POLÍTICAS DE GESTIÓN DE DATOS PERSONALES DEL CENTRO DE INVESTIGACIÓN Y DOCENCIA ECONÓMICAS, A.C. (CIDE)

Introducción

El Centro de Investigación y Docencia Económicas, A.C. (CIDE) se compromete a proteger y gestionar de manera adecuada la información personal que recaba en el ejercicio de sus actividades académicas, de investigación y administrativas. La presente Política de Gestión de Datos Personales establece los lineamientos y procedimientos para la recolección, uso, almacenamiento y disposición de datos personales, con el objetivo de asegurar el cumplimiento de la normativa vigente en materia de protección de datos.

Fundamento Legal

La presente política se fundamenta en la legislación aplicable en materia de protección de datos personales, particularmente en:

1. Constitución Política de los Estados Unidos Mexicanos: El artículo 16 de la Constitución Mexicana establece el derecho a la protección de datos personales como parte del derecho a la privacidad, garantizando que la recolección y tratamiento de datos personales se realice de conformidad con las disposiciones legales y con el respeto a la privacidad de los individuos.
2. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPSO): Esta ley regula el tratamiento de datos personales por parte de los particulares, estableciendo las obligaciones que deben cumplir las entidades que gestionan estos datos para garantizar su protección y el respeto a los derechos de los titulares de estos.

Objetivo

Establecer los principios generales para el tratamiento y protección de datos personales que deben seguir las personas servidoras públicas del (CIDE), garantizando el cumplimiento de las normativas vigentes y la salvaguarda de la privacidad y seguridad de la información.

Ámbito de aplicación

Las presentes políticas son de aplicación obligatoria para todas las áreas del. (CIDE) que gestionen datos personales. Esto incluye, sin limitación, todas las modalidades de creación, tipos de soportes (tanto físicos como electrónicos), así

como los procesos de tratamiento, procesamiento, almacenamiento y organización de dicha información.

Vigencia y Difusión

Las presentes políticas entrarán en vigor a partir del día hábil siguiente a su publicación en la página Web de Transparencia del CIDE y en los formatos establecidos para tal efecto por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). La difusión de estas políticas se realizará a través de los canales institucionales correspondientes para asegurar su conocimiento y cumplimiento por parte de todas las áreas y personas servidoras públicas del CIDE.

Para efectos de las presentes políticas se entenderá por:

Áreas: aquellas instancias del Centro de Investigación y Docencia Económicas, A.C. (CIDE) definidas en los reglamentos interiores, estatutos orgánicos o documentos equivalentes, que tienen la responsabilidad de gestionar, tratar o custodiar datos personales. Estas áreas son responsables del manejo, procesamiento y protección de la información personal en conformidad con las políticas establecidas y las normativas aplicables.

Amenaza: En el contexto de datos personales, una amenaza es un evento o circunstancia que puede causar un incidente que comprometa la protección y seguridad de la información personal.

Aviso de Privacidad: Documento proporcionado al titular de datos personales, ya sea en formato físico, electrónico o cualquier otro medio generado por el responsable, desde el momento de la recolección de sus datos. Su propósito es informar al titular sobre los fines y condiciones del tratamiento de su información personal.

Base de Datos: Conjunto organizado de datos personales de una persona física identificada o identificable, estructurado según criterios específicos, independientemente de la forma de creación, soporte, procesamiento, almacenamiento u organización.

Bloqueo: Proceso mediante el cual los datos personales se identifican y conservan después de haber cumplido la finalidad para la que fueron recabados. Este proceso se realiza con el único fin de determinar posibles responsabilidades relacionadas con su tratamiento, durante el plazo de prescripción legal o contractual. Durante

este periodo, los datos no pueden ser objeto de tratamiento. Una vez transcurrido el plazo, los datos se cancelan de la base de datos correspondiente.

Comité de Transparencia: Órgano mencionado en el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública, encargado de supervisar y garantizar el cumplimiento de las obligaciones de transparencia y acceso a la información en la organización.

Cómputo en la Nube: Modelo de provisión externa de servicios de computación bajo demanda, que ofrece infraestructura, plataformas o aplicaciones informáticas de manera flexible y dinámica, a través de recursos compartidos virtualmente.

Ciclo de Vida: Conjunto de fases del tratamiento de datos personales, que abarca desde la obtención y almacenamiento, hasta el uso, divulgación, bloqueo y cancelación de los datos.

Datos Personales: Cualquier información relativa a una persona física identificada o identificable. Una persona física es identificable si su identidad puede determinarse directa o indirectamente a través de información como nombre, número de identificación, datos de localización, identificador en línea, o cualquier elemento relacionado con su identidad física, fisiológica, genética, psíquica, patrimonial, económica, cultural o social.

Derechos ARCO: Derechos que permiten a los titulares de datos personales solicitar el acceso, la rectificación, la cancelación y la oposición al tratamiento de sus datos.

Encargado: Persona física o jurídica, pública o privada, ajena a la organización del responsable, que trata datos personales en nombre y por cuenta del responsable.

