CULTURA
SECRETARÍA DE CULTURA

INEHRM
Instituto Nacional de Estudios Históricos de las Revoluciones de México

POLÍTICA INTERNA DE GESTIÓN Y TRATAMIENTO DE LOS DATOS PERSONALES

DEL INSTITUTO NACIONAL DE ESTUDIOS HISTÓRICOS DE LAS REVOLUCIONES DE MÉXICO

UNIDAD DE TRANSPARENCIA

CULTURA

INEHRM

Índice

Dar cumplimiento a todos los principios, deberes, derechos y demás obligaciones en la materia, de conformidad con lo previsto en la Ley General y los Lineamientos Generales.

• Los roles y responsabilidades específicas de los involucrados internos y externos dentro de su organización, relacionados con los tratamientos de datos personales que se efectúen.

• Las sanciones en caso de incumplimiento;

• La identificación del ciclo de vida de los datos personales respecto de cada tratamiento que se efectúe; considerando la obtención, almacenamiento, uso, procesamiento, divulgación, retención, destrucción o cualquier otra operación realizada durante dicho ciclo en función de las finalidades para las que fueron recabados;

• El proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad; considerando el análisis de riesgo realizado previamente al tratamiento de los datos personales, y

• El proceso general de atención de los derechos ARCO.

I. MARCO JURÍDICO

- Constitución Política de los Estados Unidos Mexicanos.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley General de Transparencia y Acceso a la Información Pública.
- Ley Federal de Transparencia y Acceso a la Información Pública.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- Acuerdo mediante el cual se aprueban los Instrumentos Técnicos que refiere el Titulo Decimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- Demás leyes aplicables en materia de protección de datos personales.

II. DEFINICIONES

- **Instituto:** Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el cual es el organismo garante de la Federación en materia de protección de datos personales en posesión de los sujetos obligados.
- **Titular:** La persona física a quien corresponden los datos personales.
- **Derechos ARCO:** Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.
- **Tratamiento**: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

- **Datos personales:** Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

- **Datos personales sensibles:** Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

III. INTRODUCCIÓN

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el Sector Publico, son de aplicación y observancia directa para los sujetos obligados pertenecientes al orden federal.

De conformidad con el artículo 56 de los Lineamientos Generales de Protección de Datos Personales para el Sector Publico, el responsable deberá incluir en el diseño e implementación de las políticas internas para la gestión y el tratamiento de los datos personales, el cumplimiento de todos los principios, deberes, derechos y demás obligaciones en la materia.

Asimismo, en cumplimiento a lo dispuesto con el artículo 33, fracción I de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el responsable tiene el deber de establecer y mantener medidas de seguridad para la protección de los datos personales que reciba en ejercicio de sus facultades, para lo cual debe crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión.

IV. OBJETIVO

1. Establecer los principios generales que deberán observar los servidores públicos en el ejercicio de las funciones para el tratamiento de los datos personales, de conformidad con lo establecido en el artículo 7 de los Lineamientos Generales de Protección de Datos Personales para el Sector Publico.

2. Establecer las obligaciones y atribuciones que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados para el correcto cumplimiento en el tratamiento de los datos personales.

3. Fortalecer los conocimientos para la correcta observancia de los principios y deberes que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el Sector Publico.

4. Cumplir con las disposiciones que emanan de la Ley de la materia y demás normatividad aplicable, para garantizar el correcto tratamiento de los datos personales.

V. PRINCIPIOS GENERALES DE PROTECCIÓN DE DATOS PERSONALES

El artículo 7° de los Lineamientos Generales de Protección de Datos Personales para el Sector Publico, establece que en todo tratamiento de datos personales se deberá observar los principios rectores de la protección de datos personales:

a) Licitud.
b) Finalidad.
c) Lealtad.
d) Consentimiento.
e) Calidad.
f) Proporcionalidad.
g) Información.
h) Responsabilidad.

En observancia al correcto tratamiento de los datos personales en posesión de este Sujeto Obligado, la aplicación de los Principios Generales de Protección de Datos Personales, se formalizan como sigue:

a) Principio de **Licitud**.

