# Políticas Internas de Gestión y Tratamiento de Datos Personales de Nacional Financiera S.N.C. I.B.D.

**POLÍTICAS INTERNAS DE GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES DE NACIONAL FINANCIERA S.N.C. I.B.D.**

## INTRODUCCIÓN

El artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, reconoce el derecho humano a la autodeterminación informativa, esta prerrogativa faculta a su titular a decidir de manera libre e informada, sobre el uso de datos personales, pues a través de ellos es posible identificarlo.

Así entonces, ya que se trata de un derecho humano, su protección es relevante para cualquier organización en la que el tratamiento de datos personales sea necesario para el desarrollo su actividad sustantiva, pues un mal uso de la misma podría poner en riesgo la vida, la seguridad y la reputación de las personas físicas que la integran, así como de las personas relacionadas a ella.

Los riesgos inherentes al tratamiento de datos personales, deben reducirse a través de acciones tendientes a generar un entorno seguro para el manejo de esa información, en este sentido y de acuerdo con lo establecido en el artículo 31 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), Nacional Financiera S.N.C. I.B.D., en su carácter de Sujeto Obligado de dicho ordenamiento, tiene la obligación de establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico que aseguren la protección de los datos personales que trata, garantizando su confidencialidad, integridad y disponibilidad.

Este deber de seguridad implica la elaboración de reglas, procedimientos y controles que permitan la seguridad efectiva de los datos personales que se encuentran en posesión de NAFIN; así entonces y de conformidad con lo establecido en el artículo 33, fracción I de la LGPDPPSO una de las actividades que los responsables deberán desarrollar es la elaboración de políticas internas para la gestión y tratamiento de los datos personales,

las cuales consideren el contexto en el que ocurre el tratamiento de los datos al interior de la Institución y el ciclo de vida de los mismos.

Según lo establecido en el artículo 56 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, dichas políticas deberán contener al menos lo siguiente:

> ***I. El cumplimiento de todos los principios, deberes, derechos y demás obligaciones en la materia, de conformidad con lo previsto en la Ley General y los presentes Lineamientos generales;***
>
> ***II. 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;***
>
> ***III. Las sanciones en caso de incumplimiento;***
>
> ***IV. 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;***
>
> ***V. 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***
>
> ***VI. El proceso general de atención de los derechos ARCO.***

Es en cumplimiento de las obligaciones previamente indicadas, que se emiten las presentes Políticas Internas de Tratamiento y Gestión de Datos Personales; donde este instrumento buscará establecer las bases en las que se desarrolle el tratamiento de la información personal al interior de la organización, para lograr que el mismo sea legítimo y controlado.

## OBJETO.

Establecer reglas de carácter general respecto la gestión y tratamiento de los datos personales que se encuentran en posesión de Nacional Financiera S.N.C., con la finalidad de asegurar la seguridad y la confidencialidad de la información.

## ÁMBITO DE APLICACIÓN.

Las presente políticas están dirigidas a todos los servidores públicos de Nacional Financiera S.N.C. en cuyos procesos realicen el tratamiento de datos personales.

## CUMPLIMIENTO DE LOS PRINCIPIOS DE LA LGPDPPSO.

Tal como se establece en el Programa de Protección de Datos Personales de Nacional Financiera S.N.C. I.B.D., en cumplimiento a los principios **licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad** en el tratamiento de datos personales, los servidores públicos que integran este Sujeto Obligado deberán observar las siguientes directrices:

1. Las áreas administrativas de NAFIN deberán tratar los datos personales que sean necesarios para el desarrollo de sus actividades, siempre de acuerdo con el marco normativo que regula las mismas.

2. Las áreas administrativas de NAFIN, deberán identificar las finalidades que motivan el tratamiento de los datos personales que posean.

3. Las finalidades que motiven el tratamiento de los datos personales en posesión de las áreas administrativas deberán ser concretas y claras, apegadas a las funciones que desarrolla el área administrativa de que se trate y de acuerdo con el marco normativo aplicable.

