CONAHCYT
CONSEJO NACIONAL DE HUMANIDADES CIENCIAS Y TECNOLOGÍAS

50 ANIVERSARIO CIDE

CENTRO DE INVESTIGACIÓN Y DOCENCIA ECONÓMICAS A.C.

# Documento de Seguridad para la Protección de Datos Personales del Centro de Investigación y Docencia Económicas, A.C. (CIDE)

Unidad de Transparencia CIDE

5 de diciembre de 2024

## Tabla de contenido

Documento de Seguridad para la Protección de Datos Personales del Centro de Investigación y Docencia Económicas, A.C. (CIDE) ..... 2
Marco Jurídico ..... 2
Glosario de Términos ..... 2
Personas de quienes se obtienen datos personales ..... 4
Transferencia de los datos personales ..... 6
Bases de datos personales del CIDE ..... 7
Funciones y obligaciones de las personas que tratan datos personales ..... 7
Registro de incidencias que comprometan la seguridad de los datos personales ..... 8
Medidas de seguridad físicas, administrativas y técnicas ..... 8
Análisis de riesgo ..... 8
Análisis de brecha ..... 9
Mecanismos de monitoreo y revisión de las medidas de seguridad ..... 9
PLAN DE TRABAJO ..... 9
Capacitación continua para el manejo y protección de datos personales en el CIDE ..... 9
Actualización del documento de seguridad ..... 9

## Documento de Seguridad para la Protección de Datos Personales del Centro de Investigación y Docencia Económicas, A.C. (CIDE)

Este documento describe las medidas de seguridad administrativas, físicas y técnicas que se aplican a los sistemas de tratamiento de datos personales en el Centro de Investigación y Docencia Económicas A.C. (CIDE). Su objetivo es asegurar la integridad, confidencialidad y disponibilidad de la información personal. Además, identifica los sistemas de tratamiento de datos personales en la institución, el tipo de datos que contienen, los responsables y las medidas de seguridad implementadas.

El objetivo de este documento es implementar y mantener medidas de seguridad administrativas, físicas y técnicas que protejan los datos personales bajo la custodia del CIDE, cumpliendo con los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en su tratamiento.

## Marco Jurídico

El presente instrumento se regula por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), específicamente su capítulo II, artículo 35, que establece un conjunto mínimo de medidas de seguridad que el CIDE deberá considerar al determinar su estrategia de seguridad para la protección de datos personales

## Glosario de Términos

- **Bases de Datos:** Conjunto ordenado de datos personales en posesión del responsable, ya sea en formato escrito, impreso, digital, sonoro, visual, electrónico, informático u holográfico, referentes a una persona física identificada o identificable.
- **Datos Personales:** Información numérica, alfabética, gráfica, fotográfica, acústica, o de cualquier otro tipo concerniente a una persona física identificada o identificable.
- **Derechos ARCO**: Derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.
- **Documento de Seguridad**: Instrumento formal que describe las medidas técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.
- **CIDE**: Centro de Investigación y Docencia Económicas A.C.
- **Inventario de Datos Personales:** Lista ordenada y detallada que posee el responsable o encargado, de cualquier información numérica, alfabética,

gráfica, fotográfica, acústica, o de cualquier otro tipo, concerniente a una persona física identificada o identificable.

- **Ley:** Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- **Medidas de Seguridad:** Conjunto detallado de acciones, actividades o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.
- **Medidas de Seguridad Físicas:** Conjunto ordenado y detallado de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento, previniendo el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información.
- **Medidas de Seguridad Técnicas:** Conjunto ordenado y detallado de acciones, mecanismos y sistemas destinados a proteger los datos personales y los recursos involucrados en su tratamiento, incluyendo la revisión y gestión de la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.
- **Nube:** Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro flexible de infraestructura, plataforma o software, a través de procedimientos virtuales, utilizando recursos compartidos y dinámicamente ajustables.
- **Titular:** La persona física a la que pertenecen los datos personales.
- **Tratamiento:** Cualquier operación o conjunto de operaciones realizadas sobre los datos personales, ya sea por medios manuales o automatizados.
- **Tratamiento:** Cualquier operación o conjunto de operaciones realizadas sobre los datos personales, mediante procedimientos manuales o automatizados, que incluyen su obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, publicación, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición.

A continuación, se presentan las categorías de datos personales que el CIDE administra, organizadas por las áreas responsables de su gestión y protección.

