

Normativa (/normativa) / Resolución 47/2018 (/normativa/nacional/resoluci%C3%B3n-47-2018-312662) /

AGENCIA DE ACCESO A LA INFORMACION PUBLICA
2018-07-25

AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA

Resolución 47/2018

RESOL-2018-47-APN-AAIP

Ciudad de Buenos Aires, 23/07/2018

VISTO el EX-2018-33523527-APN-DNPDP#AAIP, la Ley N° 25.326, la Ley N° 27.275, el Decreto N° 1558 del 29 de noviembre de 2001 modificado por el Decreto N° 1160 del 11 de agosto de 2010, el Decreto N° 746 del 25 de septiembre de 2017, el Decreto N° 899 del 6 de noviembre de 2017, las Disposiciones de la DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES N° 11 del 22 de septiembre de 2006 y N° 9 del 3 de septiembre de 2008; y

CONSIDERANDO:

Que por el artículo 19 de Ley N° 27.275 se creó la AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA como ente autárquico con autonomía funcional, en la órbita de la JEFATURA DE GABINETE DE MINISTROS.

Que por el Decreto N° 746 del 25 de septiembre de 2017 se sustituyó el artículo 19 de la Ley de Acceso a la Información Pública N° 27.275, atribuyendo a la referida Agencia la facultad de actuar como Autoridad de Aplicación de la Ley de Protección de Datos Personales N° 25.326, como así también en su artículo 13, se incorporó como inciso t) al artículo 24 del capítulo IV de la de la Ley 27.275 de Derecho de Acceso a la Información Pública, la competencia de “Fiscalizar la protección integral de los datos personales asentados en archivos, registros, banco de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, y el acceso a la información que sobre las mismas se registre”.

Que por el artículo 29 del ANEXO I al Decreto N° 1558 de fecha 29 de noviembre de 2001, se creó la DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES en el ámbito de la entonces SECRETARÍA DE JUSTICIA Y ASUNTOS LEGISLATIVOS del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, para cumplir las funciones de órgano de control y autoridad de aplicación de la Ley de Protección de Datos Personales N° 25.326 y su reglamentación.

Que el Decreto N° 899 de fecha 6 de noviembre 2017, reordenó el plexo regulatorio vigente en relación a las competencias asignadas a los organismos mencionados y de conformidad con los términos del artículo 19 de la Ley N° 27.275, sustituido por el artículo 11 del Decreto N° 746/17, atribuyó a la AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA, el ejercicio de la función de órgano de control de la Ley N° 25.326, que hasta entonces detentaba la entonces DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES dependiente del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS.

Que, en virtud de lo expuesto, el Decreto N° 899/17 dispuso en su artículo 2° que “Toda referencia normativa a la DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES, su competencia o sus autoridades, se considerará referida a la AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA” .

Que, entre las atribuciones asignadas a la AGENCIA DE ACCESO A LA INFORMACIÓN PUBLICA se encuentra la de dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas en la Ley N° 25.326 artículo 29, inciso 1, apartado b), como así también, la de controlar la observancia de las normas sobre integridad y seguridad de los datos por parte de los archivos, registros o bancos de datos, artículo 29, inciso 1, apartado d), de la Ley N° 25.326.

Que, la entonces DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, dictó normas relativas a las condiciones de seguridad que deben observarse para los archivos, registros y bases o bancos de datos de carácter personal, y aprobó las medidas de seguridad para el tratamiento y conservación de los datos personales, que deben aplicar los responsables y usuarios de archivos, registros, bases y bancos de datos públicos no estatales y privados.

Que mediante Disposición N° 11 de fecha 22 de Septiembre 2006 la entonces DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES aprobó el documento “Medidas de Seguridad para el Tratamiento y Conservación de los Datos Personales Contenidos en Archivos, Registros, Bancos y Bases de Datos Públicos no estatales y Privados”, como instrumento para la especificación de la normativa de seguridad, al que debían adecuarse los responsables y usuarios de archivos, registros, bases y banco de datos públicos no estatales y privados.

Que, asimismo, por Disposición DNPDP N° 9 de fecha 3 de Septiembre de 2008 se aprobó un modelo de “Documento de Seguridad de Datos Personales” que contenía los lineamientos indispensables mínimos que permitía a los obligados diseñar un instrumento que se adecue a las necesidades de su organización y cumpla con las normas dictadas en la materia.

