BIENESTAR
SECRETARÍA DE BIENESTAR

INAPAM
INSTITUTO NACIONAL DE LAS PERSONAS ADULTAS MAYORES

DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES EN EL INSTITUTO NACIONAL DE LAS PERSONAS ADULTAS MAYORES

México 2021 Año de la Independencia

GUÍA DE CONTENIDO

Datos de elaboración.

I. Introducción.

II. Marco jurídico.

III. El inventario de datos personales en las áreas del Instituto Nacional de las Personas Adultas Mayores.

IV. Las funciones y obligaciones de las personas que intervengan en el tratamiento datos personales.

V. El análisis de riesgos.

VI. El análisis de brecha.

VII. El plan de trabajo y medidas de seguridad.

VIII. Mecanismos de monitoreo y revisión de las medidas de seguridad.

Datos de elaboración.

DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES
FECHA DE ELABORACIÓN 11 de junio de 2021
ÁREA ENCARGADA DE LA ELABORACIÓN DEL DOCUMENTO Unidad de Transparencia del Instituto Nacional de las Personas Adultas Mayores
APROBACIÓN DEL DOCUMENTO Segunda Sesión Ordinaria del Comité de la Unidad de Transparencia de fecha 15 de junio de 2021 del Instituto Nacional de las Personas Adultas Mayores

I. Introducción.

El presente documento de seguridad constituye el instrumento que describe y da cuenta sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el Instituto Nacional de las Personas Adultas Mayores, para garantizar el cumplimiento de los principios y deberes establecidos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).

Asimismo, dicho documento será de observancia obligatoria para todos los servidores públicos que intervienen en el tratamiento de datos personales que se encuentren en posesión de esta Institución, así como para toda aquella persona física o moral, pública o privada, que debido a la prestación de un servicio tenga acceso a los datos personales de conformidad con lo establecido en la LGPDPPSO.

II. Marco jurídico.

- Constitución Política de los Estados Unidos Mexicanos. (CPEUM)
- Ley General de Transparencia y Acceso a la Información Pública. (LGTAIP)
- Ley Federal de Transparencia y Acceso a la Información Pública. (LFTAIP)
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. (LGPDPPSO)
- Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales).
- Estatuto Orgánico del Instituto Nacional de las Personas Adultas Mayores.

III. El inventario de datos personales en las áreas del Banco.

El Instituto Nacional de las Personas Adultas Mayores, en términos del Estatuto promueve el desarrollo humano integral de los Adultos Mayores, brindándoles empleo, ocupación, retribuciones, asistencia y las oportunidades necesarias para alcanzar niveles de bienestar y alta calidad de vida, buscando reducir las desigualdades extremas y las inequidades de género.

En ese sentido, con motivo de dichas funciones, la Institución es responsable del tratamiento de diversos datos personales, por lo que, con fundamento en lo dispuesto por los artículos 3 fracción XIV, 35, 83 y 84 fracciones I y II de la LGPDPPSO, así como en los artículos 55 a 64 de los Lineamientos Generales, esta Institución debe establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico para la protección de los mismos.

Los datos personales de acuerdo con la LGDPPSO son cualquier información relativa a una persona física, que la identifica o hace identificable, ahora bien, por la importancia que tienen para la seguridad individual, se destacandos categorías de datos personales

- **Datos sensibles:** Son datos personales que informan sobre los aspectos más íntimos de las personas, y cuyo mal uso pueda provocar discriminaciones o ponerles en grave riesgo, por ejemplo, el origen racial o étnico; estado de salud (pasado, presente y futuro); información genética; creencias religiosas, filosóficas y morales; afiliación sindical; opiniones políticas y preferencia sexual.

- **Datos patrimoniales o financieros:** Es la información sobre la capacidad económica de las personas físicas que hace referencia a los recursos que posee y a su capacidad para hacer frente a sus deudas, como pueden ser: dinero, bienes muebles e inmuebles; información fiscal; historial crediticio; ingresos y egresos; cuentas bancarias; seguros; afores; fianzas, número de tarjeta de crédito, número de seguridad, entre otros.

