ACTA DE LA TERCERA REUNIÓN EXTRAORDINARIA 2024, DEL COMITÉ DE TRANSPARENCIA DEL CENTRO DE INVESTIGACIÓN EN ALIMENTACIÓN Y DESARROLLO, A.C. (CIAD).

En la ciudad de Hermosillo, Sonora, siendo las 10:00 horas del día 31 de mayo de 2024, se reunieron a través de videoconferencia con el propósito de celebrar la tercera reunión extraordinaria 2024 del Comité de Transparencia, en cumplimiento a los artículos 64 y 65 fracción segunda de la Ley Federal de Transparencia y Acceso a la Información Pública, con la asistencia de los siguientes integrantes: Mtra. María Guadalupe Sánchez Soto, Titular de la Unidad de Transparencia y Presidenta del Comité, Dr. Rogerio Rafael Sotelo Mundo, Coordinador de Investigación y el Lic. Alejandro Salinas Ochoa, Titular del Órgano Interno de Control; Así mismo, se hace constar la presencia de la Lic. María del Carmen Castro Cárdenas, Jefa del Departamento de Sistemas Administrativos de éste Centro, invitada en términos del segundo párrafo del artículo 64 de la Ley Federal de Transparencia y Acceso a la Información Pública, todos los antes mencionados del Centro de Investigación en Alimentación y Desarrollo, A.C.

1. Lista de Asistencia.

La Presidenta tomó lista de asistencia verificando que existía quórum para efectuar la reunión.

2. Autorización del Orden del Día.

La Presidenta procedió a dar lectura al orden del día para esta reunión, por lo que fue aprobado por unanimidad.

3. Revisión y en su caso, autorización del Documento de Seguridad del CIAD.

La Unidad de Transparencia expone al Comité de Transparencia que el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados señala como obligación de los sujetos obligados de elaborar un documento de seguridad que contenga al menos el inventario de datos personales y de los sistemas de tratamiento, las funciones y obligaciones de las personas que traten datos personales, el análisis de riesgos, el análisis de brecha, el plan de trabajo, los mecanismos de monitoreo y revisión de medidas de seguridad y el programa de capacitación. En ese sentido, la persona titular de la Unidad de Transparencia, presentó el Proyecto de Documento de Seguridad del CIAD al Comité para análisis de los integrantes, mismo que fue aprobado por unanimidad. Lo anterior con fundamento en los artículos 35, 83 y 84 fracción I, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

4. Clasificación de información relativa al Análisis de Riesgos, Análisis de Brecha y Plan de Trabajo del Documento de Seguridad.

Con relación al punto anterior, la Unidad de Transparencia expone la propuesta de clasificación ante el Comité de Transparencia analizando la información presentada en el Acta de Clasificación de Información (adjunta al presente), manifestando lo siguiente:

Se procedió al análisis de Documento de Seguridad del CIAD, el cual cuenta con los anexos 1, 2 y 3, respecto del cual el número 2 se considera que debe ser de carácter reservado, por el plazo de cinco años, toda vez que la develación de las situaciones de riesgo, el análisis de brecha, las medidas de seguridad para la protección de los datos personales (Plan de Trabajo), podría implicar la vulneración de dichas medidas, y con ello, la comisión de delitos.
De acuerdo con lo anterior, la información en cuestión se clasificó como reservada, por parte de la Unidad de Transparencia de conformidad con los artículos 113, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública, y 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública, ya que su divulgación podría obstruir la prevención de los delitos previstos en el artículo 211 bis 2 del Código Penal Federal.
En relación con la prueba de daño, la cual tiene fundamento en los artículos 103 y 104 de la Ley General de Transparencia y Acceso a la Información Pública, y 102 de la Ley Federal de Transparencia y Acceso a la Información Pública; si bien a través del derecho de acceso a la información previsto en el artículo 6, Apartado A, fracción I, constitucional, así como en la Ley General de Transparencia y Acceso a la Información Pública; cualquier persona puede tener acceso a la información en posesión de los sujetos obligados, existen determinadas restricciones al respecto, mismas que se refieren a la información reservada y a la información confidencial.
En este sentido, la divulgación de la información señalada, la cual es objeto de reserva, representa un riesgo real al interés público, ya que de darse a conocer conllevaría la obstrucción de la prevención de delitos, como ha sido señalado, y en consecuencia el conocimiento de la información relativa a las medidas de seguridad, análisis de riesgo y brecha y plan de trabajo de este Centro, por terceras personas causaría perjuicio a su protección, y con ello, se afectaría el interés público. La restricción (reserva) al derecho de acceso a la información tiene sustento en el artículo 6, Apartado A, fracción II, constitucional, y 113, fracción VII, de la citada Ley General, y 110, fracción VII, de la aludida Ley Federal.

Una vez analizada el Acta de Clasificación de Información adjunta al presente, el Comité de Transparencia confirmó (por unanimidad) la reserva de la información relativa al Anexo 2 del Documento de Seguridad, por un periodo de 5 años. Asimismo, se ordena la generación de la Versión Pública de dicho documento. Lo anterior con fundamento en el artículo 65, fracción segunda de la Ley Federal de Transparencia y Acceso a la Información Pública y a los artículos 100, 103, 106 fracción III y 111 de la Ley General de Transparencia y Acceso a la Información Pública

5. Revisión y en su caso, autorización del Programa de Protección de Datos Personales del CIAD.

La Unidad de Transparencia presentó el proyecto de Programa de Protección de Datos Personales del CIAD, al Comité de Transparencia, mismo que fue aprobado por unanimidad. Lo anterior con fundamento en el artículo 30, fracción II, 83 y 84 fracción I, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

6. Revisión y en su caso, autorización de los Mecanismos de Monitoreo y Revisión de las Medidas de Seguridad del CIAD.

La Unidad de Transparencia presentó el proyecto de Mecanismos de Monitoreo y Revisión de las Medidas de Seguridad del CIAD, al Comité de Transparencia, mismo que fue aprobado por unanimidad. Lo anterior con fundamento en el artículo 30, fracción V, 83 y 84 fracción I, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

7. Revisión y en su caso, autorización del Procedimiento para atender dudas y quejas del CIAD.

La Unidad de Transparencia presentó el proyecto de Procedimiento para atender dudas y quejas del CIAD, al Comité de Transparencia, mismo que fue aprobado por unanimidad. Lo anterior con fundamento en el artículo 30, fracción VI, 83 y 84 fracción I, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

8. Revisión y en su caso, autorización del Procedimiento interno solicitudes ARCO.

La Unidad de Transparencia presentó el proyecto de Procedimiento Interno para la Atención de Solicitudes de Ejercicio de Derechos Acceso, Rectificación, Cancelación y Oposición del CIAD, al Comité de Transparencia, mismo que fue aprobado por unanimidad. Lo anterior con fundamento en el artículo 83 y 84 fracción I y II, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

9. Análisis, y en su caso determinación de los Criterios Específicos del Comité de Transparencia para la mejor observancia de la Ley General de Datos Personales en Posesión de los Sujetos Obligados.

La Unidad de Transparencia propuso al Comité de Transparencia, establecer Criterios Específicos para la mejor observancia de la Ley General de Datos Personales en Posesión de los Sujetos Obligados. Los cuales se señalan a continuación:

Criterio 1. Suscripción de Acuerdos de Confidencialidad por parte de las personas servidoras públicas del Centro de Investigación en Alimentación y Desarrollo que tengan intervención en cualquier etapa del ciclo de vida del tratamiento de datos personales, debiendo satisfacer este requisito al momento de su incorporación al CIAD o a la posición laboral que se encuentre en este supuesto. Se adjunta formato "Acuerdo de Confidencialidad".

Criterio 2. Inclusión de cláusulas de confidencialidad en los instrumentos jurídicos que suscriba el Centro con proveedores o prestadores de servicios en los que haya tratamiento de datos personales.

Una vez analizado lo anterior, el Comité de Transparencia aprobó por unanimidad establecer los criterios señalados en los puntos 1 y 2. Lo anterior con fundamento en el artículo 83 y 84 fracción IV, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

10. Determinación de Acuerdos.

Primero. - Autorización del Documento de Seguridad del CIAD. Lo anterior con fundamento en los artículos 35, 83 y 84 fracción I, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Segundo. - Se confirma la clasificación de información como reservada, relativa al Anexo 2 del Documento de Seguridad, por un periodo de 5 años. Lo anterior con fundamento en el artículo 65, fracción segunda y 110 fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública y a los artículos 100, 103, 106 fracción III, 111 y 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública

Tercero. - Autorización del Programa de Protección de Datos Personales del CIAD. Lo anterior con fundamento en el artículo 30, fracción II, 83 y 84 fracción I, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Cuarto. - Autorización de los Mecanismos de Monitoreo y Revisión de las Medidas de Seguridad del CIAD. Lo anterior con fundamento en el artículo 30, fracción V, 83 y 84 fracción I, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Quinto. - Autorización del Procedimiento para atender dudas y quejas del CIAD. Lo anterior con fundamento en el artículo 30, fracción VI, 83 y 84 fracción I, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Sexto. - Autorización del Procedimiento Interno para la Atención de Solicitudes de Ejercicio de Derechos Acceso, Rectificación, Cancelación y Oposición del CIAD. Lo anterior con fundamento en el artículo 83 y 84 fracción I y II, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Séptimo. - Determinación de Criterios Específicos para la mejor observancia de la Ley General de Datos Personales en Posesión de los Sujetos Obligados. Los cuales se señalan a continuación:

Criterio 1. Suscripción de Acuerdos de Confidencialidad por parte de las personas servidoras públicas del Centro de Investigación en Alimentación y Desarrollo que tengan intervención en cualquier etapa del ciclo de vida del tratamiento de datos personales, debiendo satisfacer este requisito al momento de su incorporación al CIAD o a la posición laboral que se encuentre en este supuesto. Se adjunta formato "Acuerdo de Confidencialidad".
Criterio 2. Inclusión de cláusulas de confidencialidad en los instrumentos jurídicos que suscriba el Centro con proveedores o prestadores de servicios en los que haya tratamiento de datos personales.

Lo anterior con fundamento en el artículo 83 y 84 fracción IV, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

11. CLAUSURA

Habiéndose tratado todos los puntos del orden del día, se dio por terminada la sesión el día 31 de mayo de 2024 a las 12:00 horas, firmando los que en ella intervinieron.

FIRMAS

Mtra. María Guadalupe Sánchez Soto
Presidenta del Comité y Titular de la Unidad de Transparencia.

Dr. Rogerio Rafael Sotelo Mundo
Coordinador de Investigación.

Lic. Alejandro Salinas Ochoa
Titular de la Unidad Administrativa del Órgano Interno de Control Específico de Conahcyt en el Centro de Investigación en Alimentación y Desarrollo, A.C.

Lic. María del Carmen Castro Cárdenas
Jefa de Departamento de Sistemas Administrativos (Invitada).

ESTA FOJA CORRESPONDE A LA HOJA DE FIRMAS DEL ACTA DE LA TERCERA REUNIÓN EXTRAORDINARIA 2024, DEL COMITÉ DE TRANSPARENCIA DEL CENTRO DE INVESTIGACIÓN EN ALIMENTACIÓN Y DESARROLLO, A.C. (CIAD). DICTADA EN FECHA 31 DE MAYO DE 2024.

Documento de Seguridad de Datos Personales del Centro de Investigación en Alimentación y Desarrollo, A.C.

índice

Introducción

El 26 de enero de 2017 se expidió la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en lo sucesivo, la Ley General de Datos), la cual tiene como objetivo establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales que estén en posesión de los sujetos obligados.