Que el desarrollo de la tecnología e internet ha evolucionado a lo largo de los años a un ritmo vertiginoso, como así también las redes sociales, los servicios de mensajería instantánea y el comercio a través de la red. Ello pone en continuo riesgo la seguridad, integridad y confidencialidad de la información que contiene datos personales.

Que, conscientes de la importancia que reviste el resguardo de la integridad y seguridad de la información en materia de datos personales, se propicia actualizar las medidas de seguridad que deben observar quienes hagan tratamientos de datos personales en archivos, registros, bancos y bases de datos públicos y privados, con el objeto de eliminar y/o mitigar los riesgos de dicha información.

Que, de conformidad con lo prescripto por el artículo 9° de la Ley N° 25.326, el responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad y confidencialidad de los datos personales, a fin 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.

Que el Decreto N° 891 de fecha 1 de noviembre de 2017, aprueba las “Buenas Prácticas en Materia de Simplificación”, propiciándose entre otras medidas, la simplificación normativa y la mejora continua de los procesos.

Que, esta AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA, en cumplimiento de las funciones asignadas por la Ley N° 25.326 y en su carácter de Órgano de Control, estima pertinente aprobar nuevas medidas de seguridad recomendadas, las que resultan acordes con los estándares internacionales a la fecha de su dictado, para la protección de la confidencialidad e integridad de la información que contiene datos de carácter personal en todo el proceso de tratamiento, desde su recolección hasta su destrucción.

Que a tal fin, resulta necesario establecer nuevas medidas de seguridad recomendadas para la administración, planificación, control y mejora continua de la seguridad de la información, respecto al tratamiento de los datos personales.

Que la DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS de la SUBSECRETARÍA DE COORDINACIÓN ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS ha tomado la intervención que le compete.

Que, la presente medida se dicta en uso de las facultades conferidas por el artículo 29, inciso 1, apartados b) y d) de la Ley N° 25.326, modificatorios y complementarios.

Por ello,

EL DIRECTOR DE LA AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA

RESUELVE:

ARTÍCULO 1°.- Deróguense las Disposiciones de la entonces DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS N° 11 del 22 de setiembre de 2006 y N° 09 del 3 de septiembre de 2008.

ARTÍCULO 2°.- Apruébese el documento denominado “MEDIDAS DE SEGURIDAD RECOMENDADAS PARA EL TRATAMIENTO Y CONSERVACION DE LOS DATOS PERSONALES EN MEDIOS INFORMATIZADOS”, cuyo texto forma parte integrante de la presente como Anexo I (IF-2018-34800234-APN-AAIP).

ARTÍCULO 3°.- Apruébese el documento denominado “MEDIDAS DE SEGURIDAD RECOMENDADAS PARA EL TRATAMIENTO Y CONSERVACION DE LOS DATOS PERSONALES EN MEDIOS NO

INFORMATIZADOS” cuyo texto forma parte integrante de la presente como Anexo II (IF-2018-34800290-APN-AAIP).

ARTÍCULO 4º.- Comuníquese, publíquese, dese a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL y, oportunamente, archívese. Eduardo Andrés Bertoni

NOTA: El/los Anexo/s que integra/n este(a) Resolución se publican en la edición web del BORA - www.boletinoficial.gob.ar-

e. 25/07/2018 N° 53148/18 v. 25/07/2018

(Nota Infoleg: Los anexos referenciados en la presente norma han sido extraídos de la edición web de Boletín Oficial.)



República Argentina - Poder Ejecutivo Nacional
2018 - Año del Centenario de la Reforma Universitaria

Anexo

Número: IF-2018-34800234-APN-AAIP

CIUDAD DE BUENOS AIRES

Viernes 20 de Julio de 2018

Referencia: ANEXO I Medidas de seguridad recomendadas para el tratamiento y conservación de los Datos Personales en medios informatizados

ANEXO I-

'Medidas de seguridad recomendadas para el tratamiento y conservación de los Datos Personales en medios informatizados'.

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 aquí 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.

La Ley N° 25.326 en su artículo 2° define: Datos Personales (en adelante DP) a 'Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables'. Datos Sensibles (en adelante DS) a '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'.

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.