Así, se han identificado como datos personales objeto de tratamiento por parte de esta Institución los siguientes:

Datos personales de personal adscrito a esta Institución.	Nombre, domicilio, registro federal de contribuyentes (RFC), clave única del registro de población (CURP) edad, fecha de nacimiento, número de acta de nacimiento, teléfono particular, nacionalidad, número de empleado, cédula profesional, currículum vitae, número de seguridad social (NSS), clabe interbancaria para el pago de nómina, correo electrónico personal.
Datos personales de beneficiarios.	Nombre, fecha de nacimiento, domicilio, clave única del registro de población (CURP), grado de escolaridad, teléfono particular, correo electrónico personal, Licencia de manejo, Pasaporte, Credencial del IMSS, Credencial del ISSSTE, Cédula Profesional.
Datos personales con motivo de procedimientos administrativos.	Datos de cuentas bancarias de proveedores (personas físicas y morales), número de identificación oficial y/o número de pasaportes de los representantes legales, registro federal de contribuyentes (RFC), CURP, correos electrónicos y teléfonos de personas físicas, teléfono particular.

Datos personales sensibles de personal adscrito a esta Institución.	Género, nacionalidad, así como datos biométricos (huella dactilar)
Datos personales sensibles de beneficiarios y de procedimientos administrativos.	Género, nacionalidad, así como datos biométricos (huella dactilar)

I. Las funciones y obligaciones de las personas que intervengan en el tratamiento datos personales.

Es de precisar que el Instituto Nacional de las Personas Adultas Mayores, es el responsable sobre el tratamiento de los datos personales que se obtengan o utilicen con motivo de las facultades establecidas en su Estatuto Orgánico, y en ese sentido, todo el personal que por razón de sus funciones tenga acceso a los mismos debe atender al cumplimientode los principios y deberes establecidos en la LGDPPSO, mismos que consisten en los siguiente:

PRINCIPIOS Y DEBERES.

El derecho a la protección de los datos personales se sistematiza a través de ocho principios y dos deberes:

PRINCIPIOS	DEBERES
Licitud	Seguridad
Lealtad	Confidencialidad
Información	
Consentimiento	
Finalidad	
Proporcionalidad	
Calidad	
Responsabilidad	

PRINCIPIO DE LICITUD.

Este principio se encuentra previsto en el artículo 17 de la LGDPPSO y exige a los responsables que el tratamiento de los datos personales lo realicen observando lo que ordena la ley. De esta forma se busca que el tratamiento de datos personales no se efectúe de manera arbitraria sino de forma objetiva.

PRINCIPIO DE LEALTAD.

Con este principio se proscribe el tratamiento no ético de la información sobre las personas. El artículo 19 de la LGDPPSO ordena que el responsable no deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.

Así, la ley prohíbe al responsable recurrir a mecanismos ilegales o poco transparentes para recolectar y tratar los datos, los cuales deben utilizarse en la forma como se ha pactado o establecido.

PRINCIPIO DE INFORMACIÓN.

Con este principio se busca que el titular tenga conocimiento de los principales aspectos que regirán el tratamiento de sus datos personales. En este sentido, el artículo 26 de la LGDPPSO ordena al responsable informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

El aviso de privacidad constituye el mecanismo idóneo para informar al titular los aspectos indicados. **PRINCIPIO DE CONSENTIMIENTO.**

El artículo 3 de la LGDPPSO define el consentimiento como la manifestación de la voluntad libre, específica e informada del titular de los datos mediante el cual se habilita al responsable para efectuar el tratamiento de los mismos.