En su artículo primero, la Ley General señala que son sujetos obligados, en el ámbito federal, estatal y municipal, cualquier autoridad, **entidad**, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

El artículo 35 de la Ley General de Datos establece como una obligación la **elaboración de un documento de seguridad**, que se define -según la fracción XIV del artículo 3 de la Ley General- como el **instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.**

De conformidad con el artículo 35 de la Ley General de Datos, el documento deberá contener, al menos, la siguiente información:

I. El inventario de datos personales y de los sistemas de tratamiento;
II. Las funciones y obligaciones de las personas que traten datos personales;
III. El análisis de riesgos;
IV. El análisis de brecha;
V. El plan de trabajo;
VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
VII. El programa general de capacitación.

En ese sentido, en cumplimiento de las obligaciones antes descritas, a continuación, se presenta el documento de seguridad del Centro de Investigación en Alimentación y Desarrollo, A.C. (en lo sucesivo, el Centro).

Objetivo

El presente documento tiene como propósito controlar internamente el universo de datos personales en posesión del Centro de Investigación en Alimentación y Desarrollo, A.C., el tipo de datos personales que contienen los archivos, los responsables, las obligaciones, el análisis de riesgos y los mecanismos de monitoreo y revisión de las medidas de seguridad, entre otros.

Marco Normativo

- Constitución Política de los Estados Unidos Mexicanos. Publicada en el Diario Oficial de la Federación el 5 de febrero del 1917, última reforma 22 de marzo de 2024.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Publicada en el Diario Oficial de la Federación el 26 de enero del 2017.
- Lineamientos Generales Lineamientos Generales de Protección de Datos Personales para el Sector Público. Publicado en el Diario Oficial de la Federación el 1 de enero del 2018.
- Ley General de Transparencia y Acceso a la Información Pública. Publicada en el Diario Oficial de la Federación el 4 de mayo de 2015, última reforma 20 de mayo de 2021.

Ámbito de aplicación y observaciones generales

Las obligaciones que tienen las personas responsables de los tratamientos de los datos personales, se encuentran establecidas en la LGPDPPSO y en *Lineamientos Generales de Protección de Datos Personales para el Sector Público*, y son aplicables para todas las personas servidoras públicas del CIAD que en el ejercicio de sus atribuciones y funciones, tengan acceso a los datos personales y que dentro de sus Sistemas de Tratamiento de Datos Personales realicen el manejo, tratamiento, administración, transferencia, divulgación y/o eliminación de los datos personales ya sea completos, o el tramo de información que corresponde.

Aplica para aquellos datos personales que obren en soportes físicos y/o electrónicos, con independencia de la forma o modalidad de su creación, procesamiento, almacenamiento y organización. Los datos personales podrán ser expresados en forma numérica, alfabética, gráfica, alfanumérica, fotografía, acústica o en cualquier formato.

Además de las funciones y obligaciones de las personas servidoras públicas involucradas, establecidas de manera específica en el análisis de cada uno de los Sistemas, de manera general deberán observar lo siguiente:

Funciones genéricas:

- Establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.
- Establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales que lleve a cabo, en los cuales se incluyan los periodos de conservación de estos.
- Cuando no sean necesarios, suprimir los datos de forma adecuada.

Obligaciones genéricas:

- Observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.
- Guardar confidencialidad sobre la información que conozcan en el desarrollo de sus actividades.
- Tratar los datos personales de manera adecuada, pertinente y limitado a lo necesario.
- Contar con capacitación en materia de tratamiento de datos personales.
- Dar aviso a los superiores jerárquicos, ante cualquier acción que pueda poner en riesgo los datos personales y, en general, que puedan vulnerar la seguridad de los datos personales.

Las personas servidoras públicas responsables del tratamiento de datos personales en todo momento deberán observar los principios generales, así como adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.

Es importante mencionar que la obligación de confidencialidad debe subsistir aún después de que las personas servidoras públicas hayan finalizado su participación en el tratamiento de los datos personales porque hayan cambiado de funciones y aun cuando la relación laboral con el Organismo haya concluido.

I. El inventario de datos personales y de los sistemas de tratamiento.

Con fundamento en los artículos 33, fracción I, y 35 fracción I de la Ley General de Datos, así como en los artículos 58 y 59 de los Lineamientos Generales Lineamientos Generales de Protección de Datos Personales para el Sector Público (en lo sucesivo Lineamientos Generales) el Centro elaboró los inventarios de los distintos tratamientos de datos personales que realiza, identificando los elementos informativos que señala el artículo 58 de los Lineamientos Generales.

Los inventarios forman parte integral del presente documento de seguridad y se encuentran contenidos en el **Anexo 1**.

Con independencia de lo anterior, el siguiente cuadro muestra un resumen de los inventarios elaborados:

	Unidad Administrativa	Área de adscripción	Denominación del Inventario de Tratamiento de Datos Personales
1	Coordinación de Programas Académicos	Dirección General	Administración Escolar
2	Departamento de Recursos Humanos	Dirección Administrativa	Administración de Personal del CIAD
3	Unidad de Transparencia	Dirección Administrativa	Atención de solicitudes de información y ejercicio de derechos ARCO

II. Las funciones y obligaciones de las personas que traten datos personales.

El artículo 33, fracción II de la Ley General de Datos, establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la definición de las funciones y obligaciones del personal involucrado en el tratamiento de datos personales. Asimismo, de conformidad con la fracción II del artículo 35 de la Ley General, este elemento informativo forma parte del documento de seguridad.

De igual forma, el responsable debe atenerse a lo establecido en el artículo 57 de los Lineamientos Generales.

En ese sentido dentro del inventario de datos personales, anexo al presente se identifican las funciones del personal que interviene en el tratamiento de los datos personales. No obstante, a continuación, se señalan a los titulares de las distintas unidades administrativas que realizan diversos tratamientos:

- Coordinación de Programas Académicos
  Titular: Dra. Beatriz Olivia Camarena Gómez

- Unidad de Transparencia
  Titular. María Guadalupe Sánchez Soto

- Departamento de Recursos Humanos
  Titular: Mtra. María Guadalupe Sánchez Soto

Las personas que desempeñan los puestos anteriormente mencionados, tienen como funciones y obligaciones lo siguiente:

a) Garantizar la seguridad en el tratamiento de datos personales, esto con la finalidad de evitar algún riesgo, como la pérdida, robo, alteración o acceso no autorizado.
b) Garantizar la debida protección de los datos personales, conforme a la Ley y las demás disposiciones aplicables en la materia.
c) Implementar medidas de seguridad físicas, técnicas y administrativas convenientes para el tratamiento diario de los datos personales.

d) Garantizar la confidencialidad de los datos personales derivada de los procedimientos que tienen a su cargo.
e) Conocer y aplicar las acciones derivadas de este Documento de Seguridad.
f) Garantizar el cumplimiento de los derechos ARCO a los titulares de los datos personales.

Adicionalmente, conviene señalar que las funciones y obligaciones del personal que trata datos personales se encuentran definidas en la normatividad que rige el actuar del CIAD, por lo cual, para efectos del presente documento de seguridad, el marco normativo de referencia se encuentra establecido en el Manual de Organización del Centro de Investigación en Alimentación y Desarrollo, A.C. y a los perfiles de puesto correspondientes.

III. Análisis de riesgos, IV. Análisis de brecha y V. Plan de Trabajo. (información clasificada como reservada)

La información relativa al Análisis de riesgos, Análisis de brecha y Plan de Trabajo se encuentra clasificada como reservada de conformidad con Acuerdo 1 del acta de la Tercera Sesión Extraordinaria del Comité de Transparencia de fecha 31 de mayo de 2024.

VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad.

El artículo 33, fracción VII de la Ley General 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.

Como se señaló, de acuerdo con la fracción VI del artículo 35 de la Ley General, los mecanismos de monitoreo y revisión forman parte del documento de seguridad.

Así, 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 mejor 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 CIAD:

Mecanismos de Monitoreo

Para los tratamientos de datos personales del CIAD, se consideran los siguientes tipos de monitoreo:

1) **Revisión de cumplimiento de las políticas internas del CIAD, 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 Ley General, 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 al edificio del CIAD, (ii) control de acceso del personal con tarjeta de proximidad, (iii) control de acceso a través de bitácoras para visitantes y personal del CIAD que olvidó su credencial, (iv) control de asistencia a través de huella digital, y (v) circuito cerrado de cámaras de vigilancia.
b. **Monitoreo del entorno electrónico.** Para la detección continua de amenazas y vulnerabilidades, la DGTI cuenta con herramientas automatizadas de monitoreo (activo y pasivo), así como con bitácoras de los sistemas informáticos del CIAD.
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. Estos cambios se pondrán a consideración del área que apoya en el análisis de riesgos, la DGTI y el Comité de Transparencia.
d. **Revisión de avances del plan de trabajo.** A través de los mecanismos que determine el área que apoya en el análisis de riesgos, la DGTI y el Comité de Transparencia, se hará una revisión de los avances en el plan de trabajo, identificando las acciones, fechas compromiso y, en su caso, las causas por las cuales no se está cumpliendo el plan de trabajo, para hacer los ajustes correspondientes al mismo.
e. **Actualización tecnológica.** Cuando se integren nuevos equipos de cómputo, servidores, aplicaciones o tenga lugar una migración tecnológica, se realizará una actualización del análisis de riesgo, análisis de brecha y plan de trabajo.
f. **Vulneraciones a la seguridad de los datos personales.** En caso de identificar un incidente de seguridad que involucre datos personales, el área que apoya en el análisis de riesgos, la DGTI y el Comité de Transparencia se coordinarán para decidir sobre las acciones pertinentes para mitigar dicho incidente.

A continuación, se describen los mecanismos de monitoreo y revisión de este Instituto:

Elemento a revisar	Fundamento	Acciones
Los nuevos activos que se incluyan en la gestión de riesgos;	63, fracción I, de los Lineamientos Generales.	1. Revisión de cumplimiento de las políticas internas del CIAD, relacionadas con el tratamiento de datos personales.
Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;	63, fracción II, de los Lineamientos Generales.	1. Revisión de cumplimiento de las políticas internas del CIAD, relacionadas con el tratamiento de datos personales.
Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;	63, fracción III, de los Lineamientos Generales.	1. Revisión de cumplimiento de las políticas internas del CIAD, relacionadas con el tratamiento de datos personales. 2.a. Monitoreo del entorno físico. 2.b. Monitoreo del entorno electrónico.
La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;	63, fracción IV, de los Lineamientos Generales.	1. Revisión de cumplimiento de las políticas internas del CIAD, relacionadas con el tratamiento de datos personales. 2.a. Monitoreo del entorno físico. 2.b. Monitoreo del entorno electrónico.
Las vulnerabilidades identificadas para determinar aquellas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;	63, fracción V, de los Lineamientos Generales.	1. Revisión de cumplimiento de las políticas internas del CIAD, relacionadas con el tratamiento de datos personales. 2.a. Monitoreo del entorno físico. 2.b. Monitoreo del entorno electrónico.
El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo	63, fracción VI, de los Lineamientos Generales.	1. Revisión de cumplimiento de las políticas internas del CIAD, relacionadas con el tratamiento de datos personales. 2.c. Actualización del plan de trabajo. 2.d. Revisión de avances del plan de trabajo.
Los incidentes y vulneraciones de seguridad ocurridas.	63, fracción VII, de los Lineamientos Generales.	1. Revisión de cumplimiento de las políticas internas del CIAD, relacionadas con el tratamiento de datos personales. 2.f. Vulneraciones a la seguridad de los datos personales.

Mecanismos de supervisión o revisión

Además del monitoreo continuo de las medidas de seguridad, se requiere realizar una supervisión periódica de las medidas de seguridad, a través de auditorías, las cuales pueden ser internas (desarrolladas por el propio CIAD) o externas (realizando una contratación o a través de un convenio con un tercero).