**4.** Las áreas administrativas de NAFIN no deberán obtener o tratar datos personales a través de medios engañosos o fraudulentos.

**5.** Las áreas administrativas solo podrán tratar los datos personales que sean adecuados, relevantes y necesarios para cumplir con las finalidades que implique el proceso interno de que se trate.

**6.** Cuando el tratamiento de los datos personales **no** se ubique dentro de alguno de los siguientes casos, será necesario requerir del titular su consentimiento expreso, es decir, que el mismo se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología.

**a)** Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en esta Ley, en ningún caso, podrán contravenirla.
**b)** Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente.
**c)** Para el reconocimiento o defensa de derechos del titular ante autoridad competente.
**d)** Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable.
**e)** Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes.
**f)** Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria.
**g)** Cuando los datos personales figuren en fuentes de acceso público.
**h)** Cuando los datos personales se sometan a un procedimiento previo de disociación.
**i)** Cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia.

**7.** Las áreas administrativas de NAFIN deberán procurar que, en la obtención de los datos personales, los servidores públicos involucrados obtengan la evidencia necesaria para asegurar que los mismos son exactos, correctos y se encuentran actualizados.

**8.** Las áreas administrativas de NAFIN, previo a la obtención de los datos personales que deban tratar, tienen la obligación de informar a los titulares sobre la existencia y características principales del tratamiento; para ello deberán hacer del conocimiento de los titulares de los datos personales el aviso de privacidad correspondiente.

**9.** Cuando las áreas administrativas de NAFIN tengan noticia de que los datos personales que tratan han sido actualizados, deberán modificar las bases de datos en las que estos consten, a efecto de que se encuentren actualizados.

**10.** En la conservación de los datos personales, las áreas administrativas de NAFIN, no deberán exceder los plazos que son necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, para ello, deberán considerar las disposiciones aplicables, así como los aspectos administrativos, contables, fiscales, jurídicos e históricos.

**11.** Cuando los datos personales ya no sean necesarios para el cumplimiento de las finalidades informadas a los titulares y el plazo de conservación de los mismos haya concluido, las áreas administrativas de NAFIN deberán suprimir los datos, previo bloqueo de los mismos.

## RESPONSABILIDADES EN EL TRATAMIENTO DE DATOS PERSONALES.

En el desarrollo de sus actividades, las áreas administrativas de NAFIN deberán observar las siguientes reglas, ello, con el propósito de generar un ambiente seguro en el tratamiento de los datos personales, independientemente de la fase del ciclo de vida en el cual se encuentren.


## DISPOSICIONES PARA LA OBTENCIÓN DE DATOS PERSONALES.

1. Las áreas administrativas deberán obtener los datos personales de fuentes autorizadas o de transferencias que cumplan con los requisitos indicados en la normatividad aplicable, evitando el uso de medios fraudulentos o engañosos y cuidando la expectativa razonable de privacidad.

2. Las áreas administrativas de NAFIN deberán garantizar que los datos personales recabados son indispensables y no excesivos para el cumplimiento de las finalidades del tratamiento.

3. Las áreas administrativas que recaben datos personales, deberán poner a disposición de los titulares el aviso de privacidad simplificado, lo cual no exime de poner a su disposición el aviso de privacidad integral.

4. Será obligación de las áreas administrativas de NAFIN publicar en el APARTADO DE PROTECCIÓN DE DATOS PERSONALES de la página institucional, el aviso de privacidad simplificado y el aviso de privacidad integral de cada uno de los procesos en los que recaben datos personales.

5. Los servidores públicos que sean responsables de la información que consta en los avisos de privacidad, deberán actualizar los mismos cuando exista un cambio en la información respecto de las finalidades, los datos personales a recabar, los fundamentos legales que soportan la obtención de la información o respecto de las transferencias que se deban realizar.

6. En caso de que para el tratamiento o la transferencia de los datos personales se requiera del consentimiento expreso del titular, este deberá constar por escrito.