Llevar a cabo el tratamiento de los datos personales de conformidad con las atribuciones o facultades que establecen las leyes en materia de protección de datos personales.

b) Principio de **Finalidad**.

i. Verificar que los tratamientos de datos personales que se realicen atiendan los fines específicos o determinados (finalidades concretas, licitas, explicitas y legitimas) y que sean acordes a las atribuciones o facultades de este Sujeto

Obligado.

ii. Verificar que las finalidades para el tratamiento de los datos personales estén relacionadas con las atribuciones normativas de este Instituto.

iii. Identificar las finalidades que no fueron informadas en los avisos de privacidad, verificando que estas se encuentren dentro de las atribuciones legales para el tratamiento de los datos personales y recabar el consentimiento del titular al momento de obtener sus datos personales.

c) Principio de **Lealtad.**

i. Garantizar que los datos personales recabados por este sujeto obligado, no se obtengan a través de medios engañosos o fraudulentos.

ii. Garantizar y supervisar que los tratamientos de datos personales que lleva a cabo el INEHRM, no den lugar a la discriminación, trato injusto o arbitrario en contra del titular.

d) Principio de **Consentimiento.**

i. Garantizar que previo a la obtención de los datos personales de los titulares y después de haberles puesto a disposición los avisos de privacidad, se cuente con su consentimiento (tácito o expreso) para el tratamiento de datos personales que lleva a cabo este Sujeto Obligado (salvo las causales de excepción señaladas en el artículo 22 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados).

ii. Verificar que el consentimiento que se obtenga de los titulares sea libre, específico e informado.

iii. Cuando los datos personales se recaben directamente del titular y se requiera el consentimiento, éste deberá solicitarse previo a la obtención de los datos personales y después de la puesta a disposición del aviso de privacidad.

iv. Cuando los datos personales se recaben indirectamente del titular y se requiera el consentimiento, no se podrán tratar los datos personales hasta que se cuente con la manifestación libre, específica e informada del titular, en la que autorice el tratamiento de sus datos personales de manera tácita o expresa según corresponda.

v. Atender las solicitudes de revocación del consentimiento, mismas que podrán ser representadas por el titular en cualquier momento del

tratamiento.

e) Principio de **Calidad.**

i. Adoptar las medidas necesarias, para mantener exactos, completos, correctos y actualizados los datos personales que son tratados por este Instituto.

ii. Establecer los plazos de conservación de los datos personales, de conformidad con los instrumentos de clasificación archivística.

iii. Establecer y documentar los procedimientos para la conservación y supresión de los datos personales que son tratados en el INEHRM.

f) Principio de **Proporcionalidad.**

i. Garantizar que los datos personales que se recaben sean los adecuados, relevantes y necesarios para la finalidad que justifica su tratamiento.

ii. Garantizar que los datos personales recabados contengan los datos mínimos necesarios en relación con las finalidades que justifican su tratamiento.

g) Principio de **Información.**

i. Poner a disposición del titular los avisos de privacidad que correspondan (Simplificados e Integrales), antes y después de la obtención de los datos personales.

ii. Implementar mecanismos para que el titular pueda manifestar su negativa para el tratamiento de datos personales para finalidades o transferencias que requieran su consentimiento.

iii. Difundir los avisos de privacidad por medios electrónicos y físicos.

iv. Ubicar los avisos de privacidad en lugares visibles que faciliten la consulta del titular.

v. Verificar que los avisos de privacidad integrales se encuentren de manera permanente en el portal de internet del INEHRM.

vi. Poner a disposición del titular los nuevos avisos de privacidad cuando se actualicen los siguientes supuestos.

a) Cambie la identidad de este Sujeto Obligado.

b) Se requiera recabar datos personales sensibles.

c) Cambien las finalidades señaladas en el aviso de privacidad.

d) Se modifiquen las condiciones de las transferencias de datos personales o se pretendan realizar transferencias no previstas inicialmente y el consentimiento del titular sea necesario.

h) Principio de **Responsabilidad.**

i. Elaborar políticas y programas de protección de datos personales, tomando en cuenta el desarrollo tecnológico y las técnicas existentes.

ii. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y deberes en materia de protección de datos personales.

iii. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.

iv. Establecer un sistema de supervisión y vigilancia interna y/o externa, para comprobar el cumplimiento de las políticas de protección de datos personales.

v. Cuando se requiera poner en práctica el procedimiento para atender dudas y quejas de los titulares.

vi. Garantizar que las políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología, que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la ley general de protección de datos personales en posesión de sujetos obligados.

vii. Implementar mecanismos para evidenciar el cumplimiento de los principios, deberes y obligaciones ante los Titulares y el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

VI. ROLES Y RESPONSABILIDADES

Con relación a lo dispuesto en el artículo 33, fracción II de la **LGPDPPSO**, el responsable deberá establecer y documentar los roles y responsabilidades, así como la

cadena de rendición de cuentas de todas las personas que traten datos personales en su organización, conforme al sistema de gestión implementado.