Hasta el momento no se han realizado auditorías específicas en materia de protección de datos personales a los tratamientos del Instituto.

Así, respecto del programa de auditoría mencionado en el último párrafo del artículo 63 de los Lineamientos Generales, se tiene contemplada la realización de una auditoría en materia de protección

de datos personales, al menos una vez al año. Dicha auditoría se puede llevar a cabo por terceros según la disponibilidad presupuestal, o bien internamente por personal del CIAD, conforme lo determine el Comité de Transparencia.

El programa de auditoría será aquél que determine el Comité de Transparencia en el Programa de Protección de Datos Personales del CIAD.

Los resultados de las auditorías se considerarán para realizar adecuaciones al análisis de riesgos del CIAD y, por lo tanto, al plan de trabajo.

VII. El programa general de capacitación.

Atendiendo a lo mencionado en el artículo 30, fracción III, de la Ley General, el Centro está comprometido en un programa de capacitación y que busque formar al personal en el tema de protección de Datos Personales. A su vez, el artículo 48 de los Lineamientos generales menciona que dicho plan de capacitación deberá establecerse de forma anual, siendo aprobado, coordinado y supervisado por el Comité de Transparencia.

La Unidad de Transparencia se encargará, junto al Comité de Transparencia, de coordinar la capacitación continua y especializada del personal que integren el Centro. Siendo el Comité de Transparencia que, entre sus atribuciones, incluye el establecer programas de capacitación y actualización para la debida formación de servidores públicos en materia de Transparencia y Protección de Datos Personales.

A partir de lo anterior, el CIAD desarrolló su programa general de capacitación, mismo que integra el Anexo 3 de este documento de seguridad.

Actualización del documento de seguridad.

El artículo 36 de la Ley General establece la obligación de la actualización del documento de seguridad cuando ocurran los siguientes eventos:

I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, y
IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

En ese sentido, el Comité de Transparencia deberá estar atento a la actualización de alguno de los supuestos antes citado, para, en su caso, actualizar el presente documento de seguridad.

Tal sea el caso de sufrir alguna actualización el Documento de Seguridad, esté será nuevamente sometido a aprobación del pleno del Comité de Transparencia del Centro.

Fecha de Autorización

31 de mayo de 2024

El presente documento fue aprobado por el Comité de Transparencia del CIAD, en la Tercera Sesión Extraordinaria 2024, de fecha 31 de mayo de dos mil veinticuatro.

Mtra. María Guadalupe Sánchez Soto

Titular de la Unidad de Transparencia y Presidenta del Comité de Transparencia.

Lic. Alejandro Salinas Ochoa

Titular de la Unidad Administrativa del Órgano Interno de Control Específico en el Conahcyt en el Centro de Investigación en Alimentación y Desarrollo, A.C.

Dr. Rogerio Rafael Sotelo Mundo

Coordinador de Investigación

PROCEDIMIENTO PARA LA RECEPCIÓN Y RESPUESTA DE DUDAS Y QUEJAS DE LOS TITULARES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

I. OBJETIVO.

Determinar el procedimiento que deberá seguir el Centro de Investigación en Alimentación y Desarrollo, A.C., para recibir y contestar las dudas y quejas que presenten los titulares de datos personales, de conformidad con los artículos 30, fracción VI de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y 50 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

II. ÁMBITO DE APLICACIÓN.

Aplica a los titulares de los datos personales en posesión del Centro de Investigación en Alimentación y Desarrollo, A.C.

III. PROCEDIMIENTO.

Antes.

1. La tramitación de las dudas y quejas podrán ser **anónimas**, esto es, no es requisito que proporcione datos de identificación.

2. La recepción, trámite y respuesta de las dudas y quejas podrán presentarse a través de los siguientes medios:

A. Por **correo electrónico**, dirigido a la Unidad de Transparencia en la dirección electrónica transparencia@ciad.mx.

B. Por **escrito presentado físicamente** en el domicilio de la Unidad de Transparencia de la Unidad de Transparencia ubicada en Carretera Gustavo Enrique Astiazarán Rosas, No. 46, Col. La Victoria, CP. 83304, Hermosillo, Sonora, México.

C. Por **teléfono**, llamando al teléfono (622) 289 24 00, extensión 711.

El horario para la recepción de dudas y quejas por correo electrónico comprende de lunes a viernes de las ocho a las quince horas.

Las dudas o quejas cuya recepción se verifique después de los horarios señalados en los incisos anteriores, se considerarán recibidas al día hábil siguiente.

3. Los requisitos para presentar una duda o queja:

a. Nombre o, en su caso, los datos generales de su representante.
b. Descripción clara y precisa de la duda o queja.
c. La persona denunciante o quejosa podrá adjuntar los medios de prueba que estime necesarios para respaldar su duda o queja.
d. En caso de que la duda o queja se presente por escrito y/o por teléfono, deberá señalar el domicilio o medio para recibir notificaciones. Cuando la duda o queja se presente por correo electrónico, se entenderá que acepta que las notificaciones se efectúen por el mismo medio.

La información del inciso a) será proporcionada de manera voluntaria. En ningún caso el dato sobre el nombre podrá ser un requisito para la procedencia y tramite de la duda o queja.

4. Formato para presentar duda o queja.
Podrá presentar la duda o queja, a través de escrito libre en el que exprese, de forma clara y precisa, el cuestionamiento o la queja originada con motivo del tratamiento de los datos personales que obran en poder del CIAD. De igual forma podrá presentar su duda o queja a través de los formatos adjuntos al presente.

5. Atención de dudas.
Corresponderá a éste la atención de dudas, orientación y/o asesoría a las personas para el efectivo ejercicio de los derechos de acceso, rectificación, cancelación, oposición y portabilidad al tratamiento de los datos personales ante este CIAD.

Se entenderá indistintamente como duda o consulta la petición de orientación, asesoría o servicio formulada por una persona, sobre el ejercicio de los derechos de acceso a la información pública, y de acceso, rectificación, cancelación, oposición y portabilidad de sus datos personales y sobre el ejercicio del derecho a la protección de datos personales en posesión de particulares.

La Unidad de Transparencia es el área autorizada para recibir y responder las consultas que formulen las personas al CIAD.

Las dudas que reciba la Unidad de Transparencia se llevará un registro y atención, si la consulta ingresa por medios electrónicos, deberá remitirlas en un plazo no mayor a dos días hábiles, si la consulta se recibe vía telefónica deberá transferirse a la extensión 711.

El plazo para emitir una respuesta a las dudas, orientación y/o asesoría del ejercicio de los derechos acceso, rectificación, cancelación y oposición al tratamiento de sus datos personales ante este Centro, formuladas por el particular, será en un plazo no mayor a cinco días hábiles.

6. No competencia.
Cuando la Unidad de Transparencia determine la notoria incompetencia para atender la duda o queja, lo hará del conocimiento de la persona, dentro de los tres días hábiles posteriores a la recepción de la duda o queja y, en caso de poderlo determinar, le orientará con el o los sujetos obligados competentes.

7. Prevenciones o requerimientos de información adicional.
Cuando no se reúnan los requisitos o no se aporten datos o indicios mínimos para llevar a cabo el trámite de la duda o queja, la Unidad de Transparencia prevendrá al titular de los datos dentro de los cinco días hábiles siguientes a la presentación de su solicitud, por una sola ocasión, para que subsane las omisiones dentro de un plazo de diez días hábiles contados a partir del día siguiente al de la notificación.
Transcurrido el plazo sin desahogar la prevención se tendrá por no presentada la duda o queja y se archivará el expediente como concluido.

8. La duda o queja será desechada por improcedente cuando:

a. Constituyan una solicitud de acceso a la información o de protección de datos personales, en cuyo caso, se registrará en la Plataforma Nacional de Transparencia para el trámite correspondiente.

b. Cuando verse sobre el trámite de algún medio de impugnación.

c. En caso de no desahogar la prevención o requerimiento de información adicional a que se hace referencia en el numeral anterior.

9. Trámite de otro tipo de promociones. Cuando el contenido de la duda o queja corresponda a otro tipo de promoción, tal como solicitud de acceso a la información o de datos personales, recurso de revisión, denuncia por incumplimiento a las obligaciones de transparencia o trámite, se hará del conocimiento de la persona dentro de los plazos establecidos para la atención de las dudas o quejas, en cuyo caso, se reenviará el correo o escrito al área competente para su conocimiento y atención.

10. Plazos de respuesta. Los plazos para atender las dudas o quejas serán contados a partir del día siguiente de su recepción, los cuales no deberán exceder de los siguientes:

Tipo	PLAZO DÍAS HÁBILES
Duda	Cinco días
Queja	Diez días

En caso de determinar que existen hechos constitutivos de presunta responsabilidad administrativa, la Unidad de Transparencia deberá dar vista al Órgano Interno de Control Específico del Conahcyt o a la Unidad Administrativa representante de este en el CIAD, con la queja correspondiente, y enviar un expediente en que se contengan todos los elementos que sustenten la presunta responsabilidad administrativa por incumplimiento de las obligaciones previstas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y las demás disposiciones aplicables.

IV. DESCRIPCIÓN DEL PROCESO.

A. En tratándose de la tramitación de solicitudes formuladas como "Dudas".

1. Presentar la duda. El titular de los datos personales utilizará los medios electrónicos o físicos disponibles para remitir su duda.

2. Recibir y registrar la duda. La Unidad de Transparencia llevará un registro y atención.

3. Contestar la duda. La Unidad de Transparencia dará respuesta a la duda presentada.

B. En tratándose de la tramitación de solicitudes formuladas como "Quejas".

1. Presentar la queja. El titular de los datos personales utilizará los medios electrónicos o físicos disponibles para remitir su queja.
2. Recibir y registrar la queja. La Unidad de Transparencia recibirá la queja y procederá a registrarla en la base de datos, asignándole un folio.
3. Remitir al Comité de Transparencia y Unidad Administrativa competente. Una vez registrada la queja, la Unidad de Transparencia la turnará a la unidad administrativa que resulte competente.

V. FECHA DE ELABORACIÓN Y/O ÚLTIMA MODIFICACIÓN: 20 de mayo de 2024.

FORMATO PARA PRESENTAR DUDAS POR TITULARES DE DATOS PERSONALES

Fecha	Día	Mes	Año

DATOS DEL TITULAR DE LOS DATOS PERSONALES O DE SU REPRESENTANTE

Nombre: _____

Representante Legal (en su caso): _____

FORMA EN LA QUE DESEA RECIBIR NOTIFICACIONES
Marque con una X la decisión de su elección:

◯ **Domicilio** ◯ **Correo Electrónico**

Correo electrónico: _____

En caso de seleccionar la opción a "Domicilio" favor de proporcionar los siguientes:

Calle: _____

Colonia: _____ Municipio: _____

Estado: _____ Código Postal: _____

DESCRIPCIÓN CLARA Y PRECISA DE LA DUDA

FORMATO PARA PRESENTAR QUEJAS POR TITULARES DE DATOS PERSONALES

Fecha	Día	Mes	Año

DATOS DEL TITULAR DE LOS DATOS PERSONALES O DE SU REPRESENTANTE

Nombre:_____

Representante Legal (en su caso):_____

FORMA EN LA QUE DESEA RECIBIR NOTIFICACIONES
Marque con una X la decisión de su elección:

◯ **Domicilio** ◯ **Correo Electrónico**

Correo electrónico: _____

En caso de seleccionar la opción a "Domicilio" favor de proporcionar los siguientes:

Calle: _____

Colonia: _____Municipio: _____

Estado: _____Código Postal: _____

MOTIVOS DE LA QUEJA:

DESCRIPCIÓN DE LOS HECHOS.