- **Datos de identificación y contacto:** Nombre de los servidores públicos, familiares, dependientes económicos y/o beneficiarios, alumnos, y personas físicas proveedoras de bienes y servicios; estado civil; RFC; CURP; visa de residencia temporal o permanente; lugar y fecha de nacimiento; nacionalidad; domicilio; teléfono particular y celular; correo electrónico; firma autógrafa y/o electrónica; edad; fotografía; huella digital y referencias personales.

a) **Datos personales:** Puesto o cargo desempeñado, domicilio de trabajo, correo electrónico institucional, teléfono institucional, Curriculum Vitae, capacitación laboral y número de seguridad social.

b) **Datos académicos:** Trayectoria educativa, título, cédula profesional, certificados, calificaciones, número de matrícula, constancias y reconocimientos, proyectos de investigación, escuela de procedencia, salón y horario de clases.

c) **Datos Patrimoniales y/o Financieros:** Ingresos, CFDI's, códigos QR, percepciones y deducciones, datos de cuentas bancarias, situación fiscal, préstamos, bienes inmuebles y muebles, y vehículos con datos de identificación.

d) **Datos Legales:** Situación jurídica de las personas, incluyendo juicios, procedimientos administrativos y pensiones alimenticias.

e) **Datos de Salud:** Tipo de sangre, seguro de gastos médicos mayores, estado de salud físico y/o mental, y procedimientos quirúrgicos.

f) **Datos personales de Naturaleza Pública:** Datos que, conforme a la normatividad en materia de transparencia, están sujetos a acceso público.

**Personas de quienes se obtienen datos personales**

a) Personas que laboran en el CIDE.
b) Aspirantes, estudiantes y egresados del CIDE.
c) Familiares, dependientes económicos y/o beneficiarios.
d) Personas físicas que proveen o prestan servicios al CIDE.
e) Personas interesadas que participan en actividades académicas del CIDE.
f) Personas que adquieren publicaciones del CIDE.

Para proteger los datos personales almacenados en bases de datos físicas o electrónicas, se implementan medidas de seguridad. Estas medidas garantizan el cumplimiento de los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, conforme al artículo 16 de la Ley. Además, cumplen con los deberes de seguridad y confidencialidad establecidos en los artículos 31 y 42.

**Principio de Licitud:** Consiste en la obligación del responsable de realizar el tratamiento de datos personales de acuerdo con las facultades y atribuciones conferidas por la normativa aplicable.

**Principio de Finalidad:** Implica que todo tratamiento de datos personales realizado por el responsable debe estar justificado por finalidades concretas, lícitas, explícitas y legítimas, en consonancia con las atribuciones expresas conferidas por la normativa aplicable (Artículo 18 LGPDPPSO). El responsable puede modificar las finalidades del tratamiento inicialmente establecidas en el aviso de privacidad, siempre que tenga atribuciones legales para ello y obtenga nuevamente el consentimiento del titular.

**Principio de Lealtad:** Implica que el responsable no debe obtener ni tratar datos personales mediante medios engañosos o fraudulentos, priorizando la protección de los intereses del titular y respetando su expectativa razonable de privacidad.

**Principio de consentimiento:** Consiste en la obligación del responsable de obtener la autorización o consentimiento del titular para el tratamiento de sus datos personales, especialmente cuando se trata de datos sensibles. Este principio permite a los titulares decidir de manera informada, libre, inequívoca y específica si desean compartir su información y qué datos compartirán.

El consentimiento puede ser otorgado por el titular de datos personales al responsable en dos modalidades distintas:

**a) Expreso:** Se presenta cuando la voluntad del titular se manifiesta de manera verbal, por escrito, mediante medios electrónicos, ópticos, signos inequívocos o cualquier otra tecnología aceptada.

**b) Tácito:** Se presenta cuando, tras haber puesto el aviso de privacidad a disposición del titular, éste no expresa su voluntad en sentido contrario. Por regla general, el consentimiento tácito es válido, salvo que la ley o las disposiciones aplicables exijan una manifestación expresa de la voluntad del titular. En el caso de datos personales sensibles, el consentimiento debe ser expreso y por escrito, ya sea mediante firma autógrafa, firma electrónica o cualquier mecanismo de autenticación establecido.

**Principio de calidad:** Consiste en la obligación del responsable de adoptar las medidas necesarias para mantener los datos personales exactos, completos, correctos y actualizados. Esta obligación busca asegurar que los datos bajo su resguardo y posesión no pierdan veracidad y se mantengan adecuados para cumplir con las finalidades concretas, explícitas, lícitas y legítimas que motivaron su tratamiento. Se presume que se cumple con el principio de calidad cuando los datos son proporcionados directamente por el titular, hasta que éste no manifieste y acredite lo contrario.