En el caso del INEHRM las funciones y obligaciones de las personas que tratan datos personales se han identificado el tratamiento por área:

a) Se realizan a través de los propios procesos que realiza cada área de conformidad con sus atribuciones, identificando el personal que realiza el tratamiento, el área al que está adscrito y la finalidad de dicho tratamiento.

En el Documento de Seguridad del INEHRM se tiene acceso a los roles y responsabilidades de las personas que realizan tratamientos de datos personales y las obligaciones inherentes a dicho tratamiento.

VII. SANCIONES

Las sanciones por incumplimiento en estas políticas serán las previstas por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la normatividad vigente en la materia.

DE CONFORMIDAD CON EL ARTÍCULO 163 DE LA LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS SERÁN CAUSAS DE SANCIÓN LAS SIGUIENTES:

*"**Artículo 163.** Serán causas de sanción por incumplimiento de las obligaciones establecidas en la materia de la presente Ley, las siguientes:*
I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO;
II. Incumplir los plazos de atención previstos en la presente Ley para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate;
III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;
IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la presente Ley;
V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la presente Ley, según sea el caso, y demás disposiciones que resulten aplicables en la materia;
VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos

personales;
VII. Incumplir el deber de confidencialidad establecido en el artículo 42 de la presente Ley;
VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la presente Ley;
IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la presente Ley;
X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la presente Ley;
XI. Obstruir los actos de verificación de la autoridad;
XII. Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la presente Ley;
XIII. No acatar las resoluciones emitidas por el Instituto y los Organismos garantes, y
XIV. Omitir la entrega del informe anual y demás informes a que se refiere el artículo 44, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, o bien, entregar el mismo de manera extemporánea."

VIII. CICLO DE LA VIDA

La Identificación del Ciclo de Vida de los Datos Personales respecto de cada tratamiento que se efectúe; considerando la obtención, almacenamiento, uso, procesamiento, divulgación, retención, destrucción o cualquier otra operación realizada durante dicho ciclo en función de las finalidades para las que fueron recabados.

OBTENCIÓN
(licitud, información, consentimiento, proporcionalidad, seguridad, confidencialidad)

USO
registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia, disposición. (calidad, finalidad, lealtad, seguridad, confidencialidad)

ELIMINACIÓN
(calidad, seguridad)

IX. PROCESO GENERAL PARA EL ESTABLECIMIENTO, ACTUALIZACIÓN, MONITOREO Y REVISIÓN DE LOS MECANISMOS Y MEDIDAS DE SEGURIDAD

El artículo 33, fracción VII de la **LGPDPPSO** establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, el monitoreo y revisión de manera periódica de las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

De acuerdo con la fracción VI del artículo 35 de la **LGPDPPSO**, los mecanismos de monitoreo y revisión forman parte del documento de seguridad. sí, respecto a los mecanismos de monitoreo y revisión de las medidas de seguridad, el artículo 63 de los Lineamientos Generales señala lo siguiente:

> *"**Monitoreo y supervisión periódica de las medidas de seguridad implementadas***
>
> ***Artículo 63.** Con relación al artículo 33, fracción VII de la Ley General, el responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua.*
> *Para cumplir con lo dispuesto en el párrafo anterior del presente artículo, el responsable deberá monitorear continuamente lo siguiente:*
>
> *I. Los nuevos activos que se incluyan en la gestión de riesgos;*
> *II. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;*
> *III. Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;*
> *IV. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;*
> *V. Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;*
> *VI. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y*
> *VII. Los incidentes y vulneraciones de seguridad ocurridas.*
>
> *Aunado a lo previsto en las fracciones anteriores del presente artículo, el responsable deberá contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión."*

De lo anterior es posible identificar que el monitoreo y revisión de las medidas de seguridad tiene el objetivo de fortalecer, a través de un ciclo de mejora continua, la protección de los datos personales que resguarda este Instituto.

A continuación, se desarrollan las acciones de monitoreo y supervisión periódica para las medidas de seguridad del INEHRM:

- Mecanismos de Monitoreo

Para los tratamientos de datos personales del INEHRM, considera los siguientes tipos de monitoreo:

1. **Revisión de cumplimiento de las políticas internas del INEHRM, relacionadas con el tratamiento de datos personales.**

   Tiene el objetivo de asegurar que las personas servidoras públicas realicen los tratamientos de datos personales en concordancia con lo dispuesto en la **LGPDPPSO**, los Lineamientos Generales, y demás normatividad que resulte aplicable.