Fecha en que ocurrieron los hechos: _____

Hora aproximada de los hechos: _____

Lugar donde sucedieron los hechos: _____

Describa como ocurrieron los hechos:

MENCIONE LOS MEDIOS DE PRUEBA QUE ESTIME NECESARIOS (fotografías, documentos, testigos, entre otros).

El presente documento fue aprobado por el Comité de Transparencia del CIAD, en la Tercera Sesión Extraordinaria 2024, de fecha 31 de mayo de dos mil veinticuatro.

Mtra. María Guadalupe Sánchez Soto

Titular de la Unidad de Transparencia y Presidenta del Comité de Transparencia.

Lic. Alejandro Salinas Ochoa

Titular de la Unidad Administrativa del Órgano Interno de Control Específico en el Conahcyt en el Centro de Investigación en Alimentación y Desarrollo, A.C.

Dr. Rogerio Rafael Sotelo Mundo

Coordinador de Investigación

Programa de Protección de Datos Personales del Centro de Investigación en Alimentación y Desarrollo, A.C. (CIAD)

Contenido

I. Glosario de Términos Comunes

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva para determinar el grado de cumplimiento de los criterios preestablecidos para la misma.

Aviso de privacidad: Documento de forma física, electrónica o en cualquier formato, que es generado por el responsable y puesto a disposición de los titulares de los datos personales, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de estos.

Bases de datos: Conjunto ordenado de datos personales bajo criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Centro: Centro de Investigación en Alimentación y Desarrollo, A.C. (CIAD)

Comité de Transparencia: Instancia a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública y 83 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

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.

Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

Documento de Seguridad: Instrumento que describe y da cuenta, de manera general, sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Encargado: Persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o juntamente con otras trate datos personales a nombre y por cuenta del responsable.

LGPDPPSO: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Lineamientos Generales: Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Programa: Programa de Protección de Datos Personales.

Responsable: Sujeto obligado de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados que decide sobre el tratamiento de los datos personales.

Revisión: Actividad estructurada, objetiva y documentada, llevada a cabo con la finalidad de constatar el cumplimiento continuo de los contenidos establecidos en este Programa.

Riesgo: Combinación de la probabilidad de un evento y su consecuencia desfavorable.

Sujeto Obligado: Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, del ámbito federal.

Titular: Persona física a quien corresponden los datos personales.

Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

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.

Unidad Administrativa: Área a la que se le confieren atribuciones específicas en el Estatuto Orgánico del CIAD, incluidas las ponencias de los Comisionados.

Unidad de Transparencia: Instancia a la que hace referencia el artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública.

II. Presentación

De conformidad con el artículo 34 de la LGPDPPSO, un sistema de gestión es un conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, así como, el cumplimiento de los principios, deberes y obligaciones previstos en dicha ley y las demás disposiciones que resulten aplicables en la materia.

El sistema de gestión del Centro desarrolla las siguientes cuatro fases: planificar, hacer, verificar y actuar (PHVA), de acuerdo con lo descrito en la tabla siguiente:

	Elemento	Fase del ciclo PHVA	Actividades
PROCESO		**P**lanificar	Identificar políticas, objetivos, riesgos, planes, procesos y procedimientos necesarios para obtener el resultado esperado por el responsable o encargado.
	Medios de acción	**H**acer	Implementar y operar las políticas, objetivos, planes, procesos y procedimientos establecidos en la fase anterior.
		Verificar	Evaluar y medir los resultados de lo implementado, a fin de verificar el adecuado funcionamiento del sistema de gestión y el logro de la mejora esperada.
		Actuar	Adoptar medidas correctivas y preventivas en función de los resultados y de la revisión realizada, o de otra información relevante, para lograr la mejora continua.

Para la elaboración del presente documento, se identificaron las obligaciones que establece la LGPDPPSO y los Lineamientos Generales y, a partir de ello, se definieron las acciones a seguir para su cumplimiento.

III. Objetivos del Programa

El Programa de Protección de Datos Personales del CIAD busca la realización de los siguientes objetivos:

1. Estipular los elementos, actividades, operación y procesos que realiza el Centro que permiten la protección continua de los Datos Personales en su posesión.
2. Establecer los mecanismos para cumplir con sus obligaciones conforme a la LGPDPPSO, así como demás normatividad aplicable.
3. Elaboración de programas de capacitación y actualización del personal del Centro, en materia de Protección de Datos Personales.
4. Fomentar la cultura de la Protección de Datos Personales en el Centro.
5. Implementar un sistema de gestión de seguridad de Datos Personales, el cual permita planificar, implementar, operar, monitorear y mejorar la seguridad en sus modalidades administrativa, físico y técnico.

IV. Responsabilidades

Con fundamento en lo dispuesto por los artículos 83 y 84, fracción I de la LGPDPPSO y 47, segundo párrafo, y 48 de los Lineamientos Generales, que señalan que el Comité de Transparencia es la autoridad máxima en materia de protección de datos personales y que tiene entre sus funciones la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, dicho órgano tendrá las siguientes funciones con relación a este programa:

I. Elaborar, aprobar, coordinar y supervisar el Programa, en conjunto con las áreas técnicas que estime necesario involucrar o consultar;
II. Proponer cambios y mejoras al Programa, a partir de la experiencia de su implementación;
III. Dar a conocer el Programa al interior del sujeto obligado;
IV. Supervisar la correcta implementación del Programa;
V. Elaborar, aprobar, coordinar y supervisar el programa anual de capacitación, en conjunto con las áreas técnicas que estime necesario involucrar o consultar, y
VI. Las demás que de manera expresa señale el propio Programa.

V. Alcance del Programa

El presente programa aplicará a todas las unidades administrativas del CIAD que realicen tratamiento de datos personales en ejercicio de sus atribuciones, y a todos los tratamientos de datos personales que éstas efectúen en ejercicio de sus atribuciones.

Para ello, resulta fundamental que el Programa se conozca al interior del sujeto obligado, por lo que el Comité de Transparencia se encargará de difundirlo entre los servidores públicos.

Asimismo, en virtud de que uno de los objetivos del Programa es cumplir con las obligaciones establecidas en la LGPDPPSO, se cubrirán todos los principios, deberes y obligaciones que establece dicha norma para los responsables del tratamiento.

Quedan exceptuados de la aplicación de este programa, los datos personales que correspondan al cumplimiento de las obligaciones de transparencia a las que refieren el artículo 120 de la Ley General de Transparencia y Acceso a la Información Pública y numeral 117 de la Ley Federal de Transparencia y Acceso a la Información Pública.

Las unidades administrativas que forman parte de CIAD, y que deberán observar el Programa son las siguientes:

1. Dirección General
2. Dirección de Administración

3. Subdirección de Recursos Materiales y Servicios Generales:
4. Departamento de Mantenimiento y Obra Pública
5. Departamento de Adquisiciones
6. Departamento de Control Patrimonial y Servicios Generales

7. Departamento de Personal
8. Departamento de Contabilidad y Tesorería
9. Departamento de Presupuestos
10. Departamento Administrativo de Culiacán
11. Departamento Administrativo de Mazatlán
12. Departamento de Control y Sistemas Administrativos.
13. Departamento de Tecnologías de la Información y Comunicaciones.

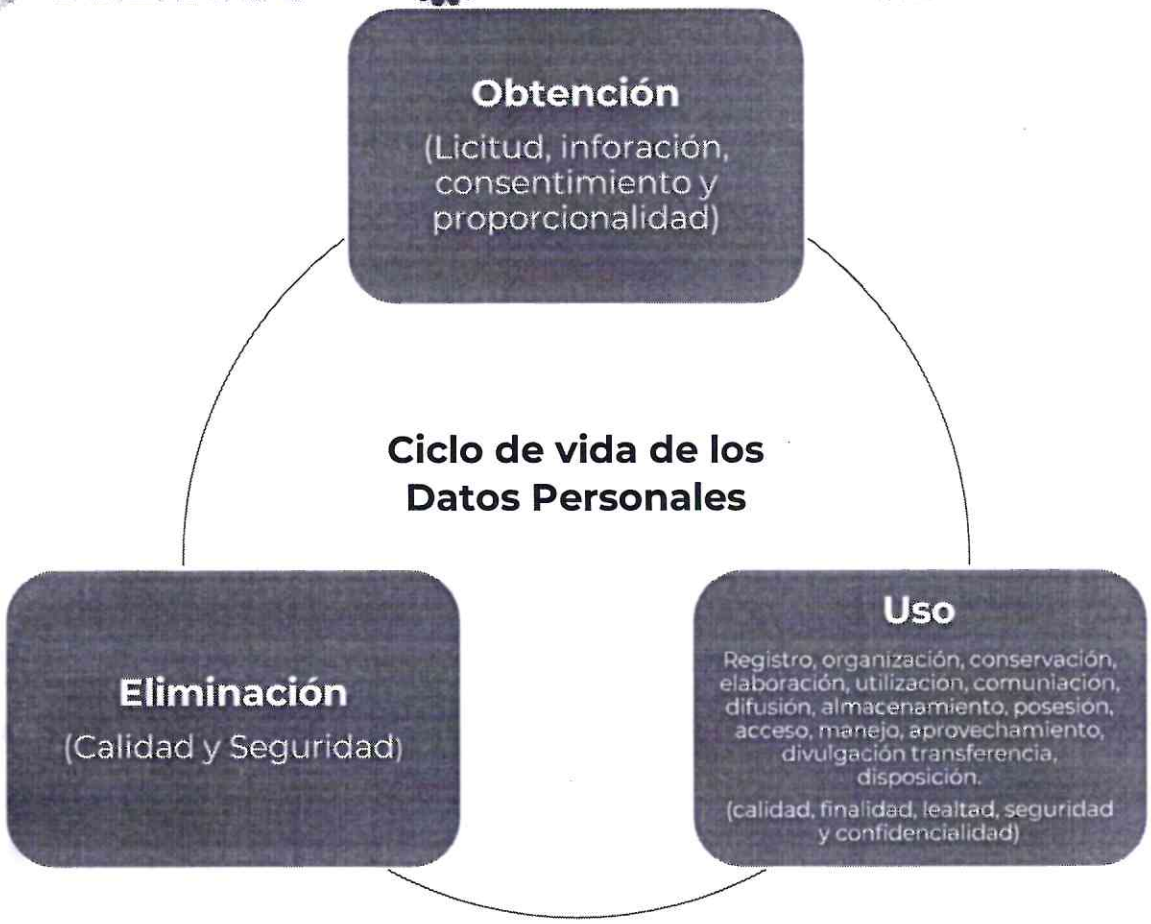
14. Coordinación de Vinculación
15. Coordinación de Investigación
16. Coordinación de Programas Académicos

VI. Política de Gestión de los Datos Personales

El tratamiento de datos personales que realicen las unidades administrativas deberá cumplir con los principios, deberes y obligaciones que prevé la LGPDPPSO, para lo cual este programa establecerá el marco de trabajo mínimo que se deberá seguir para alcanzar dicho objetivo.

Para ello, se identificarán las obligaciones que se deberán cumplir en todos los tratamientos de datos personales que realicen las unidades administrativas, de acuerdo con lo que establece la LGPDPPSO y los Lineamientos Generales, y según el ciclo de vida de los datos personales.

Asimismo, el CIAD procurará la adopción de mejores prácticas para la protección de datos personales, en aquellos tratamientos que así lo permitan y según el nivel de madurez que exista.



VII. Inventario de Tratamiento de Datos Personales

El diagnóstico en mención se basa en la elaboración de un inventario con la información básica de cada tratamiento de datos personales que se realizan en el Centro.