Asimismo, en el artículo 20 de la LGDPPSO se precisa que el consentimiento será

libre cuando no medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular; específico, cuando las finalidades sean concretas, lícita, explícitas y legítimas que justifiquen el tratamiento; e informado, cuando el titular tenga conocimiento del aviso de privacidad previo el tratamiento a que serán sometidos sus datos personales.

Adicionalmente la LGDPPSO establece que el consentimiento puede ser expreso o tácito, indicando que es tácito cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentidocontrario.

PRINCIPIO DE FINALIDAD.

Este principio se encuentra previsto en el artículo 18 de la LGDPPSO y busca que el tratamiento tenga como objetivo la realización de finalidades concretas, lícitas, explícitas y legítimas.

Así, quien trate datos no puede usarlos para cualquier propósito sino para aquellos establecidos en el aviso de privacidad, salvo que cuenten con atribuciones conferidas en la ley y medie el consentimiento del titular, situación en la cual excepcionalmente podrá tratar los datos para otras finalidades.

En suma, el principio de finalidad busca evitar que se recolecten datos para hacer con ellos lo que sea y delimita losusos que pueda darle el responsable.

PRINCIPIO DE PROPORCIONALIDAD.

En línea con lo anterior, el artículo 25 de la LGDPPSO ordena que sólo se pueden tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

En otras palabras, el tratamiento de datos personales sólo deberá circunscribirse a los que resulten adecuados, relevantes y no excesivos en relación con la finalidad del tratamiento. Por lo tanto, no está permitido recolectar o usar datos que no guarden estrecha relación con la finalidad del tratamiento.

PRINCIPIO DE CALIDAD.

El artículo 23 de la LGDPPSO exige que los datos personales sean veraces, exactos, completos, correctos y actualizados, teniendo el responsable la obligación de adoptar medidas para cerciorarse de lo anterior.

Ahora bien, este principio también se relaciona con la vigencia de los datos, pues existe la obligación de dejar de tratar información que ya no es necesaria para cumplir con las finalidades previstas en el aviso de privacidad.

En estos casos, los datos deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos. En ese sentido, la parte final del artículo 23 de la LGDPPSO señala que los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, y deberán atender a las disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales.

En suma, los datos personales no se deben tratar indefinidamente sino sólo por el período de tiempo necesario para cumplir la finalidad para la cual fueron recolectados.

PRINCIPIO DE RESPONSABILIDAD.

Los artículos 29 y 30 de la LGDPPSO ordenan que se adopten medidas que garanticen que los principios de la ley ysus demás disposiciones se cumplan en la práctica.

Se exige a los responsables y encargados del tratamiento de datos personales, el adoptar medidas apropiadas para cumplir sus obligaciones legales y estar en capacidad de evidenciar el correcto cumplimiento de sus deberes.

Con este principio se quiere que los mandamientos constitucionales y legales sobre tratamiento de datos personales sean una realidad verificable y redunden

en beneficio de la protección de los derechos de las personas.

DEBER DE SEGURIDAD.

Los titulares de los datos personales tienen derecho a que la información personal que proporcionen a los responsables se resguarde bajo medidas de seguridad adecuadas, que eviten su pérdida, alteración, destrucción, daño o uso, acceso o tratamiento no autorizado.

En ese sentido, los responsables estamos obligados a resguardar los datos personales en bases de datos protegidas con medidas de seguridad administrativas, físicas o técnicas.

- **Medidas administrativas:** Implementar controles que ayuden a evitar prácticas inadecuadas del personal que pongan en riesgo los datos personales, por ejemplo, evitar compartir contraseñas o dejar los expedientes al alcancede personas que no estén encargadas de su estudio o tramitación.

- **Medidas físicas**: Controles aplicados en los espacios físicos e infraestructura que minimicen el robo o acceso noautorizado, por ejemplo, mantener las áreas de trabajo, mobiliario y equipos debidamente cerrados con los controles y candados suficientes.

- **Medidas técnicas:** Controles para proteger equipos de cómputo y dispositivos de almacenamiento de virus, entre otros.