   Para ello, cuando se identifica algún cambio en los instrumentos antes mencionados, se deberán realizar las siguientes actividades:

   a) Revisar y, en su caso, actualizar los procesos involucrados en el tratamiento de datos personales.

   b) Revisar y, en su caso, actualizar los avisos de privacidad, las funciones y obligaciones del personal y los inventarios de datos personales, según corresponda.

   c) Evaluar si hubo cambios en las amenazas, vulnerabilidades o impacto de los riesgos relacionados con las modificaciones a la normativa, para actualizar los análisis de riesgos, análisis de brecha y plan de trabajo.

   d) Revisar y, en su caso, adecuar los sistemas de tratamiento para cumplir con los cambios normativos.

2. **Revisión del riesgo.** Tiene el objetivo de identificar modificaciones a los riesgos identificados en los tratamientos de datos personales, para ello, se implementarán los siguientes monitoreos:

   a) Monitoreo del entorno físico
   Para la detección continua de amenazas y vulnerabilidades en el entorno

físico, se cuenta con:

(i) Personal de vigilancia en los accesos a ambas sedes del Instituto.
(ii) Oficinas con llave para almacenar expedientes que contienen datos personales.

b) Monitoreo del entorno electrónico
Para la detección continua de amenazas y vulnerabilidades, la Dirección de Tecnologías de la Información de la Secretaría de Cultura, implementa controles dentro de su infraestructura, misma que provee de los recursos de seguridad para nuestros portales institucionales, asimismo la Subdirección de Tecnologías de la información del INEHRM implementa a nivel usuario accesos seguros a los equipos mediante contraseña, actualización de antivirus, antimalware y firewall de sistema, así como la utilización de filtros antispam en los correos institucionales

c) Actualización del plan de trabajo
Derivado del monitoreo del entorno físico o electrónico, se pueden realizar actualizaciones en el plan de trabajo en caso de que se identifiquen cambios en las amenazas, las vulnerabilidades o el impacto de los riesgos identificados.

d) Vulneraciones a la seguridad de los datos personales
En caso de identificar un incidente de seguridad que involucre datos personales, las áreas notificaran a la Subdirección de Tecnologías de la información del INEHRM y a la Unidad de Transparencia con el fin de brindar apoyo para solventar incidentes y según el caso de notificar a la Dirección de Tecnologías de la Información de la Secretaría de Cultura, para realizar las acciones que consideren necesarias ante eventualidades por infraestructura.

- Mecanismos de supervisión o revisión

La Subdirección de Tecnologías de la información del INEHRM verifica la vigencia y actualización de los mecanismos de seguridad en los equipos por usuario y a nivel infraestructura de los sistemas es la Dirección de Tecnologías de la Información de la Secretaría de Cultura quien implementa los medios de verificación que garanticen la seguridad y continuidad de los servicios.

X. Proceso General de Atención de los Derechos Arco

1. EJERCICIOS DE LOS DERECHOS ARCO

La solicitud podrá ser presentada por escrito libre, verbalmente en la Unidad de

Trasparencia, quien proporcionará los formatos correspondientes o a través de los siguientes medios electrónicos:

- Plataforma Nacional de Transparencia (PNT) en la dirección electrónica: https://www.plataformadetransparencia.org.mx señalando como sujeto obligado al Instituto Nacional de Estudios Históricos de las Revoluciones de México.

- Enviando un correo electrónico a la cuenta: unidadenlaceinehrm@cultura.gob.mx

Cuando la solicitud se presente a través de la PNT, se asignará automáticamente un número de folio con el que la persona solicitante podrá dar seguimiento a su requerimiento.

Si la solicitud se presenta por otro medio, la UT registrará la solicitud en la PNT y enviará el acuse de recibo a la persona solicitante. El acuse deberá tener la fecha de recepción, el folio correspondiente y los plazos de respuesta aplicables.

De conformidad con los artículos 52 de la LGPDPPSO y 83 de los Lineamientos Generales, las solicitudes de derecho ARCO deben incluir:

- Nombre y domicilio o cualquier otro medio para recibir notificaciones.
- Los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante.
- De ser posible, el área responsable que trata los datos personales y ante el cual se presenta la solicitud. · La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCO, salvo que se trate del derecho de acceso.
- La descripción del derecho ARCO que se pretende ejercer, o bien, lo que solicita el titular.
- Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso.

Cuando la solicitud se presente a través de un representante, será necesario demostrar que está autorizado para presentar la solicitud a nombre del titular.

Si a la solicitud le falta uno o más requisitos, la Unidad de Transparencia, en un plazo de máximo 5 días hábiles siguientes a la recepción de la solicitud, le hará, por una sola vez, un requerimiento al solicitante. Éste tendrá 10 días hábiles para atender el requerimiento.