DP

A	RECOLECCIÓN DE DATOS	
A.1	Integridad	
A.1.1	Asegurar completitud	la Verificar que los campos que componen el formulario de recolección de datos permitan el ingreso completo de los datos requeridos.
A.1.2	Minimizar los errores de ingreso	Indicar en forma clara y concreta el tipo de información a ingresar y el formato de la misma.
A.1.3	Asegurar integridad	la Verificar la exactitud del dato ingresado en caso de que el tipo de registro lo permita (ej. Fecha formato: DD/MM/AAAA)
A.2	Confidencialidad	
A.2.1	Asegurar confidencialidad durante el proceso de recolección	la Cifrar la comunicación cliente-servidor durante la recolección.
A.2.2	Limitar el acceso a la recolección de los datos	Limitar cache del formulario en el cliente únicamente al momento de carga de datos. Limitar la carga de datos en el cliente a una sola sesión de usuario.
A.2.3	Limitar el acceso no autorizado durante la recopilación	Utilizar certificados digitales seguros y validados por entidades autorizadas (CA).

DS

A.2.3	Limitar el acceso no autorizado durante la recopilación	Cifrar la comunicación durante el 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.

DP

B	CONTROL DE ACCESO	
B.1	Identificación de activos	
B.1.1	Identificar los activos	Elaborar un 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 de activos informáticos que almacenen o gestionen datos personales. Especificar a los propietarios de activos informáticos autorizaciones de acceso (tipo de acceso y validez).
B.1.3	Verificar la aplicación de	Elaborar un procedimiento de actualización periódica del inventario. Elaborar un procedimiento de verificación de autorizaciones.

	controles	Elaborar un procedimiento para nuevos activos informáticos, definiendo responsable asignado y autorizaciones.
B.2	Acceso a los datos	
B.2.1	Gestionar los accesos a los sistemas	Elaborar un documento interno que defina los controles de acceso a cada sistema. Definir e identificar aquellos usuarios que por su rol de superusuarios (administradores) puedan evadir los controles de acceso definidos para el propietario. Controlar y monitorear a los superusuarios (registrando accesos y actividad).
B.2.2	Asignar permisos	Disponer de una notificación concreta y formal de las responsabilidades asumidas por cada usuario que acceda internamente a los sistemas (notificación fehaciente).
B.2.3	Verificar la identificación y autorización	Disponer de un sistema que identifique inequívocamente a cada usuario. Establecer una política de contraseñas seguras. Disponer de un registro de acceso a los sistemas. Disponer de un registro de uso de los sistemas. Disponer de un procedimiento de Alta, Baja, Modificación de usuarios. Limitar el acceso de los superusuarios a los datos personales o establecer un seguimiento de su actividad. Asegurar la implementación de la política de contraseñas seguras en todos los sistemas. Evitar el uso de usuarios genéricos.
B.2.4	Controlar el acceso físico al centro de datos	Disponer de un control de acceso físico al centro de datos. Elaborar un procedimiento de control de acceso físico. Disponer de un registro de los accesos físicos (identificando día, hora, ingresantes y motivo). Asegurar el sistema de registro del control de acceso.
B.2.5	Monitorear la actividad	Definir un procedimiento de limpieza de cuentas inactivas con privilegios de acceso.

DS

B.2.5	Monitorear la actividad	Limitar el acceso interno a los sistemas con un mismo usuario a una sola sesión concurrente. Monitorear y controlar las 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.

DP

C	CONTROL DE CAMBIOS	
C.1	Control de cambios	
C.1.1	Asegurar los cambios	Verificar que los cambios a realizar en entornos productivos mantengan y aseguren la integridad de los datos.
		Asegurar durante los procesos de cambio las medidas de Recolección de datos (punto A) y Control de acceso (punto B).
		Disponer de un registro de las verificaciones y/o pruebas realizadas para asegurar la integridad, disponibilidad y confidencialidad de los datos.

DS

C.1.1	Asegurar los cambios	Definir un responsable de control de entornos productivos.
		Disponer de un procedimiento de control de cambios en entornos productivos.

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.