Por "inventario de tratamientos de datos personales" se entenderá el control documentado que se llevará de los tratamientos que realizan las unidades administrativas del Centro, realizado con orden y precisión.

El inventario de datos personales al que hace referencia la LGPDPPSO en los artículos 33, fracción III, 35, fracción I, y 58 de los Lineamientos Generales, identificará los siguientes elementos relevantes:

1. ¿Qué tratamientos de datos personales realiza la unidad administrativa?
Hay que identificar cada uno de los procesos en los que la unidad administrativa trata datos personales.

2. ¿Qué unidad administrativa está a cargo de estos procesos y que por tanto sea la administradora de las bases de datos o archivos que se generen con motivo de dichos tratamientos?
Hay que identificar o definir si la unidad administrativa está a cargo del proceso en donde se tratan los datos personales, según las atribuciones o facultades normativas.

Podría ocurrir que una unidad administrativa trate datos personales recabados en el marco de un proceso del cual no es responsable. Por ejemplo, con motivo de una consulta, la unidad administrativa "X" podría tener acceso a datos de contacto del particular que realizó la consulta, sin embargo, la unidad administrativa que está a cargo del procedimiento de atención a consultas, y quien administra la base de datos de las consultas que recibe la institución es la unidad administrativa "Y".

Asimismo, podría darse el caso en que dos o más unidades administrativas estén a cargo de un proceso mediante el cual se recaban los datos personales y que administren las bases de datos correspondientes de manera conjunta.

En ese sentido, para definir quién está a cargo del proceso mediante el cual se recaban los datos personales y que, por tanto, administre las bases de datos o archivos correspondientes, es necesario analizar la función que realiza cada unidad administrativa dentro del proceso, y las atribuciones o facultades normativas que resulten aplicables.

3. Una vez que hayan sido identificados los tratamientos de los cuales está a cargo la unidad administrativa, será necesario determinar lo siguiente, de acuerdo con el ciclo de vida de los datos personales:

a. ¿Cómo se obtienen los Datos Personales?

- Directamente del titular
    - De manera personal, con la presencia física del titular de los datos personales o su representante, en su caso.
    - Vía telefónica
    - Por correo electrónico
    - Por internet o sistema informático
    - Por escrito presentado directamente en las oficinas del sujeto obligado
    - Por escrito enviado por mensajería

- Mediante una transferencia
  - Quién transfiere los Datos Personales y para qué fines
  - Medios por los que se realiza la transferencia.

- De una fuente de acceso público

b. ¿Qué tipo de Datos Personales se tratan? ¿son sensibles?

c. ¿Dónde se almacenan y realiza el tratamiento de los Datos Personales?
- Sección, serie y subserie de archivos
- Formato en que se encuentra la base de datos: físico y/o electrónico
- Ubicación de la base de datos

d. ¿Para qué finalidades se utilizan los datos personales?

Las finalidades son acciones más específicas de los procesos de los que derivan los tratamientos de datos personales. Por ejemplo, el procedimiento podría ser "contratación de personal" y las finalidades "evaluación de currículum para la selección de personal".

Será necesario identificar si se requiere el consentimiento o no de los titulares y el tipo de consentimiento (tácito o expreso y por escrito), y en caso de que no se requiera, definir qué supuestos (fracciones) del artículo 22 de la LGPDPPSO se actualizan.

Asimismo, se deberá señalar el marco jurídico que da facultades para el tratamiento de datos personales (disposición normativa, artículo, fracción, inciso, párrafo).

e. ¿Quién tiene acceso a la base de datos o archivos (sistemas de tratamiento) y a quién se comunican los datos personales al interior del sujeto obligado?

Se deberá identificar el catálogo de personas servidoras públicas al interior del sujeto obligado que tienen acceso a los datos personales y para qué fin.

f. ¿Intervienen encargados en el tratamiento de los datos personales?

Es necesario identificar el nombre del encargado y el número de contrato, pedido o convenio correspondiente.

g. ¿Qué transferencias se realizan o se podrían realizar de los datos personales y con qué finalidad?

Hay que identificar las autoridades o terceros externos al Centro a quienes se comunican los datos personales y los fines de las transferencias.

Asimismo, es necesario señalar si se requiere el consentimiento para la transferencia, el tipo de consentimiento que se requiere en su caso (tácito o expreso y por escrito), y en caso de que no se requiera el consentimiento, se deberá definir qué supuestos (fracciones) de los artículos 22, 66 o 70 de la LGPDPPSO se actualizan.

h. ¿Se difunden los datos personales?
Hay que señalar si los datos personales se difunden y el fundamento jurídico para ello.

i. ¿Cuál es el plazo de conservación de los datos personales?
Este plazo tendría que estar definido en los instrumentos de clasificación archivística, por lo que es necesario identificar a qué serie documental pertenecen los archivos o bases de datos en los que están contenidos los datos personales.

Una vez que se haya realizado este diagnóstico inicial, estaremos preparados para cumplir de mejor manera con las obligaciones previstas en la LGPDPPSO y los Lineamientos Generales.

VIII. Tratamiento de Datos personales

La información dentro del Centro es transmitida en diversos medios, pudiendo ser impresa, escrita en papel, transmitida por correo, almacenada electrónicamente, utilizada por medios electrónicos, expuesta en una conversación o almacenada electrónicamente, independientemente del medio, dicha información debe ser protegida de forma adecuada.

El tratamiento de los Datos Personales se conforma por diversas etapas que permiten recabar los datos, registrarlos en una base de datos, lo que a su vez permite modificarlos, utilizarlos, comunicarlos, bloquearlos o destruirlos, por lo que es esencial la protección de los mismos.

Las etapas del Tratamiento de Datos Personales se integra de la siguiente manera:

1. **Obtención:** Momento en que se recaban los datos del titular, ya sea que él mismo los proporcione, o a través de un tercero, mediante el uso de diversos medios.

2. **Uso:** Etapa donde los Datos Personales recabados se someten a diversos procedimientos, de manera que son registrados en una base de datos para ser modificados, consultados o utilizados en cualquier forma. El manejo de los datos puede ser hecha por el responsable autorizado para cumplir con el propósito por el que fueron recabados, o también siendo difundidos o distribuidos con un tercero, para la prestación de un servicio determinado al propio responsable.

3. **Eliminación, bloqueo, destrucción de los Datos Personales:** Etapa donde los Datos Personales han dejado de ser necesarios o han cumplido con las finalidades establecidas en el Aviso de Privacidad, por lo que, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya su plazo de conservación de los mismos.

El tratamiento de Datos Personales implica cualquier operación o conjunto de operaciones efectuadas mediante procedimientos informáticos, manuales, digitales o electrónicos, enfocados en la obtención, registro, organización, conservación, utilización, cotejo, interconexión o cualquier forma que permita la obtención de información y facilite al interesado el acceso, rectificación, cancelación u oposición de sus datos.

Para el cumplimiento de las obligaciones establecidas en la Ley de la materia, se deberá observar lo siguiente:

- **Obtención de Datos Personales:**

  Los Datos Personales podrán ser recabados de forma enunciativa, más no limitativa, por los siguientes medios:

  - Visita a las instalaciones.
  - Llenado de formatos.
  - Formularios electrónicos.
  - Presentación de un escrito.

Los medios por los cuales se obtenga y traten los Datos Personales deberán ser lícitos, privilegiando en todo momento la protección de los intereses del titular y la expectativa razonable de privacidad, evitando utilizar medios engañosos o fraudulentos.

Previo al tratamiento de Datos Personales, se deberá obtener el consentimiento del titular, de manera libre, especifica e informada, se considerará que el consentimiento del titular es tácito, cuando habiéndose puesto a su disposición el Aviso de Privacidad, aquel no manifieste su voluntad en sentido contrario.

En el caso de Datos Personales Sensibles, se deberá obtener el consentimiento expreso y escrito por el titular para su tratamiento, a través de firma autógrafa, electrónica o cualquier mecanismo de autenticación que al efecto se establezca.

- **Uso y almacenamiento de Datos Personales**

El responsable deberá adoptar las medidas necesarias para mantener exactos, pertinentes, completos, correctos y actualizados los Datos Personales en su posesión, a fin de que se no se altere la veracidad de éstos.

El tratamiento de Datos Personales que lleven a cabo las distintas áreas administrativas del Centro deberá sujetarse a establecido por los artículos 9 de los Lineamientos Generales y 18 de la LGPDPPSO, por lo que todo tratamiento de Datos Personales que se efectúe deberá estar justificado por finalidades:

I. Concretas: cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión en el titular;
II. Explícitas: cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad;
III. Lícitas: cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones o facultades del responsable, conforme a lo previsto en la legislación mexicana y el derecho internacional que le resulte aplicable, y
IV. Legítimas: cuando las finalidades que motivan el tratamiento de los datos personales se encuentran habilitadas por el consentimiento del titular, salvo que se actualice alguna de las causales de excepción previstas en el artículo 22 de la Ley General.

En el tratamiento de Datos Personales, se deberán mantener mecanismos efectivos de seguridad de carácter administrativo, físico y técnico para la protección de los mismos, con el objetivo de impedir, que se contravenga las disposiciones de la normatividad en la materia. Dichos mecanismos deberán permitir:

- Mantener identificada, clasificada y controlada la información propiedad del Centro a fin de garantizar su confidencialidad, integridad y disponibilidad.
- Establecer normas y controles internos durante la recolección, procesamiento, almacenamiento, acceso y disposición de la información.
- Identificar, evaluar y tomar medidas que disminuyan riesgos en la administración de la información y garantizar la continuidad en los procesos.
- Implantar y mantener un modelo de seguridad de la información, eficiente, tolerante a fallas y fácil de monitorear, que involucren a todo el Centro.
- Proteger al Centro de posibles responsabilidades legales derivadas del uso indebido de los activos de información.
- Implantar y mantener un modelo de seguridad para conservar la confidencialidad e integridad de la información que se genere en el Centro y se transmita a través de medios electrónicos o redes ya sean internas o externas.
- Implantar mecanismos necesarios que permitan conservar la integridad de los documentos y transacciones generados y entregados en el Centro o fuera a terceras personas.
-

- Implantar mecanismos para almacenamiento y recuperación de la información en casos de desastre.
- Implantar mecanismos para prevención y corrección contra ataque de virus informáticos, códigos, maliciosos y demás variantes.
- Recomendar y/o sugerir cambios o mejoras en el establecimiento de seguridad física dentro de las instalaciones del Centro.
- Implantar y mantener mecanismos necesarios para determinar los accesos a los recursos del Centro, como lo son impresoras, equipos, etc.

El responsable deberá informar a los titulares a través del Aviso de Privacidad, la existencia y las características principales del tratamiento al que serán sometidos sus datos personales.

IX. Vulneraciones

El responsable deberá llevar una bitácora de las vulneraciones a la seguridad en la que se describa ésta, la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.

Se considera como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:

- La pérdida o destrucción no autorizada;
- El robo, extravío o copia no autorizada;
- El uso, acceso o tratamiento no autorizado o,
- El daño, la alteración o modificación no autorizada

El responsable deberá informar en un plazo máximo de **setenta y dos hora** al titular y al Comité de Transparencia, las vulneraciones que afecten de forma significativa los **derechos patrimoniales** (de forma enunciativa más no limitativa relacionado con sus bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, AFORES, fianzas, servicios contratados o las cantidades o porcentajes relacionados con la situación económica del titular) o **morales** (de manera enunciativa, más no limitativa, relacionados con sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspectos físicos, menoscabo ilegalmente de la libertad o integridad), en cuanto se confirme que ocurrió la vulneración y que el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados, puedan tomar las medidas para la defensa de sus derechos.