DEBER DE CONFIDENCIALIDAD.

De acuerdo con el artículo 42 de la LGDPPSO toda persona tiene derecho a que sus datos personales sean tratadoscon confidencialidad, es decir, a que éstos no se difundan o compartan con terceros, salvo que exista consentimiento para ello o alguna obligación normativa requiera su difusión.

Ahora bien, sólo bajo ciertas circunstancias está permitida la comunicación de datos personales con terceros, principalmente si el titular de los mismos ha otorgado su consentimiento, pero también cuando se presente alguno de los

siguientes supuestos:

- Cuando la transferencia esté prevista en una ley, convenios o Tratados Internacionales suscritos y ratificados por México;
- Cuando la transferencia se realice entre responsables del sector público, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;
- Cuando la transferencia se realice a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable del sector privado, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas;
- Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia;
- Cuando la transferencia sea necesaria para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última;
- Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados;
- Cuando la transferencia sea requerida para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular;
- Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero, o
- Cuando la transferencia sea necesaria por razones de seguridad nacional.
- En ese sentido, se solicita se considere lo anterior, y en el ámbito de su competencia, se dé cumplimiento a los principios y deberes que rigen la materia

de protección de datos personales, a efecto de garantizar y proteger derechos de terceros.

IV. El análisis de riesgos.

Debido a las circunstancias generales, tanto físicas como humanas, en las que las diversas unidades administrativas que integran el Instituto Nacional de las Personas Adultas Mayores tratan datos personales, se han identificado los siguientes posibles riesgos:

- Obtención de datos incompletos o incorrectos.
- Omitir la notificación al titular de los datos personales del aviso de privacidad.
- No difundir el aviso de privacidad.
- No tener un lugar seguro y de acceso restringido en donde se puedan archivar los datos personales en físico.
- Permitir a todo servidor público o personas ajenas a la dependencia, el acceso a los expedientes que contienen datos personales.
  - Daño de la base de datos que contenga información confidencial.
  - Fallas en los equipos de cómputo en donde se encuentran las bases de datos.
  - Falta de capacitación de los servidores públicos en relación a la confidencialidad que deben guardar sobre los datos personales que conozcan debido al desempeño de sus funciones.
  - Pérdida, robo o extravío de expedientes.
  - Alteración de la información.

Ahora bien, es necesario hacer un análisis en el que se identifiquen las posibles consecuencias que pueden generarse por no dar cumplimiento a los principios y

deberes establecidas en la LGDPPSO.

RIESGOS	POSIBLE CONSECUENCIA
Acceso de personas no autorizadas a los sistemas oplataformas oficiales.	Que personal no autorizado tenga acceso a la informacióny la divulgue, modifique o le dé un mal uso. Robo de información. Robo de identidad.
Falta de capacitación de los servidores públicosencargados del tratamiento de datos personales.	Pérdida de datos personales. Divulgación y transferencia indebida de los datospersonales. Actualización de supuestos de infracción previstos en lanormativa aplicable.
Daño o fallas en las bases de datos físicas o almacenadas en medios electromagnéticos.	Pérdida, destrucción y daño de los datos personales.
Falta de contraseñas altamente efectivas o de mecanismos para identificar o autenticar a los usuarios.	Pérdida, destrucción y daño de información. Divulgación y transferencia de datos personales. Modificaciones no autorizadas. Robo de información.
Mantenimiento insuficiente. Falla en equipos. Poca o absoluta renovación de equipos detelecomunicaciones o cómputos. Cambios de voltaje.	Pérdida, destrucción y daño de información.
Procesos carentes de formalidad para administración, acceso o cualquier tratamiento de	Pérdida, destrucción y daño de información. Divulgación y transferencia de datos

datos personales.	personales. Modificaciones no autorizadas. Robo de información.
Carencia de un servidor o sistema que almacene losdatos personales. La falta de registros, controles o bitácoras, para regular la entrada y salida de personal autorizado, al área donde se almacenan o archivan los datos personales.	Pérdida, destrucción y daño de información. Divulgación y transferencia de datos personales. Modificaciones no autorizadas

