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 aquéllas 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

Carretera Gustavo Enrique Astiazarán Rosas, No. 46, Col. La Victoria, CP. 83304, Hermosillo, Sonora, México.
Tel. 662 289 2400 www.ciad.mx