Conforme al artículo 67 de los Lineamientos Generales, la notificación de vulneración de seguridad al Comité de Transparencia deberá contener los siguientes elementos:

I. La hora y fecha de la identificación de la vulneración;
II. La hora y fecha del inicio de la investigación sobre la vulneración;

III. La naturaleza del incidente o vulneración ocurrida;
IV. La descripción detallada de las circunstancias en torno a la vulneración ocurrida;
V. Las categorías y número aproximado de titulares afectados;
VI. Los sistemas de tratamiento y datos personales comprometidos;
VII. Las acciones correctivas realizadas de forma inmediata;
VIII. La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida;
IX. Las recomendaciones dirigidas al titular;
X. El medio puesto a disposición del titular para que pueda obtener mayor información al respecto;
XI. El nombre completo de la o las personas designadas y sus datos de contacto, para que puedan proporcionar mayor información al Centro, en caso de requerirse, y
XII. Cualquier otra información y documentación que considere convenientes hacer del conocimiento del Centro.

- **Eliminación de datos personales**

Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el Aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, deberán ser Suprimidos, previo Bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos.

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.

Se deberán establecer métodos y técnicas para la supresión definitiva de los Datos Personales, de tal manera que la posibilidad de recuperarlos o reutilizarlos sea nula; para lo cual se deberán considerar los medios de almacenamiento físicos y/o electrónicos en los que se encuentren los Datos Personales, así como los siguientes atributos:

- **Irreversibilidad:** Que el proceso utilizado no permita recuperar los Datos Personales.
- **Seguridad y confidencialidad:** En la eliminación definitiva de los Datos Personales, se deberán observar los deberes de confidencialidad y seguridad establecidos en la ley de le la materia.
- **Favorable al medio ambiente:** Que el método utilizado produzca el mínimo de emisiones y desperdicios que afecten al medio ambiente.

X. Obligaciones de las Unidades Administrativas

Con la finalidad de mejorar el tratamiento y seguridad de los datos personales, así como, el cumplimiento de los principios, deberes y obligaciones previstos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, las unidades administrativas deberán elaborar y mantener actualizado, de conformidad con lo señalado en los puntos anteriores y la normativa aplicable, lo siguiente:

1. Inventario de datos personales
2. Aviso de privacidad
3. Bitácora de vulneraciones.
4. Análisis de Riesgos de Activos
5. Proponer y establecer medidas de seguridad al interior del área en materia de seguridad de la información en su posesión.
6. Promover la capacitación de los servidores públicos que integran la unidad administrativa.
7. Atender las sugerencias y recomendaciones del Comité de Transparencia.
8. Las demás que señale la normativa correspondiente.

XI. Revisiones

Con la finalidad de establecer y mantener las medidas de seguridad para los Datos Personales, el Comité de Transparencia evaluará y medirá los resultados de las políticas, planes, proceso y procedimientos implementados en materia de seguridad y tratamiento de datos, a fin de verificar el cumplimiento de los objetivos planteados, se deberá monitorear continuamente los siguientes aspectos:

- Los nuevos activos que se incluyan en la gestión de riesgos
- Las modificaciones necesarias a los activos
- Las nuevas amenazas que podrían estar activas dentro y fuera del Centro y que no han sido valoradas.
- La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes
- Las vulnerabilidades identificadas para determinar aquellas expuestas a amenazas nuevas o pasadas que vuelvan a surgir.
- El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.
- Los incidentes y vulneraciones ocurridos.

XII. Acciones para la mejora continua del Programa

En esta fase del Programa, se adoptarán las medidas preventivas y correctivas que hayan resultado de las revisiones realizadas, o bien que se hayan obtenido de otras fuentes de información relevantes.

Los puntos de mejora de la implementación del Programa pueden ser de dos tipos:

1. Acciones preventivas: El objetivo de las acciones preventivas es disminuir la probabilidad de ocurrencia.

2. Acciones correctivas: El objetivo de las acciones correctivas es eliminar la causa de la no conformidad, o bien, reducir su grado de prevalencia.

El Comité de Transparencia deberá establecer un plazo límite para que se corrijan las no conformidades detectadas.

El Comité de Transparencia deberá documentar las medidas preventivas o correctivas realizadas para la mejora continua en la implementación de este Programa.

Obligaciones	**Actividades para su cumplimiento**	**Unidades administrativas/ponencias responsables del cumplimiento**	**Medios para acreditar el cumplimiento**
El responsable deberá implementar acciones para evitar o corregir cualquier no conformidad.	1. Elaborar un procedimiento para la gestión de las acciones preventivas y correctivas.	Comité de Transparencia	• Procedimiento para la gestión de acciones preventivas y correctivas. • Documentación que acredite las acciones preventivas o correctivas implementadas, así como los resultados y revisiones de las acciones una vez implementadas.

XIII. Sanciones por Incumplimiento

Cuando el Comité de Transparencia tenga conocimiento del incumplimiento de alguna obligación prevista en este Programa, deberá realizar a la unidad administrativa correspondiente un exhorto para que lleve a cabo las acciones que resulten pertinentes con objeto de modificar dicha situación y evitar incumplimientos futuros o situaciones de riesgo que los pudieran ocasionar.

De manera adicional, es importante que las personas servidoras públicas que están a cargo del tratamiento de datos personales tengan presente que de conformidad con el artículo 163 de la LGPDPPSO serán causas de sanción por incumplimiento de las obligaciones establecidas en dicha 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 LGPDPPSO 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 LGPDPPSO;
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 LGPDPPSO, 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 LGPDPPSO;
VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la LGPDPPSO;
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 LGPDPPSO;
X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la LGPDPPSO;
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 LGPDPPSO;

XIII. No acatar las resoluciones emitidas por el Centro, 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.

Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, XII, y XIV, así como la reincidencia en las conductas previstas en el resto de las fracciones, serán consideradas como graves.

Asimismo, de conformidad con el artículo 105 de los Lineamientos Generales, cuando alguna unidad administrativa se niegue a colaborar con la Unidad de Transparencia en la atención de las solicitudes para el ejercicio de los derechos ARCO, ésta dará aviso al superior jerárquico para que le ordene realizar sin demora las acciones conducentes.

Si persiste la negativa de colaboración, la Unidad de Transparencia lo hará del conocimiento del Comité de Transparencia para que, a su vez, dé vista al Órgano interno de Control Específico y, en su caso, dé inicio el procedimiento de responsabilidad administrativo respectivo.

Cabe destacar que las sanciones de carácter económico no podrán ser cubiertas con recursos públicos.

Las responsabilidades que resulten de los procedimientos administrativos correspondientes son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.

El Comité de Transparencia tomará las medidas necesarias para que las personas servidoras públicas del sujeto obligado conozcan esta información.

Fecha de autorización
30 de mayo de 2024

El presente documento fue aprobado por el Comité de Transparencia del CIAD, en la Tercera Sesión Extraordinaria 2024, de fecha 31 de mayo de dos mil veinticuatro.

Mtra. María Guadalupe Sánchez Soto

Titular de la Unidad de Transparencia y Presidenta del Comité de Transparencia.

Lic. Alejandro Salinas Ochoa

Titular de la Unidad Administrativa del Órgano Interno de Control Específico en el Conahcyt en el Centro de Investigación en Alimentación y Desarrollo, A.C.

Dr. Rogerio Rafael Sotelo Mundo

Coordinador de Investigación

Mecanismos de Monitoreo y Revisión de las Medidas de Seguridad del Centro de Investigación en Alimentación y Desarrollo, A.C. (CIAD)

El artículo 30, fracción V, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establece que entre los mecanismos que se deberán adoptar para cumplir con el principio de responsabilidad, se encuentra el de establecer un sistema de supervisión y vigilancia, incluyendo, que permita comprobar el cumplimiento de las políticas de protección de datos personales.

En ese sentido, el artículo 35, fracción VI, de la Ley General establece que el documento de seguridad deberá contener, entre otros aspectos, los mecanismos de monitoreo y revisión de las medidas de seguridad.

Al respecto, el artículo 33, fracción VII, de la Ley General, dispone que se deberán de monitorear y revisar de manera periódica los aspectos siguientes:

1. Las medidas de seguridad implementadas en la protección de datos personales.

2. Las amenazas y vulneraciones a que están sujetos los tratamientos o sistemas de datos personales

En ese sentido, el artículo 63 de los **Lineamientos Generales de protección de datos personales para el sector público** establece que 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 anterior, el responsable deberá monitorear continuamente lo siguiente:

1. Los nuevos activos que se incluyan en la gestión de riesgos.

2. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras.

3. Las nuevas amenazas que podrían estar activas dentro y fuera del sujeto obligado y que no han sido valoradas.

4. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.

5. Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir.

6. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.

7. Los incidentes y vulneraciones de seguridad ocurridos.

Asimismo, el responsable deberá monitorear y revisar la eficacia y eficiencia del sistema de gestión.

En ese sentido, el CIAD desarrollará el cumplimiento de dicha obligación a través de los siguientes mecanismos:

A. Mecanismo de monitoreo y supervisión

La Unidad de Transparencia será la encargada de ejecutar el mecanismo de monitoreo y supervisión de las medidas de seguridad implementadas en la protección de datos personales, a través de los siguientes ejes:

I. **Etapa de Monitoreo**. La Unidad de Transparencia requerirá a cada una de las áreas que reportaron tratamientos de datos personales, a través de sus inventarios, la elaboración de un reporte, en el que deberán precisarse:

	Sí	No
1. Se han definido y se establecen y mantienen las medidas de seguridad administrativas, técnicas y físicas necesarias para la protección de los datos personales.	☐	☐
2. Se ha revisado el marco normativo que regula en lo particular el tratamiento de datos personales en cuestión, a fin de identificar si éste contempla medidas de seguridad específicas o adicionales a las previstas en la LGPDPPSO y los Lineamientos Generales, y se ha definido la procedencia de su implementación.	☐	☐
3. Se han definido las funciones y obligaciones de cada servidor público que trata datos personales.	☐	☐

4. Se ha comunicado a cada servidor público sus funciones, obligaciones y cadena de mando con relación al tratamiento de datos personales que efectúa.	☐	☐
5. Se ha elaborado el inventario de datos personales con los siguientes elementos: • El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales; • Las finalidades de cada tratamiento de datos personales; • El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no; • El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales; • La lista de servidores públicos que tienen acceso a los sistemas de tratamiento; • En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable, y • En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que las justifican.	☐	☐
6. En el inventario de datos personales se tomó en cuenta el ciclo de vida de los datos personales, conforme a lo siguiente: • La obtención de los datos personales; • El almacenamiento de los datos personales; • El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin; • La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen; • El bloqueo de los datos personales, en su caso, y • La cancelación, supresión o destrucción de los datos personales.	☐	☐
7. Se ha realizado el análisis de riesgo, considerando lo siguiente: • Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico; • El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida; • El valor y exposición de los activos involucrados en el tratamiento de los datos personales; • Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida; • El riesgo inherente a los datos personales tratados, contemplando el ciclo de vida de los datos personales, las amenazas y vulnerabilidades existentes para los datos personales y los recursos o activos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal o cualquier otro recurso humano o material, entre otros; • La sensibilidad de los datos personales tratados; • El desarrollo tecnológico; • Las transferencias de datos personales que se realicen; • El número de titulares; • Las vulneraciones previas ocurridas en los sistemas de tratamiento, y	☐	☐

• El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.		
8. Se ha realizado el análisis de brecha, tomando en cuenta lo siguiente: • Las medidas de seguridad existentes y efectivas; • Las medidas de seguridad faltantes, y • La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.	☐	☐
10. Se monitorea y revisa de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, tomando en cuenta lo siguiente: • Los nuevos activos que se incluyan en la gestión de riesgos; • Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras; • Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas; • La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes; • Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir; • El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y • Los incidentes y vulneraciones de seguridad ocurridas.	☐	☐

II. Etapa de Supervisión. La Unidad de Transparencia analizará los reportes de las áreas, verificando aquellos puntos en los que se hubiera reportado "No" como respuesta y se emitirá un dictamen o ficha técnica en el que se plasmarán las recomendaciones o requerimientos que se consideren pertinentes en materia de seguridad, con la finalidad de que las áreas las atiendan y remitan las evidencias de su cumplimiento.