V. El análisis de brecha.

Una vez identificados los posibles riesgos a los que esta Institución se encuentra susceptible de enfrentar, podemosrealizar el análisis de brecha, utilizando como base las medidas de seguridad reportadas por las diversas unidades administrativas, las cuales consisten en lo siguiente:

- Quien recaba los datos personales, es un servidor público del área, asignado especialmente para recabar datos en general necesarios para cada trámite.

- El espacio físico o área donde se recaban datos personales, es dentro de las instalaciones.

- Cuando los datos personales son recabados de forma digital, se realiza por medio de plataformas oficiales o correo electrónico oficial.

- En la mayoría de las áreas, el acceso (al área donde se recibe a los ciudadanos y se recaban datos personales) setiene restringido, una vez que el dato se encuentra en posesión del servidor público, es decir si fue recabado frente a un escritorio, ventanilla, área abierta o pasillo, los ciudadanos no podrán pasar detrás de estos, ya que al terminar de recabar datos estos se colocan fuera del alcance de los ciudadanos.

- Las llaves que se tienen de cada área se encuentran en manos de servidores públicos, autorizados por cada área.

- Una vez recabados los datos personales, el servidor público genera un expediente para cada trámite o servicio, del cual se obtuvieron los datos personales, ya sea físico o electrónico.

- Una vez recabados los datos personales, ya realizada la carpeta o expediente (electrónica, física, en plataformas, o cualquiera generada) y guardada esta en archiveros o puesta en resguardo electrónico, tienen acceso a esta áreaservidores públicos del área.

- Una vez recabados los datos personales, en caso de que se les dé proceso electrónico, el servidor público guardalos mismos en carpeta electrónica, ya sea en su computadora, carpeta compartida, correo electrónico oficial o plataforma.

- Una vez concluido el trámite, los datos personales recabados se dejan intactos en la carpeta, archivo o expedientedel trámite al que pertenecen.

Ahora bien, a efecto de evitar la vulneración de los datos personales en posesión de esta Institución, se considera que además de las medidas existentes, se puede reforzar la seguridad de la información con la adopción de las siguientes prácticas:

➢ Control de acceso a la información, consistente en mantener un control sobre las personas que recaban, administran, usas, almacenan o difunden datos personales.

Dicho control puede realizarse a través de una bitácora en la que se señale el nombre y cargo del servidor públicoresponsable, el proceso de tratamiento de datos personales que realiza, así como las medidas de seguridad queadopta a efecto de resguardar la información.

➢ Activos del responsable, la cual se refiere a la asignación de responsabilidades y a la clasificación de la información. En ese sentido, se propone que las áreas realicen un estudio pormenorizado acerca de los procesosque se vinculen con tratamiento de información confidencial, los tramos de responsabilidad de cada

encargadode la información y se documenten mediante una bitácora.

- Seguridad física, en este apartado se sugiere tener más archiveros en buen estado y con seguridad para el resguardo de la información; en cuanto hace a la información que se resguarda de manera electrónica, se recomienda la actualización de los sistemas y el mantenimiento de los equipos.

- Incidentes de seguridad de información, en relación con este punto y derivado del diagnóstico realizado, no se ha presentado ninguna eventualidad en la cual se hayan vulnerados los datos personales que trata el Banco, no obstante, se recomienda generar programas de capacitación respecto a las acciones a realizar ante una posible incidencia y de los mecanismos de mitigación del daño.

VI. Plan de trabajo y medidas de seguridad.

A continuación, conforme a los elementos identificados en el análisis de brecha se sugiere implementar las siguientes medidas de seguridad y plan de trabajo.

a) Medidas de Seguridad.