## DISPOSICIONES PARA EL ALMACENAMIENTO DE DATOS PERSONALES.

1. Las áreas administrativas de NAFIN deberán archivar los datos personales de conformidad con los instrumentos de control y consulta archivística de la Institución.

2. Respecto del plazo de conservación de los datos personales, las áreas administrativas deberán atender a lo dispuesto en el catálogo de disposición documental de la Institución.

3. El plazo de conservación de los datos personales no deberá exceder de los términos señalados en la normatividad aplicable.

4. Las áreas administrativas deberán integrar los datos personales que obtengan, de acuerdo con los expedientes que su actividad sustantiva genere.

5. Las áreas administrativas deberán identificar el tipo de soporte en el que se almacenarán los datos personales, es decir, si se tratará de un expediente físico o un expediente electrónico, con el propósito de mantener un control sobre los mismos.

6. En el caso de soportes físicos, las áreas administrativas de la Institución deberán asegurarse que los mismos se resguarden en lugares que garanticen su conservación e integridad.

7. En el caso de soportes electrónicos, las áreas administrativas deberán asegurarse de que su acceso se limite al personal que se encuentre facultado para su tratamiento.

8. Respecto de los soportes electrónicos, en todo momento se deberá proteger la información personal a través de contraseñas.

9. En el caso de soportes físicos que contengan datos personales, las áreas administrativas deberán llevar un control sobre las personas que acceden a los espacios en los que los, mismos se reguardan.

10. Los servidores públicos procurarán no dejar a la vista aquella documentación que contenga algún tipo de dato personal.

## DISPOSICIONES PARA EL USO DE DATOS PERSONALES.

1. Las áreas administrativas deberán limitar el tratamiento de datos personales a las facultades y atribuciones que la normatividad aplicable les confiera.

2. Los servidores públicos deberán usar los datos personales de acuerdo con las finalidades expresadas en el aviso de privacidad entregado a su titular.

3. El acceso a los datos de autenticación tales como contraseñas, información biométrica, firma autógrafa y electrónica se deberá restringir a aquellos servidores públicos que tengan los permisos otorgados por las áreas administrativas encargadas de la administración de las bases de datos en las que consten dichos datos.

4. El acceso y uso de bases de datos y archivos en los que consten datos personales, deberá estar documentado a través de los manuales internos en los que se describan los procesos en los que ocurre el tratamiento de dicha información.

5. Respecto del acceso y uso de datos personales sensibles, las áreas administrativas encargadas de su tratamiento deberán establecer altos controles de seguridad.

6. En la comunicación interna que desarrollen las áreas administrativas en la ejecución de sus funciones, deberán cumplir con las medidas de seguridad que estén dirigidas a conservar la confidencialidad de la información.

7. Las áreas administrativas deberán asegurarse de que el tratamiento de datos personales no dará lugar a una situación de discriminación, trato injusto o arbitrario en contra del titular.

8. Las áreas administrativas deberán publicar aquellos datos personales que son requeridos en cumplimiento a las obligaciones de transparencia señaladas en los 70 y 77 de la Ley General de Transparencia y Acceso a la Información Pública y en los Lineamientos Técnicos Generales para la publicación, homologación y estandarización de la información de las obligaciones establecidas en el Título Quinto y en la fracción IV del artículo 31 de la Ley General de Transparencia y Acceso a la Información Pública, que deben de difundir los sujetos obligados en los portales de Internet y en la Plataforma Nacional de Transparencia.

9. Salvo aquellos datos personales que deban ser publicados de conformidad con los preceptos citados en el numeral inmediato anterior, las áreas administrativas deberán proteger la información de las personas físicas de acuerdo con las disposiciones de la Ley General de Transparencia y Acceso a la Información Pública y a la Ley Federal de Transparencia y Acceso a la Información.

10. Cuando exista la remisión de datos personales, las áreas administrativas deberán garantizar el cumplimiento de las obligaciones establecidas en la Ley por parte del encargado de la información.

## DISPOSICIONES PARA EL BLOQUEO DE DATOS PERSONALES.

1. Las áreas administrativas deberán llevar a cabo el bloqueo de los datos personales, cuando las finalidades para las cuales fueron recabados concluyeron.