**Principio de proporcionalidad:** Se refiere a la obligación del responsable de tratar únicamente los datos personales que sean adecuados, relevantes y estrictamente necesarios para la finalidad concreta, explícita, lícita y legítima que justifica su tratamiento.

**Principio de información:** Implica que el responsable debe informar al titular, a través del aviso de privacidad, sobre la existencia y las características principales del tratamiento al que serán sometidos sus datos personales, para que el titular pueda tomar decisiones informadas. Por regla general, el aviso de privacidad deberá ser difundido mediante los medios electrónicos y físicos disponibles para el responsable. Para cumplir eficazmente su función informativa, el aviso de privacidad debe estar redactado y estructurado de manera clara y sencilla.

**Principio de responsabilidad:** Se traduce en la obligación del responsable de implementar mecanismos de protección y seguridad en el tratamiento de datos personales, incluyendo: destinar recursos autorizados para desarrollar programas y políticas de protección de datos; llevar a cabo un programa de capacitación y actualización del personal sobre sus obligaciones y deberes en esta área; revisar periódicamente las políticas y programas de seguridad de datos personales; establecer un sistema de supervisión y vigilancia interna y/o externa sobre dichas políticas; crear procedimientos para recibir y responder a dudas y quejas de los titulares; y diseñar, desarrollar e implementar políticas públicas, programas, servicios, sistemas, plataformas informáticas, aplicaciones electrónicas u otras tecnologías que impliquen el tratamiento de datos personales, asegurando que estos cumplan por defecto con las obligaciones establecidas en la Ley y la normativa aplicable.

**Deber de seguridad:** Implica que los titulares de los datos personales tienen el derecho a que la información que proporcionan a los responsables sea protegida mediante medidas de seguridad adecuadas, que prevengan su pérdida, alteración, destrucción, daño, o uso, acceso o tratamiento no autorizado. En consecuencia, los responsables están obligados a almacenar los datos personales en bases de datos protegidas mediante medidas de seguridad administrativas, físicas y técnicas.

**Deber de confidencialidad:** Consiste en la obligación del responsable de implementar controles o mecanismos para asegurar que todas las personas involucradas en cualquier fase del tratamiento de los datos personales mantengan la confidencialidad de dicha información. Esta obligación de confidencialidad perdurará incluso después de que dichas personas hayan concluido su relación con el responsable.

## Transferencia de los datos personales

Toda transferencia de datos personales ya sea nacional o internacional, está sujeta al consentimiento del titular, salvo en las excepciones previstas en los artículos 22, 66 y 70 de la Ley.

## Bases de datos personales del CIDE

- Sistema integral de personal, credencialización y nómina.
- Expedientes de alumnos.
- Sistema de correo electrónico.
- Sistema de mobiliario y equipo de cómputo.
- Sistema de administración de biblioteca.
- Sistema de integración financiera.
- Sistema de compras y servicios.
- Expedientes clínicos.

## Funciones y obligaciones de las personas que tratan datos personales

Las áreas encargadas de tratar datos personales son las siguientes:

- Administración Escolar.
- Becas y Apoyos Financieros.
- Biblioteca y Servicios de Información.
- Coordinación de Administración y Finanzas.
- Dirección de Recursos Materiales y Servicios Generales.
- Oficina de exalumnos.
- Oficina de Internacionalización Educativa.
- Recursos Financieros.
- Recursos Humanos.
- Servicios Médicos (Enfermería)

Las personas que ocupan los puestos en las áreas previamente mencionadas tienen las siguientes funciones y obligaciones:

a) Garantizar la seguridad en el tratamiento de datos personales es una prioridad fundamental, con el propósito de mitigar riesgos como la pérdida, robo, alteración o acceso no autorizado.
b) Asegurar la adecuada protección de los datos personales, de acuerdo con lo establecido en la legislación vigente y las disposiciones pertinentes en la materia.
c) Implementar medidas de seguridad, tanto físicas como técnicas y administrativas, que sean apropiadas para proteger los datos personales de la comunidad institucional y de terceros relacionados con la misma.
d) Asegurar la confidencialidad de los datos personales en virtud de los procedimientos bajo su responsabilidad.
e) Mantener actualizado el inventario de datos personales.
f) Conocer y aplicar las medidas y procedimientos estipulados en el presente documento de seguridad.
g) Asegurar el cumplimiento de los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO) de los titulares de los datos personales.

h) Realizar copias de seguridad de los datos personales bajo su custodia.