De no atender la prevención se tendrá por no presentada la solicitud de derechos ARCO, conservando su derecho a presentarla nuevamente.

Si el ejercicio de derechos ARCO requiere de un trámite específico, la Unidad de Transparencia cuenta con 5 días hábiles contados a partir del día siguiente de la recepción de la solicitud para hacerle saber al solicitante para que decida si ejerce sus derechos a través del trámite específico o por medio del procedimiento establecido por el INEHRM.

Si se determina la incompetencia del INEHRM para responder la solicitud, la Unidad de Transparencia tiene 3 días hábiles, después de haber recibido la solicitud, para notificar a la persona solicitante y, de ser posible, señalará el sujeto obligado competente para atender su solicitud.

Si la solicitud se trata de un derecho diferente a los derechos ARCO, la Unidad de Transparencia contará con 3 días hábiles para reconducir la vía, haciéndolo del conocimiento del titular.

Una vez ingresada la solicitud, la Unidad de Transparencia tiene 20 días hábiles contados a partir del día siguiente de la fecha de recepción para dar trámite y respuesta a la misma.

La Unidad de Transparencia deberá turnar la solicitud a las áreas administrativas correspondientes para que realicen las gestiones necesarias para hacer efectivo el ejercicio de los derechos ARCO.

La unidad administrativa deberá informar a la Unidad de Transparencia, dentro de los 2 días hábiles siguientes a la notificación de la solicitud, si requiere información adicional para que la Unidad de Transparencia realice el requerimiento correspondiente y la persona solicitante contará con 10 días hábiles para atender el requerimiento.

De no atender el requerimiento, se tendrá por no presentada la solicitud de derechos ARCO, conservando el derecho a presentarla nuevamente.

Si la solicitud es improcedente, la Unidad de Transparencia deberá notificarlo al solicitante en un plazo no mayor a 5 días hábiles a partir de la presentación. En su respuesta indicará las causales de improcedencia, con fundamento en el artículo 55 de la LGPDPPSO, y deberá anexar la resolución del Comité de Transparencia donde confirma la improcedencia.

Si necesita más tiempo para atender la solicitud, la Unidad de Transparencia deberá notificar al solicitante dentro de los 8 días hábiles siguientes a su presentación la ampliación del plazo, acompañada de la resolución del Comité de Transparencia donde confirma la ampliación del plazo. Ésta se hará por 10 días hábiles adicionales, por una sola ocasión, siempre y cuando esté debidamente justificada.

En caso de resultar procedente la solicitud, la unidad administrativa deberá remitir

la información completa a la Unidad de Transparencia, a más tardar 8 días hábiles siguientes a la notificación. A su vez, la Unidad de Transparencia deberá notificar a la persona solicitante y el INEHRM contará con máximo 15 días hábiles siguientes a la notificación para hacerlo efectivo.

2. MECANISMOS ESTABLECIDOS POR LA UNIDAD DE TRANSPARENCIA SOLICITUDES DE DERECHOS ARCO DENTRO DEL INEHRM

El Instituto de Estudios Históricos de las Revoluciones de México comprometido con dar respuesta de manera eficiente a las solicitudes de derechos ARCO, de conformidad a lo establecido en la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, hace del conocimiento los siguientes mecanismos establecidos por su Unidad de Transparencia, señalándolos a continuación:

Una vez realizada la solicitud de ejercicio del derecho de acceso, rectificación, cancelación u oposición de datos personales ante la Unidad de Transparencia del INEHRM, con la finalidad de que el Instituto se encuentre en posibilidades de realizar la entrega de la respuesta respectiva, es necesaria la acreditación de la identidad de la persona titular de los datos personales; de modo que una vez fijada la modalidad y en su caso, realizado el pago de reproducción respectivo, su recepción deberá realizarse previa muestra de su identificación oficial legible, íntegra (ambos lados) y vigente, a través, de cualquiera de las opciones siguientes:

1. Deberá ingresar al portal electrónico de la PNT https://www.plataformadetransparencia.org.mx/ habilitando un usuario personal con un correo electrónico.

2. Mediante cita, en la Unidad de Transparencia del INEHRM, con domicilio en Barranca del Muerto número 275 Planta Baja, Colonia San José Insurgentes, Alcaldía Benito Juárez, Ciudad de México, código postal 03900; de lunes a viernes 09:00 a 15:00 y de 16:00 a 18:00 horas.

Ambas opciones podrán ser realizadas de igual modo a través de una persona representante de la persona titular de los datos personales, quien deberá acreditar su identidad y su representación correspondiente.