DP

D	RESPALDO Y RECUPERACIÓN	
D.1	Copias de respaldo y proceso de recuperación	
		Disponer de un procedimiento de resguardo de información donde se identifique:
		qué tipo de información se resguardará
		qué medio físico se utilizará
		cantidad de copias de resguardo que se realizarán
		periodicidad de las ejecuciones de copias de resguardo
		descripción del proceso de la realización de

D.1.1	Asegurar un proceso formal de respaldo y recuperación	copias de resguardo
		tiempo de almacenamiento de copias de resguardo
		responsable de la realización de copias de resguardo
		Definir y verificar procedimiento de pruebas de recuperación.
		Disponer de un registro de pruebas de recuperación realizadas identificando:
		tipo de información recuperada
		lugar y fecha donde se realizaron las pruebas de recuperación
		resultado de las pruebas de recuperación
		responsable de la realización de las pruebas de recuperación
		personal interviniente en las pruebas de recuperación
		notificación al responsable de datos
		Disponer de un inventario que identifique las copias de seguridad, su ubicación real y el medio físico en donde se encuentran.
D.1.2	Asegurar control de acceso en los medios	Aplicar las medidas de Control de acceso (B) a las copias de resguardo.
		Cifrar las copias de resguardo utilizando herramientas seguras.
		Asegurar los entornos de prueba de recuperación utilizando las mismas medidas de seguridad que un entorno productivo.
		Eliminar en forma segura la información recuperada durante las pruebas una vez verificada su exactitud.

DS

D.1.2	Asegurar control de acceso en los medios	Disponer medidas de protección contra incendios o inundaciones en el sitio de almacenamiento de los medios físicos que contienen las copias de resguardo.
		Almacenar las copias de resguardo en una locación física diferente a la del sistema productivo.
		En caso de traslado de copias de resguardo, disponer de un procedimiento de registro y control del tránsito.
		Asegurar los entornos de prueba de recuperación utilizando las mismas medidas de seguridad que un entorno productivo.

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.

DP

E	GESTIÓN DE VULNERABILIDADES	
E.1	Gestión de vulnerabilidades	
E.1.1	Prevenir incidentes de seguridad desde el diseño	<p>Considerar y analizar las posibles amenazas a la que estarán expuestos los sistemas informatizados.</p> <p>Disponer de un mapa conceptual que permita conocer el flujo de la información entre los distintos sistemas informatizados.</p> <p>Establecer un documento de seguridad que indique las medidas de seguridad adoptadas para los sistemas de información.</p>
E.1.2	Asegurar una protección adecuada	<p>Establecer controles de seguridad para las aplicaciones que procesen datos personales, entre ellas:</p> <ul style="list-style-type: none"> Segmentación de roles y perfiles Autenticación segura Gestión de sesiones (cumpliendo apartado de Control de acceso (B)) Gestión de mensajes de error en aplicaciones <p>Implementar reglas y controles de seguridad en los servidores que estén conectados a una red externa y almacenen o gestionen datos personales, programando alertas ante posibles ataques.</p> <p>Segmentar en forma física o lógica la red de la entidad, separando las áreas públicas de las privadas.</p> <p>Separar los ambientes de Producción, QA, Prueba y Desarrollo.</p> <p>Implementar controles para la prevención de virus informáticos en los servidores que almacenen o gestionen datos personales.</p> <p>Implementar controles para la prevención de ataques en las estaciones de trabajo que gestionen datos personales.</p> <p>Implementar controles para la prevención de virus informáticos en las estaciones de trabajo que gestionen datos personales.</p> <p>Establecer y ejecutar un procedimiento de actualización periódica de software/hardware de todo el equipamiento.</p> <p>Definir a una persona responsable del cumplimiento de las medidas de seguridad.</p>
		Disponer de un sistema de auditoria de incidentes implementando un sistema de registro que permita realizar un seguimiento ante eventos o acciones de un

E.1.3	Detectar posibles incidentes de seguridad	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 un proceso de denuncia que permita que los usuarios alerten eventos de seguridad.
		Disponer de un sistema de gestión de incidentes capaz de mostrar fecha de registro, documentación relevante, personas involucradas, activos afectados.