## Registro de incidencias que comprometan la seguridad de los datos personales

El registro de incidencias deberá incluir los siguientes elementos esenciales:

1. **Fecha de la Incidencia:** Especificar el día, mes y año en que ocurrió la incidencia.
2. **Tipo de Incidencia:** Categorizar la incidencia según su naturaleza (por ejemplo, técnica, administrativa, de seguridad, etc.).
3. **Descripción:** Proporcionar una descripción detallada y clara de los hechos relacionados con la incidencia.
4. **Persona que Registra:** Indicar el nombre y cargo de la persona que está documentando la incidencia.
5. **Persona a Quien se Comunica:** Registrar el nombre y cargo de la persona a quien se notifica la incidencia.
6. **Consecuencias:** Detallar las posibles consecuencias derivadas de la incidencia, incluyendo cualquier impacto en las operaciones o en la seguridad.

## Medidas de seguridad físicas, administrativas y técnicas

Las áreas encargadas del tratamiento de datos personales deberán implementar un control riguroso sobre el acceso a sus bases de datos, tanto físicas como electrónicas. Es esencial que se establezcan y mantengan medidas de seguridad adecuadas para garantizar la confidencialidad e integridad de la información almacenada. Esto incluye, pero no se limita a, controles de acceso físicos y electrónicos, políticas de protección de datos y procedimientos para la gestión segura de la información.

Estas medidas deben asegurar que solo el personal autorizado tenga acceso a los datos personales y que cualquier riesgo potencial para la confidencialidad e integridad de la información sea mitigado de manera efectiva.

## Análisis de riesgo

### Información Reservada

De acuerdo con el Artículo 113 de la Ley General de Transparencia y Acceso a la Información Pública, la información clasificada como "reservada" no debe ser publicada debido a su potencial para comprometer la seguridad del CIDE. Esta clasificación se aplica a la información que detalla medidas de seguridad físicas,

administrativas y técnicas, cuyo acceso público podría poner en riesgo la integridad y protección de las medidas implementadas para salvaguardar la institución.

### Análisis de brecha

**Información Reservada**
De acuerdo con el Artículo 113 de la Ley General de Transparencia y Acceso a la Información Pública, la información clasificada como "reservada" no debe ser publicada debido a su potencial para comprometer la seguridad del CIDE. Esta clasificación se aplica a la información que detalla medidas de seguridad físicas, administrativas y técnicas, cuyo acceso público podría poner en riesgo la integridad y protección de las medidas implementadas para salvaguardar la institución.

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

**Información Reservada**
De acuerdo con el Artículo 113 de la Ley General de Transparencia y Acceso a la Información Pública, la información clasificada como "reservada" no debe ser publicada debido a su potencial para comprometer la seguridad del CIDE. Esta clasificación se aplica a la información que detalla medidas de seguridad físicas, administrativas y técnicas, cuyo acceso público podría poner en riesgo la integridad y protección de las medidas implementadas para salvaguardar la institución.

## PLAN DE TRABAJO

### Capacitación continua para el manejo y protección de datos personales en el CIDE.

El personal del CIDE que maneja datos personales deberá participar en programas de capacitación continua para asegurar el adecuado manejo y protección de esta información. Estos programas incluirán cursos y talleres, tanto presenciales como en línea, ofrecidos por entidades especializadas como el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el Archivo General de la Nación, entre otras instituciones relevantes. La participación en estas actividades formativas es esencial para mantener al personal actualizado sobre las mejores prácticas y normativas vigentes en materia de protección de datos personales.

### Actualización del documento de seguridad

El presente documento de seguridad se actualizará en los siguientes casos:

1. **Modificaciones Sustanciales en el Tratamiento de Datos Personales:** Cuando se produzcan cambios significativos en el tratamiento de datos personales que impliquen una alteración en el nivel de riesgo asociado.

2. **Proceso de Mejora Continua:** Como resultado de un proceso de mejora continua, derivado del monitoreo y la revisión periódica del sistema de gestión de seguridad de datos.
3. **Acciones Correctivas y Preventivas:** Tras la implementación de medidas correctivas y preventivas en respuesta a una vulneración de seguridad.
4. **Recomendaciones y Documentación Oficial:** Cuando se aprueben nuevos documentos, recomendaciones o formatos por parte del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Estas actualizaciones garantizarán que el documento de seguridad se mantenga vigente y en consonancia con las mejores prácticas y requisitos normativos aplicables.