Objetivo de control	Descripción de la medida de seguridad
Control de servidores públicos querecaban los datos personales.	Debe realizarse un listado de los servidores públicos que recaban datos personales, esto es, de los servidores públicos que tienen contacto con el titular de los datos personales por sus funciones. Actualización del listado: cada 6 meses.
	Forzosa asistencia a por lo menos un curso de capacitación en materia de datos personales.
	Remitir el documento de seguridad para el conocimiento y cumplimiento de las medidas de seguridad aplicables para un correcto tratamiento de datos personales.

Obtención de datos	Para evitar el riesgo de obtener datos personales incompletos o incorrectos, el servidor público autorizado para recabarlos, deberá pedir al ciudadano acredite su personalidad.
Aviso de privacidad	El servidor público que reciba los datos personales deberá tener a lavista de todos los ciudadanos el aviso de privacidad, y darlo a conocer al momento de la recepción del trámite.
	Si el trámite del cual se recabarán datos personales, cuenta con un formato, este deberá contener la mención del aviso de privacidad institucional ya sea simplificado o integral. Los formatos nuevos que se impriman posteriores a la emisión del presente documento deberán contar con la liga al aviso de privacidad oen su defecto el aviso de privacidad integral.
	Si el trámite del cual se recabarán datos personales, fue recabado mediante una plataforma electrónica oficial, esta plataforma deberá contener la mención y debe dar a conocer el aviso de privacidad integral.
Espacio físico.	Los datos personales recabados deberán ser recibidos únicamente en las instalaciones de cada área.
	El área específica donde se recaben los datos deberá contar con puertas que tengan llave, sin excepción alguna, para asegurar de forma efectivael resguardo adecuado de los datos personales, y así evitar mal uso de los mismos o vulneraciones.
	Las llaves de las puertas de cada dependencia, deberán ser guardadas únicamente por servidores públicos del área autorizados para tal efecto.
	Al término de las labores deberá cerrarse cada oficina de las áreas, paraevitar el contacto de otros servidores públicos o ciudadanos con los datos personales recabados.
	Al concluir la jornada laboral, se deberá guardar los expedientes para no dejarlos al alcance de ciudadanos

	o personal no autorizado.
Resguardo provisional, durante eldesahogo del trámite.	Una vez recabados los datos personales, al generar el expediente (derivado del trámite), este deberá ponerse en algún lugar que esté fuera del alcance de los ciudadanos, ya sea en una caja, archivero, o mueble.
Archivo, al finalizar el desahogo deltrámite.	Al finalizar el desahogo de los expedientes estos deberán archivarse enun lugar adecuado con las siguientes características: No estar al alcance de los ciudadanos o servidores públicos ajenos alárea. · Deberá ser un área específica para guardar los expedientes. · Este archivo debe estar bajo llave. La llave del mismo solo puede estar en manos de un servidor autorizadopara esto.
Acceso al archivo.	Se deberá crear por cada área, un control o bitácora de los servidores públicos que tienen acceso al archivo, el control debe contener losiguiente: Registro para anotar el nombre y puesto del servidor públicoautorizado. · Fecha, hora de entrada y hora de salida del archivo. · Registrar el expediente que se consultó. Registrar el expediente que se extrae del archivo, y fecha en la quese regresa el expediente. · Firma de conformidad del servidor público que entró. Firma de consentimiento del servidor público autorizado para llevar el control de este archivo.
Control de archivos electrónicos.	Cuando los datos personales sean recabados por medios electrónicos, se deberá generar expediente por cada trámite, dicho expediente deberá ser guardado en base de datos, correo electrónico oficial, o en plataforma autorizada, no en cualquier plataforma o correo electrónico

	personal.
	Para evitar riesgos, respecto a los expedientes electrónicos, se debe contar con un respaldo electrónico. Dicho respaldo deberá realizarse, como mínimo, de manera semestral.
Transferencia de datos personales.	En caso de que se requiera realizar alguna transferencia de datos en virtud de las funciones de las áreas responsables, se deberá informar al sujeto que reciba los datos el aviso de privacidad para que se sujete al mismo.
Versiones públicas.	En los casos en los cuales se realice la clasificación de información confidencial, que incluya datos personales, los documentos que contengan los datos deberán entregarse en versión pública.