B. Mecanismos de actuación ante vulneraciones a la seguridad de los datos personales

El artículo 33, fracción VII, de la Ley General, dispone que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá monitorear y revisar de manera periódica las medidas de seguridad implementadas, **así como las amenazas y vulneraciones a las que están sujetos los datos personales.**

En ese sentido, el artículo 63, fracción VII, de los Lineamientos Generales de Protección de Datos Personales para el Sector Publico, entre otras disposiciones estipula que, para evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, **se deberán monitorear las vulneraciones de seguridad ocurridas.**

Por ello, la Unidad de Transparencia deberá monitorear y revisar de manera periódica las medidas de seguridad, así como las amenazas y vulneraciones a las que están sujetos los datos personales, para lo cual se podrá auxiliar del área de Tecnologías de la Información y Comunicaciones.

1. Verificar si el hecho o evento podía dar como consecuencia una vulneración a la seguridad (posible incidente de seguridad), esto es:

   - Que exista una amenaza que, de haberse concretado, hubiera producido sus efectos en el tratamiento de los datos personales.
   - Que dichos efectos, de haberse materializado, hubieran representado un daño en los activos.

2. El área que advirtió de la alerta de seguridad deberá enviar un reporte a la Unidad de Transparencia, en un plazo no mayor a 72 horas, en el que deberá informar:

   - Circunstancias de modo, tiempo y lugar en que se detectó la amenaza.
   - Sistema de Tratamiento de Datos Personales, conforme al Inventario (Anexo 1), en el que se detectó la amenaza.
   - Datos personales involucrados.
   - Datos de identificación y de contacto de la persona servidora pública responsable del tratamiento de los datos personales.
   - Actuaciones que pueden evitar la explotación de la amenaza.
   - Descripción de los controles físicos o electrónicos involucrados en la amenaza.

3. La Unidad de Transparencia registrará la alerta de seguridad y analizará el impacto de la amenaza y, de ser posible, determinará una estrategia de prevención, para lo cual, podrá apoyarse de las áreas técnicas y normativas del CIAD, con la finalidad de evitar que la alerta de seguridad pueda desencadenarse.

20 de mayo de 2024

El presente documento fue aprobado por el Comité de Transparencia del CIAD, en la Tercera Sesión Extraordinaria 2024, de fecha 31 de mayo de dos mil veinticuatro.

Mtra. María Guadalupe Sánchez Soto

Titular de la Unidad de Transparencia y Presidenta del Comité de Transparencia.

Lic. Alejandro Salinas Ochoa

Titular de la Unidad Administrativa del Órgano Interno de Control Específico en el Conahcyt en el Centro de Investigación en Alimentación y Desarrollo, A.C.

Dr. Rogerio Rafael Sotelo Mundo

Coordinador de Investigación

PROCEDIMIENTO INTERNO PARA LA ATENCIÓN DE SOLICITUDES DE EJERCICIO DE DERECHOS ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN

I. OBJETIVO.

Establecer los medios y procedimientos habilitados por el Centro de Investigación en Alimentación y Desarrollo, A.C., (CIAD) para atender las solicitudes de ejercicio de los derechos de acceso, rectificación, cancelación y oposición (ARCO).

II. ÁMBITO DE APLICACIÓN.

Aplica a las unidades administrativas del CIAD para la atención de solicitudes de ejercicio de derechos ARCO.

III. DEFINICIONES.

Para los efectos del presente documento se entenderá por:

I. **Centro:** Centro de Investigación en Alimentación y Desarrollo, A.C.;

II. **Comité de Transparencia:** Instancia a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública;

III. **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;

IV. **Derechos ARCO:** Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales;

V. **Días:** Días hábiles;

VI. **Plataforma Nacional:** La Plataforma Nacional de Transparencia a que hace referencia el artículo 49 de la Ley General de Transparencia y Acceso a la Información Pública;

VII. **Titular:** La persona física a quien corresponden los datos personales;

VIII. **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, y

IX. **Unidad de Transparencia:** Instancia a la que hace referencia el artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública.

IV. PROCEDIMIENTO INTERNO.

Artículo 1. En materia de solicitudes de acceso, rectificación, cancelación y oposición de datos personales, la Unidad de Transparencia y las unidades administrativas deberán atender lo siguiente:

I. **Registro en la Plataforma Nacional de Transparencia.** La Unidad de Transparencia deberá registrar las solicitudes de ejercicio de derechos ARCO el mismo día de su recepción, excepto cuando se reciban después de las dieciocho horas o en días inhábiles, en cuyo caso se podrán capturar al día hábil siguiente;

II. **Turno de solicitudes a las áreas competentes.** La Unidad de Transparencia deberá recibir y turnar las solicitudes a las unidades administrativas responsables dentro de los dos días hábiles siguientes a aquél en que se hayan recibido;

III. **Incompetencia.** La Unidad de Transparencia deberá comunicar al solicitante la notoria incompetencia, dentro de los tres días posteriores a la recepción de la solicitud, en los casos en que los datos no correspondan a este Centro, orientándole de ser posible con el responsable competente;

IV. **Reconducción del ejercicio de derecho.** La Unidad de Transparencia, en caso de advertir que la solicitud corresponde a un derecho diverso, deberá reconducir la vía y comunicarlo al titular, dentro de los cinco días posteriores a la recepción de la solicitud;

V. **Prevención o requerimiento de información adicional.** Si la Unidad de Transparencia requiere información adicional del solicitante para aclarar los términos de su solicitud, deberá requerirle para que lo haga dentro de los cinco días hábiles posteriores a la recepción;

VI. **Requerimiento de información adicional por parte de las áreas.** Si alguna unidad administrativa requiere información adicional del solicitante para aclarar los términos de su solicitud, ello se deberá hacer del conocimiento de la Unidad de Transparencia dentro de los tres días hábiles posteriores a la recepción, a efecto de que ésta gestione lo conducente dentro del plazo referido en la fracción anterior;

VII. **Respuesta a la solicitud por parte de las áreas competentes.** Si los datos obran en los archivos, bases de datos, registros, expedientes o sistemas de la unidad administrativa, se deberá responder a la Unidad de Transparencia, dentro de los ocho días hábiles posteriores a la recepción de la solicitud en la unidad administrativa;

VIII. **Respuesta a la solicitud por parte de la Unidad de Transparencia.** La respuesta deberá ser remitida al solicitante, por conducto de la Unidad de Transparencia, a través de la Plataforma Nacional de Transparencia, comunicándole la disponibilidad de la información en la oficina habilitada, siguiendo los criterios para acreditar la identidad del titular y, en su caso, la identidad y personalidad con la que actúe el representante.

IX. **Costos por reproducción de información.** La Unidad de Transparencia deberá recabar el comprobante por el costo de reproducción de los documentos entregados al solicitante, así como de su certificación o envío, excepto cuando ello

implique la entrega de no más de veinte hojas simples o certificadas, o bien, en su caso, cuando el titular proporcione el medio magnético, electrónico o el mecanismo o dispositivo necesario para su reproducción;

X. **Ampliación de plazo de respuesta.** Si se considera necesario ampliar el plazo legal de veinte días hábiles para responder la solicitud, en términos de lo previsto en el artículo 51 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), ello se deberá solicitar al Comité de Transparencia, a través de un documento que será enviado a la Secretaría Técnica, con la firma del titular de la unidad administrativa correspondiente, fundando y motivando las razones de la ampliación, dentro de los ocho días hábiles posteriores a la recepción;

XI. **Respuesta del área derivado de la ampliación del plazo.** La ampliación del plazo legal será por el término de diez días hábiles, por lo que la unidad administrativa deberá dar respuesta, dentro de los primeros cinco días hábiles del plazo de ampliación:

XII. **Inexistencia de los datos personales.** Si los datos personales respectivos no obran en los archivos, bases de datos, registros, expedientes o sistemas de la unidad administrativa, ello se deberá hacer del conocimiento del Comité de Transparencia, a través de un documento firmado por el titular de la unidad administrativa correspondiente, fundando y motivando la inexistencia, dentro de los cinco días hábiles posteriores a la recepción. Lo anterior, siempre que ninguna otra área cuente con los datos en cuestión, lo cual deberá ser corroborado con la Unidad de Transparencia;

XIII. **Clasificación de datos personales de titulares diversos a quien ejerce el derecho.** Si en los documentos anexos a la respuesta existe información que no pertenece al titular y debe ser clasificada como reservada o confidencial, se deberá hacer del conocimiento del Comité de Transparencia, a través de un oficio con la firma del titular de la unidad administrativa correspondiente, fundando y motivando la clasificación, anexando, en su caso, la versión pública, dentro de los ocho días hábiles posteriores a la recepción. De considerarlo necesario, se solicitará a la unidad administrativa poner a disposición del Comité de Transparencia el documento, registro o expediente clasificado;

XIV. **Remisión de versión pública.** En relación con la fracción anterior, únicamente deberán ser remitidos al Comité de Transparencia, los documentos que contengan información clasificada, en versión pública, por lo que no se deberán presentar documentos en versión íntegra que no sean sujetos de clasificación;

XV. **Improcedencia del ejercicio del derecho**. En el supuesto de que se niegue por cualquier otro motivo el derecho de acceso, rectificación, cancelación y oposición al tratamiento de datos personales, se deberá remitir el asunto al Comité de Transparencia, a través de un documento por el titular de la unidad administrativa

correspondiente, fundando y motivando la negativa, dentro de los ocho días hábiles posteriores a la recepción;

XVI. **Envío de datos personales por correo certificado.** Sólo procederá el envío por correo certificado de los datos personales o de las constancias del ejercicio efectivo de los derechos ARCO, cuando la solicitud sea presentada personalmente por el titular ante el Centro, no medie representación alguna del titular, y no se trate de menores de edad o de datos personales de fallecidos.

XVII. **Envío de datos personales por medios electrónicos.** Sólo procederá el envío por medios electrónicos de los datos personales o de las constancias que acrediten el ejercicio efectivo de los derechos ARCO, cuando el titular hubiere acreditado fehacientemente su identidad y, en su caso, la identidad y personalidad de su representante mediante cualquier mecanismo en los términos previstos en la Ley General y los Lineamientos generales de protección de datos personales para el sector público.

XVIII. **Plazo para hacer efectivos los derechos ARCO.** En caso de resultar procedente el ejercicio de los derechos ARCO, el Centro deberá hacerlo efectivo en un plazo no mayor a quince días contados a partir del día siguiente en que se hubiere notificado la respuesta al titular, previa acreditación de la identidad del titular y, en su caso, la identidad y personalidad con la que actúe su representante legal.

Artículo 2. La Unidad de Transparencia será la responsable de requerir a las unidades administrativas y dar respuesta a las solicitudes, así como realizar todas las gestiones correspondientes a sus funciones y aquellas que el Comité le encomiende, durante la atención de las solicitudes y la sustanciación del recurso de revisión, el cumplimiento a las resoluciones emitidas por el INAI, así como las inconformidades.

Artículo 3. El Comité de Transparencia conocerá del procedimiento de clasificación de información, en aquellos casos en que, con motivo del trámite de los procedimientos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales, los titulares de las unidades administrativas determinen que exista información que sea total o parcialmente clasificada como reservada o confidencial.