DS

E.1.2	Asegurar una protección adecuada	Establecer controles de seguridad para las aplicaciones que procesen datos personales, entre ellas:
		Filtros de inyección de código en bases de datos
		Filtros de inyección de código en aplicaciones
		Implementar controles para la detección de intrusiones en la red.
E.1.4	Garantizar medidas eficaces y perdurables	Implementar controles para la detección de intrusos y/o fuga de información en las estaciones de trabajo que tengan acceso al tratamiento de datos personales.
		Implementar periódicamente procesos de auditoría interna para verificar el cumplimiento de lo mencionado con anterioridad, exportando informes y resguardándolos.
		Realizar auditorías externas a fin de evaluar la seguridad de los 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.

DP

F	DESTRUCCIÓN DE LA INFORMACIÓN	
F.1	Asegurar la destrucción de la información	
F.1.1	Establecer modelo/formato de destrucción	Establecer un procedimiento de 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
	Establecer	Implementar un proceso de destrucción físico o lógico de la información que asegure el borrado total de la información sin posibilidad de recuperación de

F.1.2	mecanismos seguros de eliminación	la misma cumpliendo tres premisas: irreversibilidad seguridad confidencialidad
F.1.3	Designar responsable de destrucción	Establecer una persona autorizada para la destrucción y documentar su autorización.
F.1.4	Monitorear el proceso	Disponer de un inventario que identifique los medios destruidos.

DS

F.1.2	Descarte de medios magnéticos	Implementar un 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 lógica, implementar un 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.

DP

G	INCIDENTES DE SEGURIDAD	
G.1	Notificación ante incidentes de seguridad	
G.1.1	Establecer responsabilidades y procedimientos	Elaborar un procedimiento de gestión ante incidentes de seguridad. Establecer una persona responsable de la comunicación.
G.1.2	Elaborar informe	Elaborar un informe del incidente de seguridad que tenga de contenido mínimo: la naturaleza de la violación categoría de datos personales afectados Identificación de usuarios afectados medidas adoptadas por el responsable para mitigar el incidente medidas aplicadas para evitar futuros incidentes
		Enviar notificación de incidente anexando el informe a: Av. Pte. Gral. Julio A. Roca 710 - CABA -
G.1.3	Enviar notificación	C1067ABP Correo electrónico: 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.

DP

H	ENTORNOS DE DESARROLLO	
H.1	Seguridad en los entornos de desarrollo	
H.1.1	Implementar política de desarrollo seguro	Utilizar técnicas de enmascaramiento o disociación de la información en entornos de desarrollo, prueba y QA.
En caso de no cumplir el punto H.1.1 y utilizar datos personales en entornos de desarrollo, prueba y QA, deberán considerarse y aplicar todas las medidas recomendadas anteriormente en los puntos A,B,C,D,E,F,G.		

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
 DN: cn=GESTION DOCUMENTAL ELECTRONICA - GDE, o=AR, o=MINISTERIO DE MODERNIZACION,
 ou=SECRETARIA DE MODERNIZACION ADMINISTRATIVA, serialNumber=CUIT 30715117564
 Date: 2018.07.20 16:28:09 -0300'

Eduardo Andrés Bertoni
 Director
 Agencia de Acceso a la Información Pública



República Argentina - Poder Ejecutivo Nacional
 2018 - Año del Centenario de la Reforma Universitaria

Anexo

Número: IF-2018-34800290-APN-AAIP

CIUDAD DE BUENOS AIRES

Viernes 20 de Julio de 2018

Referencia: ANEXO II Medidas de seguridad recomendadas para el tratamiento y conservación de los Datos Personales en medios NO informatizados

ANEXO II -

'Medidas de seguridad recomendadas para el tratamiento y conservación de los Datos Personales en medios NO informatizados'.

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 aquí 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.

La Ley N° 25.326 en su artículo 2° define: Datos Personales (en adelante DP) a 'Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables'. Datos Sensibles (en adelante DS) a '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'.

A - Recolección de datos

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

DP

A	RECOLECCIÓN DE DATOS	
A.1	Integridad	
A.1.1	Asegurar la completitud	Verificar que los campos que componen el formulario de recolección de datos permitan el ingreso completo de los datos requeridos.
A.1.2	Minimizar los errores de ingreso	Indicar en forma clara y concreta el tipo de información a ingresar y el formato de la misma.