b) **Plan de trabajo.**

Actividades	Temporalidad	Áreas involucradas	Actualización
Creación de políticas internas para el tratamiento de datos personales.	Anual.	Delimitación del personal que maneja datos personales en todas las direcciones.	En acontecimientos que se susciten y los lineamientos que se publiquen.
Revisión de los inventarios de datos personales	Anual.	Todas las direcciones.	Mensual.

Actualización, realización y monitoreo de la bitácora del manejo de datos personales.	Anual.	Comunicación directa con el responsable de la realización de la misma, en cada dirección.	Mensual.
Establecer comunicación directa con la Unidad de Transparencia en relación a cuestionamientos relativos a la protección de datos personales.	Siempre que sea necesaria.	Director de área, Enlace de transparencia, o cualquier persona que maneje datos personales.	Siempre que sea necesaria.
Seguimiento al plan de capacitación en relación a la protección de datos personales.	Según la temporalidad de las sesiones establecidas.	Personal que maneje datos personales.	Siempre que sea necesario.
Revisión periódica de las medidas de seguridad señaladas en el documento de seguridad.	Mensual.	Personal que maneje datos personales.	Mensual.
Formular el análisis y matriz de riesgos.	Anual.	Personal que maneje datos personales.	Mensual.

VII. Mecanismos de monitoreo y revisión de las medidas de seguridad.

Se debe realizar un monitoreo y revisión de la aplicación de las medidas de seguridad, para valorar las amenazas, vulnerabilidades, aplicación correcta o incorrecta, impacto y actualización.

Mecanismos de monitoreo	Objetivo del monitoreo
Se realizarán visitas a las áreas responsables del tratamiento de datos personales de manera semestral.	Verificar la aplicación, actualización e impacto de las medidas de seguridad aplicadas.
Pedir reportes a los responsables de cada área generadora de información o a los responsables del sistema de datos personales o a sus administradores sobre el manejo de datos personales conforme a las medidas de seguridad.	Monitorear avances, aplicación, eventualidades y novedades respecto a la aplicación de las medidas de seguridad.

VIII. Programa general de capacitación.

De acuerdo con lo establecido en el artículo 35 fracción VII de la LGPDPPSO, esta Institución debe realizar un programa de capacitación, y en ese sentido, se plantea generar un programa anual para desarrollar la cultura en seguridad de la información, conforme a los siguientes ejes:

a) Programas a corto plazo para la difusión en general de la protección de datos personales en la organización y su importancia en el entorno laboral.

b) Programas a mediano plazo que tienen por objetivo capacitar al personal de manera específica respecto a sus funciones y responsabilidad en el tratamiento y seguridad de los datos personales y;

c) Programa general a largo plazo que tiene por objetivo incluir la seguridad en el tratamiento de los datos personales dentro de la cultura de organización de la Institución.

Asimismo, el personal de enlace de cada área administrativa del Instituto Nacional de las Personas Adultas Mayores estará en capacitación constante por medio de cursos y/o talleres presenciales o en línea por parte del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Finalmente, conforme a lo establecido en la LGPDPPSO y en los Lineamientos Generales, el presente documento deberá actualizarse por lo menos una vez al año, en función de las medidas de seguridad adoptadas o de las nuevas circunstancias que se presenten en materia de seguridad y protección de datos personales.

REALIZÓ	AUTORIZÓ
Lic. Lucina Molina Herrera Secretaria Técnica de la Unidad de Transparencia	Lic. Edgar Olivares Agustín Presidente del Comité de la Unidad de Transparencia