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 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.
A.1.3	Asegurar la integridad	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 la confidencialidad durante el proceso de recolección	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 los 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 realizaran
		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	Considerar y analizar las posibles amenazas a la que estarán expuestos los sistemas informatizados.
		Disponer de un mapa conceptual que permita conocer el flujo de la información entre los distintos sistemas informatizados.
		Establecer un documento de seguridad que indique las medidas de seguridad adoptadas para los sistemas de información.
E.1.2	Asegurar una protección adecuada	Establecer controles de seguridad para las aplicaciones que procesen datos personales, entre ellas:
		Segmentación de roles y perfiles
		Autenticación segura
		Gestión de sesiones (cumpliendo apartado de Control de acceso (B))
		Gestión de mensajes de error en aplicaciones
		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.
		Segmentar en forma física o lógica la red de la entidad, separando las áreas públicas de las privadas.
		Separar los ambientes de Producción, QA, Prueba y Desarrollo.
		Implementar controles para la prevención de virus informáticos en los servidores que almacenen o gestionen datos personales.
		Implementar controles para la prevención de ataques en las estaciones de trabajo que gestionen datos personales.
		Implementar controles para la prevención de virus informáticos en las estaciones de trabajo que gestionen datos personales.
		Establecer y ejecutar un procedimiento de actualización periódica de software/hardware de todo el equipamiento.
		Definir a una persona responsable del cumplimiento de las medidas de seguridad.
		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.
		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.
E.1.4	Garantizar medidas eficaces y perdurables	Implementar periódicamente procesos de auditoria 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, c=AR, o=MINISTERIO DE MODERNIZACION, ou=SECRETARIA DE MODERNIZACION ADMINISTRATIVA, serialNumber=CUIT 30715117564
Date: 2018.07.20 16:28:09 -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 16:28:10 -03'00'