2. Durante el periodo de bloqueo, las áreas administrativas deberán evitar el uso de los datos personales.

## DISPOSICIONES PARA LA SUPRESIÓN DE DATOS PERSONALES.

1. Las áreas responsables de los datos personales, previo a la supresión deberán realizar el bloqueo de los mismos.

2. En la supresión de los datos personales, las áreas administrativas deberán priorizar los métodos de borrado seguro tales como la trituración y la incineración en el caso de soportes físicos y la desmagnetización y sobreescritura en el caso de los medios electrónicos.

3. En la destrucción de los soportes que contengan datos personales se deberá garantizar que la recuperación de la información no sea posible, que los soportes conserven su seguridad y confidencialidad y que el método seleccionado para la eliminación de la información sea favorable con el medio ambiente.

4. En el caso de que la supresión de los datos personales sea consecuencia del ejercicio del derecho de cancelación por parte del titular, será necesario que se notifique la evidencia de que la cancelación se ha realizado.

## SANCIONES

En caso de incumplimiento a lo dispuesto en las presentes políticas, el Comité de Transparencia, como autoridad máxima en la materia, podrá requerir a las áreas administrativas responsables para que den cumplimiento a lo señalado en este instrumento, otorgándoles en su caso, un plazo para demostrar que han realizado las acciones necesarias para la atención de estas disposiciones.

En caso de que el área administrativa no atienda las observaciones del Comité, este podrá dar vista al Órgano Interno de Control Especifico en NAFIN a efecto de que pueda iniciar el proceso correspondiente.

## ESTABLECIMIENTO, ACTUALIZACIÓN, MONITOREO Y REVISIÓN DE LOS MECANISMOS Y MEDIDAS DE SEGURIDAD.

En virtud de lo establecido en el artículo 31 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, NAFIN tiene la obligación de establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico a través de las cuales se logre la protección de los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Es por virtud de este deber, y en cumplimiento a la obligación establecida en el artículo 35 del ordenamiento previamente citado, que, para el establecimiento de las medidas de seguridad concernientes a los datos personales se deberá atender al análisis de riesgo y brecha que constan en el Documento de Seguridad de la Institución.

Así entonces, será a través de la constante actualización de ambos análisis y del cumplimiento al Plan de Trabajo que se desarrolle como consecuencia de los mismos, la Institución deberá fijar las medidas de seguridad, las cuales deberán ser monitoreadas y revisadas a través de auditorías y/o revisiones administrativas que garanticen la seguridad de la información y reduzcan el riesgo a las vulneraciones que podría sufrir ante cualquier amenaza.

# SOLICITUD PARA EL EJERCICIO DE LOS DERECHOS ARCO

NAFIN tiene **20 días** para notificar la respuesta, contados a partir del día siguiente al que se recibió la solicitud.

**Trámite o procedimiento especifico,** se tienen 5 días para notificar al solicitante

**Incompetencia,** se tienen 3 días para notificar al solicitante

**¿La solicitud cumple con los requisitos?**

Si

No

Se **turna** a las áreas responsables

Las áreas entregan **respuesta** a la Unidad de Transparencia para su notificación al solicitante.

Las áreas de la institución pueden solicitar **prórroga** de 10 días cuando sea necesario justificando las circunstancias

**Procedencia**

**Inexistencia**

Unidad de Transparencia **pone a disposición del solicitante la respuesta** previa acreditación

Se somete a confirmación de **Comité de Transparencia**

El solicitante podrá **inconformarse por la respuesta** entregada, e interponer recurso de

Unidad de Transparencia pone a disposición del solicitante la **resolución del Comité de Transparencia** previa acreditación para su entrega.

Se tienen 5 días para realizar la **Prevención** al solicitante

Solicitante cuenta con **10 días** para subsanar

En caso de que **SÍ subsane, se interrumpe** el plazo para la atención de la solicitud y se reinicia el proceso de atención

En caso de **NO subsane,** se tiene por no presentada la solicitud.