B - Control de acceso

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

DP

B	CONTROL DE ACCESO	
B.1	Identificación de activos	
B.1.1	Identificar los activos	Elaborar un inventario de los archivos de documentos que contengan datos personales.
B.1.2	Definir responsables y responsabilidades	Definir responsables de los archivos de documentos que contengan datos personales. Notificar a los responsables de los archivos de documentos que contengan datos personales. Especificar a los responsables de los archivos autorizaciones de acceso (tipo de acceso y validez).
B.1.3	Definir procedimientos	Elaborar un procedimiento de actualización periódica del inventario. Elaborar un procedimiento de verificación de autorizaciones de acceso. Elaborar un procedimiento para nuevos archivos, definiendo responsable asignado y autorizaciones.
B.2	Acceso a los datos	
B.2.1	Gestionar los accesos	Elaborar un documento interno que defina los controles de acceso a cada archivo.
B.2.2	Asignar los permisos	Disponer de una notificación concreta y formal de las responsabilidades asumidas por cada responsable que acceda internamente a los archivos (notificación fehaciente).
B.2.3	Verificar la identificación y autorización	Disponer de un registro de acceso a los archivos.
B.2.4	Controlar el acceso físico	Disponer de un control de acceso físico a los armarios u otros elementos en los que se almacenen los archivos. Elaborar un procedimiento de control de acceso físico. Disponer de un registro de los accesos físicos (identificando día, hora, ingresantes y motivo). Asegurar el sistema de registro del control de acceso.
B.3	Copia o reproducción	

B.3.1	Controlar la copia o reproducción	la generación de copias o la reproducción de los documentos.
B.4	Traslado de documentación	
B.4.1	Controlar el traslado	Adoptar medidas de seguridad a fin de asegurar la confidencialidad e impedir la sustracción, pérdida, manipulación o acceso indebido de la información objeto de traslado.

DS

B.3.2	Asegurar la eliminación	Asegurar las medidas de Destrucción de la información (punto D) en la eliminación de las copias o reproducciones desechadas para evitar el 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.

DS

DS

C	CONSERVACIÓN DE LA INFORMACIÓN	
C.1	Control de 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 las condiciones de temperatura y humedad en el local de depósito.
C.2	Control de incendios e inundaciones	
C.2.1	Incendios e inundaciones	Disponer de 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.

DP

D	DESTRUCCIÓN DE LA INFORMACIÓN	
D.1	Asegurar la destrucción de la información	
		Establecer un procedimiento de destrucción de datos en donde se identifique:

D.1.1	Establecer modelo/formato de destrucción	tipo de información a destruir
		archivo que contiene la información
		responsable de la destrucción
		descripción del proceso y método de destrucción utilizado
D.1.2	Establecer mecanismos seguros de eliminación	Implementar un proceso de destrucción físico de la información que asegure la destrucción total de la información sin posibilidad de recuperación de la misma cumpliendo tres premisas:
		irreversibilidad
		seguridad
D.1.3	Designar responsable de destrucción	confidencialidad
		Establecer una persona autorizada para la destrucción y documentar su autorización.
D.1.4	Monitorear el proceso	Disponer de un inventario que identifique los archivos destruidos.

DS

D.1.5	Descarte de archivos	Implementar un 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.

DP

E	INCIDENTES DE SEGURIDAD	
E.1	Notificación ante incidentes de seguridad	
E.1.1	Establecer responsabilidades y procedimientos	Elaborar un procedimiento de gestión ante incidentes de seguridad.
		Establecer una persona responsable de la comunicación.
E.1.2	Elaborar informe	Elaborar un informe del incidente de seguridad que tenga de contenido mínimo:
		la naturaleza de la violación
		categoría de datos personales afectados
		identificación de usuarios afectados
		medidas adoptadas por el responsable para mitigar el incidente
		medidas aplicadas para evitar futuros incidentes
		Enviar notificación de incidente anexando
E.1.3	Enviar notificación	el informe a: Av. Pte. Gral. Julio A. Roca 710 - CABA - C1067ABP Correo electrónico: incidente.seguridad@aaip.gob.ar

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
DN: cn=GESTION DOCUMENTAL ELECTRONICA - GDE, o=AR, o=MINISTERIO DE MODERNIZACION,
ou=SECRETARIA DE MODERNIZACION ADMINISTRATIVA, serialNumber=CUIT 30715117564
Date: 2018.07.20 16:28:09 -0300

Eduardo Andrés Bertoni
Director
Agencia de Acceso a la Información Pública

[Volver](#)