artículo 33:

"La acción de protección de los datos personales o de hábeas data procederá:

a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos;

b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización."

Legitimación activa según el artículo 34:

"La acción de protección de los datos personales o de hábeas data podrá ser ejercida por el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado.

Cuando la acción sea ejercida por personas de existencia ideal, deberá ser interpuesta por sus representantes legales, o apoderados que éstas designen al efecto.

En el proceso podrá intervenir en forma coadyuvante el Defensor del Pueblo."

Legitimación pasiva según el artículo 35:

"La acción procederá respecto de los responsables y usuarios de bancos de datos públicos, y de los privados destinados a proveer informes."

8. Registro Nacional de Documentos Cuestionados

Mediante Disposición DNPDP N° 24/2010, publicado por Boletin Oficial el 7 de Octubre 2010, la Agencia de Acceso a la Información Pública (Dirección Nacional de Protección de Datos Personales) crea el REGISTRO NACIONAL DE DOCUMENTOS DE IDENTIDAD CUESTIONADOS

Los objetivos de dicho Registro son:

- organizar y mantener actualizado un registro informatizado donde consten el número y tipo de documentos de identidad que fueran denunciados a este registro por las autoridades públicas competentes y/o los propios titulares de los mismos con motivo de pérdida, hurto, robo o cualquier otra alteración.
- tramitar las consultas de quienes deseen saber si un documento de identidad ha sido incluido en el Registro antes citado, a través del sistema que se diseñará al efecto.

9. Ley 26.388 de Delitos Informáticos

La Ley 26.388 de Delitos Informáticos fue promulgada el 25 de Junio de 2.008, de este modo se incorpora Argentina a la lista de países que cuentan con regulación legal sobre la materia.

Se trata de una ley que modifica, sustituye e incorpora figuras típicas a diversos artículos del Código Penal (CP) vigente, con el objeto de regular las nuevas tecnologías como medios de comisión de delitos previstos en el CP.

Tipifica, entre otros, los siguientes delitos informáticos:

- Pornografía infantil por Internet u otros medios electrónicos (art. 128 CP)
- Violación, apoderamiento y desvío de comunicación electrónica (art. 153, párrafo 1º CP)
- Intercepción o captación de comunicaciones electrónicas o telecomunicaciones (art. 153, párrafo 2º CP)
- Acceso a un sistema o dato informático (artículo 153 bis CP)
- Publicación de una comunicación electrónica (artículo 155 CP)
- Acceso a un banco de datos personales (artículo 157 bis, párrafo 1º CP)
- Revelación de información registrada en un banco de datos personales (artículo 157 bis, párrafo 2º CP)
- Inserción de datos falsos en un archivo de datos personales (artículo 157 bis, párrafo 2º CP; anteriormente regulado en el artículo 117 bis, párrafo 1º, incorporado por la Ley de Hábeas Data)
- Fraude informático (artículo 173, inciso 16 CP)
- Daño o sabotaje informático (artículo 183 y 184, incisos 5º y 6º CP)

Las penas establecidas son: a) prisión; b) inhabilitación (cuando el delito lo comete un funcionario público o el depositario de objetos destinados a servir de prueba); c) multa (ej: art. 155).

10. Ley 26.951. Registro Nacional No Llame

La Ley 26.951 de Servicios de Telefonía fue promulgada el 30 de Julio de 2.014, de este modo crea el Registro Nacional No Llame.

La Dirección Nacional de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos de la Nación **es** el organismo que tiene a cargo la administración del Registro Nacional No Llame, así como también llevar adelante las actuaciones administrativas por incumplimiento de la Ley 26.951.

El Registro Nacional No Llame, brinda la opción de evitar el contacto telefónico no solicitado que recibís en tu teléfono fijo o celular.

Dentro de los 30 días de inscripción de un número de teléfono o celular en el Registro, quienes publiciten, oferten, vendan o regalen bienes o servicios deberán dejar de contactar ese número.

OBJETO

El Registro Nacional No Llame garantiza el Derecho a no recibir llamadas que publiciten, oferten, vendan o regalen bienes o servicios.

El Registro Nacional No Llame facilita y simplifica el "derecho de bloqueo" que la Ley 25.326 contempla en el artículo 27 inciso 3. Este derecho se ejerce individualmente ante cada empresa. El Registro Nacional No Llame permitirá ejercer en un solo lugar y de manera simple y eficiente la opción de no ser contactado.

COMO

El trámite de inscripción y baja del Registro es **gratuito y sencillo.** Se efectúa por Internet o telefónicamente mediante el número 146.

Quienes publiciten, oferten, vendan o regalen bienes o servicios utilizando como medio de contacto los servicios de telefonía no podrán dirigirse a los inscriptos en el Registro Nacional No Llame. Para ello, deberán consultar al menos cada 30 días la base de datos de inscriptos, proporcionada por este organismo. Para acceder a la ella deberán previamente registrarse y generar un usuario y contraseña.

El titular o usuario autorizado podrá denunciar ante este organismo el incumplimiento de lo establecido en esta ley. El organismo de control podrá aplicar las sanciones de apercibimiento, suspensión, clausura o cancelación de la base de datos y/o multas de mil pesos ($ 1.000.-) a cien mil pesos ($ 100.000.-), por cada infracción que se constate.

11. Fuentes de consultas

- www.jus.gov.ar/dnpdp
- Constitución Nacional
- Ley N° 25.326 de Protección de los Datos Personales, promulgada el 30 de Octubre
- de 2.000
- Ley N° 26.343 de Protección de los Datos Personales. Modificación ley 25.326, promulgada el 08 de Enero de 2.008
- Resoluciones y Disposiciones Varias de la Agencia de Acceso a la Información Publica (Ex Dirección Nacional de Protección de Datos Personales)
- Palazzi Pablo, *"La protección de los datos personales en la Argentina"*, Errepar,
- Argentina, 1° edición, 2004

- Ley N° 26.388 de Delitos Informáticos, promulgada el 25 de Junio de 2008.

- www.carranzatorres.com.ar

- Ley N° 26.951 de Registro Nacional No Llame, promulgada el 25 de Julio de 2014.