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 Personale
s 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	Asegurar un control del responsable autorizado en 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

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
		confidencialidad
D.1.3	Designar responsable de destrucción	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, c=AR, o=MINISTERIO DE MODERNIZACION, ou=SECRETARIA DE MODERNIZACION ADMINISTRATIVA, serialNumber=CUIT 30715117564
Date: 2018.07.20 16:28:18 -03'00'

Eduardo Andrés Bertoni
Director
Agencia de Acceso a la Información Pública

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
DN: cn=GESTION DOCUMENTAL ELECTRONICA - GDE, c=AR, o=MINISTERIO DE MODERNIZACION, ou=SECRETARIA DE MODERNIZACION ADMINISTRATIVA, serialNumber=CUIT 30715117564
Date: 2018.07.20 16:28:19 -03'00'