El Comité de Transparencia podrá confirmar, modificar o revocar, parcial o totalmente, la clasificación de la información realizada por los titulares de las unidades administrativas.

Artículo 4. El Comité de Transparencia tramitará el procedimiento de inexistencia de información, en aquellos casos en que, con motivo de los procedimientos de acceso a la información, así como de acceso, cancelación, rectificación y oposición al tratamiento de datos personales, los titulares de las unidades administrativas determinen que la información o datos solicitados son parcial o totalmente inexistentes.

La resolución del Comité de Transparencia a que se refiere el artículo 53, segundo párrafo de la Ley General deberá contar con los elementos mínimos que permitan al titular tener

la certeza de que se utilizó un criterio de búsqueda exhaustivo; así como señalar las circunstancias de tiempo, modo y lugar que generaron la inexistencia en cuestión y la unidad administrativa competente de contar con los mismos.

Artículo 5. El Comité de Transparencia sustanciará el procedimiento para conocer negativas de datos personales, en aquellos casos en que, con motivo del trámite de los procedimientos de acceso, cancelación, rectificación u oposición al tratamiento de datos personales, los titulares de las unidades administrativas nieguen por cualquier causa el derecho ejercido. El Comité de Transparencia podrá confirmar, modificar o revocar, parcial o totalmente, la negativa formulada por los titulares de las unidades administrativas.

Artículo 6. En la respuesta a la solicitud para el ejercicio de los derechos ARCO, el Centro deberá señalar los costos de reproducción, certificación y/o envío de los datos personales o de las constancias que acrediten el ejercicio efectivo de los derechos ARCO que, en su caso, correspondan.

El plazo que tiene el titular para realizar el pago no podrá ser menor de tres días contados a partir del día siguiente de que se notifique la repuesta.

Artículo 7. La Unidad de Transparencia tendrá a disposición del titular y, en su caso, de su representante los datos personales en el medio de reproducción solicitado y/o las constancias que acrediten el ejercicio efectivo de los derechos ARCO durante un plazo máximo de sesenta días, contados a partir del día siguiente en que se hubiere notificado la respuesta de procedencia al titular.

En caso de que el titular no acuda a la Unidad de Transparencia a concluir el procedimiento de atención de su solicitud de derechos ARCO, el Centro dará por concluida la atención a la solicitud y procederá a la destrucción del material en el que se reprodujeron los datos personales o de las constancias que acrediten el ejercicio efectivo de los derechos ARCO, dejando a salvo el derecho que le asiste al titular de presentar una nueva solicitud.

Artículo 8. La Unidad de Transparencia deberá dar vista al Órgano Interno de Control Específico del Conahcyt o a la Unidad Administrativa representante de este en el CIAD, respecto de cualquier responsabilidad administrativa atribuible a las personas servidoras públicas por incumplimiento de las obligaciones previstas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

V. PROCEDIMIENTO CON LOS TITULARES DE LOS DATOS PERSONALES

Artículo 9. La solicitud para el ejercicio de los derechos ARCO deberá contener la siguiente información:

I. Nombre del titular de los datos personales.

II. Documentos que acrediten la identidad del titular.

III. En su caso, nombre del representante del titular y documentos para acreditar su identidad y personalidad.

IV. Domicilio o cualquier medio para recibir notificaciones.

V. Descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCO, salvo que se trata del derecho de acceso.

VI. Descripción del derecho que se quiere ejercer o de lo que solicita el titular.

VII. En su caso, documentos o información que faciliten la localización de los datos personales.

Artículo 10. Además de la información general antes señalada, dependiendo del derecho que desee ejercer el titular de los datos personales, deberá incluir la siguiente información en la solicitud:

I. Derecho de **ACCESO**: la modalidad en la que prefiere que se reproduzcan los datos personales solicitados.

II. Derecho de **RECTIFICACIÓN**: las modificaciones que solicita que se realicen a los datos personales, así como aportar los documentos que sustenten la solicitud.

III. Derecho de **CANCELACIÓN**: las causas que motivan la petición de que se eliminen los datos de los archivos, registros o bases de datos del responsable del tratamiento.

IV. Derecho de **OPOSICIÓN**: las causas o la situación que lo llevan a solicitar que finalice el tratamiento de sus datos personales, así como el daño o perjuicio que le causaría que dicho tratamiento continúe; o bien, deberá indicar las finalidades específicas respecto de las cuales desea ejercer este derecho.

Si la información proporcionada resulta insuficiente para atenderla por no satisfacer alguno de los requisitos previstos en el artículo 52 de la Ley General, o bien, no proporcione los documentos para acreditar su identidad o representación legal, el Centro podrá solicitar la información faltante por medio de una prevención, la cual se deberá emitir en un plazo máximo de cinco días hábiles contados a partir del día siguiente de la presentación de la solicitud. El titular contará con un plazo de diez días para atender la prevención, contados a partir del día {siguiente al de la notificación, en caso contrario, se tendrá como no presentada la solicitud para el ejercicio de los derechos ARCO.

Artículo 11. Para acreditar la identidad del titular y, en su caso, la de su representante, así como la personalidad de este último, se seguirán las siguientes reglas:

A. Tratándose del titular de los datos personales.

I. Medios para acreditación de la identidad del titular mayor de edad y en pleno uso y goce de sus derechos (capacidad jurídica). Deberá presentar original de identificación oficial (credencial para votar, pasaporte, cédula profesional).

II. Medios para acreditación de la identidad de una persona menor de edad. Se podrá acreditar mediante acta de nacimiento, Clave Única de Registro de Población, credenciales expedidas por instituciones educativas o instituciones de seguridad social, pasaporte o cualquier otro documento oficial utilizado para tal fin.

III. Medios para acreditación de la identidad de una persona en estado de interdicción o incapacidad declarada. Se podrá acreditar mediante acta de nacimiento, Clave Única de Registro de Población, pasaporte o cualquier otro documento oficial utilizado para tal fin.

B. Tratándose del representante legal.

I. Cuando el titular mayor de edad y en pleno uso y goce de sus derechos (capacidad jurídica) ejerza sus derechos ARCO a través de su representante. Deberá presentar copia simple de la identificación oficial del titular, identificación oficial del representante e instrumento público; carta poder simple firmada ante dos testigos anexando copia simple de las identificaciones oficiales de quienes intervengan en la suscripción de este, o declaración en comparecencia personal del titular.

II. Cuando la persona menor de edad está representanta por los padres que ejercen la patria potestad. manifieste, bajo protesta de decir verdad, que el padre o la madre es quien ejerce la patria potestad del menor, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la patria potestad.

III. Cuando la persona menor de edad está representada por persona distinta a sus padres. Además de acreditar la identidad del titular, deberá presentar acta de nacimiento de la persona menor de edad, documento legal que acredite la posesión de la patria potestad, identificación oficial de quien ejerce la patria potestad (credencial para votar, pasaporte, cédula profesional) y carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la patria potestad del menor, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la patria potestad

IV. Cuando la persona menor de edad está representada por un tutor. Además de acreditar la identidad del titular, deberá presentar acta de nacimiento de la persona menor de edad, documento legal que acredite la tutela, identificación oficial del tutor (credencial para votar, pasaporte,

cédula profesional) y carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la tutela del menor, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la tutela.

V. Cuando la persona en estado de interdicción o incapacidad. Además de acreditar la identidad del titular, deberá presentar instrumento legal de designación del tutor, identificación oficial del tutor (credencial para votar, pasaporte, cédula profesional) y carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la tutela del menor, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la tutela.

VI. Cuando el titular de los datos personales es una persona fallecida. La persona que acredite tener un interés jurídico deberá presentar ante el Centro, acta de defunción del titular, documentos que acrediten el interés jurídico de quien pretende ejercer el derecho, y documento de identificación oficial de quien solicita el ejercicio de los derechos ARCO (credencial para votar, pasaporte, cédula profesional). Por interés jurídico se entiende aquel que tiene una persona física que, con motivo del fallecimiento del titular, pretende ejercer los derechos ARCO de éste, para el reconocimiento de derechos sucesorios, atendiendo a la relación de parentesco por consanguinidad o afinidad que haya tenido con el titular, el cual se acreditará en términos de las disposiciones legales aplicables. Puede alegar interés jurídico, de manera enunciativa más no limitativa, el albacea, herederos, legatarios, familiares en línea recta sin limitación de grado y en línea colateral hasta el cuarto grado, lo que se acreditará con copia simple del documento delegatorio, pasado ante la fe de notario público o suscrito ante dos testigos.

Artículo 12. El Centro deberá atender la solicitud de ejercicio de derechos ARCO, conforme a lo siguiente:

a. En un plazo no mayor de veinte días hábiles, contados a partir del día siguiente a la recepción de la solicitud, informándole si procede o no el ejercicio del derecho solicitado. Dicho plazo podrá ser ampliado por una sola vez, hasta por diez días cuando así lo justifiquen las circunstancias, y siempre y cuando se le notifique al titular dentro del plazo de respuesta.
b. En caso de que haya procedido el ejercicio del derecho, el Centro deberá llevar a cabo las acciones necesarias para hacerlo efectivo, en un plazo no mayor a quince días hábiles, contados a partir del día siguiente en el que le haya notificado la respuesta anterior.

Artículo 13. El ejercicio de los derechos ARCO es GRATUITO, y sólo podrán realizarse cobros para recuperar los costos de reproducción, certificación o envío de información, bajo las siguientes reglas:

a. Cuando el titular proporcione medio magnético, electrónico o el mecanismo necesario para la reproducción de los datos personales (ejemplo: USB o CD), éstos deberán ser entregados sin costo.
b. La información deberá ser entregada sin costo cuando implique la entrega de no más de 20 hojas simples o certificadas.

Artículo 14. Si la normatividad aplicable al tratamiento de datos personales en cuestión establece un trámite o procedimiento específico para el ejercicio de los derechos ARCO, el sujeto obligado le deberá informar la existencia de dicho trámite o procedimiento en un plazo máximo de cinco días hábiles, contados a partir del día siguiente de la presentación de la solicitud, a fin de que el titular decida si presentará su solicitud de acuerdo con el trámite específico o con base en el procedimiento descrito en el presente documento.

Artículo 15. Cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos. Cuando el titular haya facilitado los datos personales y el tratamiento se base en el consentimiento o en un contrato, tendrá derecho a transmitir dichos datos personales y cualquier otra información que haya facilitado y que se conserve en un sistema de tratamiento automatizado a otro sistema en un formato electrónico comúnmente utilizado, sin impedimentos por parte del responsable del tratamiento de quien se retiren los datos personales.

Artículo 16. Se entenderá que un formato adquiere la calidad de estructurado y comúnmente utilizado, con independencia del sistema informático utilizado para su generación y reproducción, cuando se cumplan todos los siguientes supuestos:

I. Se trate de un formato electrónico accesible y legible por medios automatizados, de tal forma que éstos puedan identificar, reconocer, extraer, explotar o realizar cualquier otra operación con datos personales específicos;
II. El formato permita la reutilización y/o aprovechamiento de los datos personales, y
III. El formato sea interoperable con otros sistemas informáticos

Datos de autorización
30 de mayo de 2024

El presente documento fue aprobado por el Comité de Transparencia del CIAD, en la Tercera Sesión Extraordinaria 2024, de fecha 31 de mayo de dos mil veinticuatro.

Mtra. María Guadalupe Sánchez Soto

Titular de la Unidad de Transparencia y Presidenta del Comité de Transparencia.

Lic. Alejandro Salinas Ochoa

Titular de la Unidad Administrativa del Órgano Interno de Control Específico en el Conahcyt en el Centro de Investigación en Alimentación y Desarrollo, A.C.

Dr. Rogerio Rafael Sotelo Mundo

Coordinador de Investigación