Exposición al Riesgo: Situación en la que un activo (datos personales) está potencialmente vulnerable a una amenaza, en caso de que esta se materialice.

Garantía de la Seguridad de la Información: Implementación de medidas administrativas, físicas y técnicas eficaces para asegurar la integridad, confidencialidad y disponibilidad de los datos personales.

Impacto: Consecuencia resultante de la materialización de una amenaza sobre los datos personales.

Inventario de Datos Personales: Identificación y documentación de las bases de datos gestionadas por las unidades administrativas, incluyendo información básica sobre cada tratamiento realizado y el ciclo de vida de los datos personales, independientemente de su forma de almacenamiento.

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

Medidas de Seguridad: Conjunto de acciones, controles y mecanismos administrativos, técnicos y físicos destinados a proteger los datos personales y los sistemas que los gestionan.

Medidas de Seguridad Administrativas: Políticas y procedimientos para la gestión de la seguridad de la información, incluyendo la identificación, clasificación y eliminación segura de datos, así como la sensibilización y capacitación del personal en protección de datos personales.

Medidas de Seguridad Físicas: Acciones y mecanismos diseñados para proteger el entorno físico donde se almacenan y procesan los datos personales, así como los recursos involucrados en su tratamiento.

Medidas de Seguridad Técnicas: Conjunto de acciones y mecanismos basados en tecnología, tanto de hardware como de software, destinados a proteger el entorno digital de los datos personales y los recursos asociados a su tratamiento.

Órgano Garante: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, encargado de supervisar y garantizar el cumplimiento de las normativas de protección de datos en México.

Portabilidad de Datos Personales: Derecho de los titulares de datos personales para recibir, bajo las condiciones establecidas por la normativa aplicable, sus datos en un formato estructurado, de uso común y lectura mecánica, y para transmitirlos a otro responsable del tratamiento sin impedimentos.

Principios: Directrices fundamentales que regulan el derecho a la protección de datos personales, traducidas en obligaciones específicas: licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.

Remisión: Comunicación de datos personales realizada exclusivamente entre el responsable y el encargado del tratamiento, ya sea dentro o fuera del territorio mexicano.

Responsable: Entidades sujetas a lo estipulado en el artículo 1 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, que toman decisiones sobre el tratamiento de datos personales.

Riesgo: Posibilidad o probabilidad de que ocurra un daño o impacto negativo sobre los datos personales.

Supresión: Proceso de baja archivística de los datos personales conforme a la normativa aplicable, que implica su eliminación, borrado o destrucción, siguiendo las medidas de seguridad previamente establecidas por el responsable.

Titular de la Unidad Administrativa: Persona responsable del tratamiento de los datos personales en la unidad administrativa a su cargo.

Titular: Persona física a quien pertenecen los datos personales.

Transferencia: Comunicación de datos personales, ya sea dentro o fuera del territorio mexicano, realizada a una persona distinta del titular, del responsable o del encargado.

Tratamiento: Cualquier operación o conjunto de operaciones realizadas sobre datos personales mediante procedimientos manuales o automatizados, que incluyen la obtención, uso, registro, organización, conservación, elaboración, comunicación, difusión, almacenamiento, posesión, acceso, cotejo, interconexión, manejo, aprovechamiento, divulgación, transferencia, supresión, destrucción o disposición de datos personales.

Usuario: Persona autorizada por el responsable y parte de la organización del sujeto obligado, que realiza el tratamiento y/o tiene acceso a los datos y/o a los sistemas de datos personales.

Vulneración: Debilidades o fallos en los activos (datos personales) que pueden ser explotados por amenazas para causar daño.

DISPOSICIONES GENERALES

1. Los datos personales tratados por el Centro de Investigación y Docencia Económicas, A.C. (CIDE), en el ejercicio de sus atribuciones, deberán ser protegidos de conformidad con lo establecido en la Ley General y en los Lineamientos aplicables, asegurando su seguridad, confidencialidad e integridad.

2. En el tratamiento de datos personales por parte del CIDE, se deberán observar los principios de licitud, lealtad, información, consentimiento, calidad, finalidad, proporcionalidad y responsabilidad, así como cumplir con los deberes de seguridad y confidencialidad establecidos por la normativa aplicable.

3. En el tratamiento de datos personales de menores de edad, el CIDE deberá priorizar el interés superior de las infancias y adolescencias, de conformidad con las disposiciones establecidas en la Ley General de los Derechos de Niñas, Niños y Adolescentes. Esta prioridad implica asegurar que el tratamiento de dichos datos se realice de manera que proteja y promueva el bienestar integral de los menores.

4. Los datos personales solo podrán ser tratados por el CIDE conforme a las atribuciones o facultades que le correspondan de acuerdo con la normatividad vigente y aplicable. En consecuencia, el tratamiento de dichos datos deberá estar justificado por finalidades concretas, lícitas, explícitas y

legítimas, asegurando que se ajusten a los propósitos establecidos y autorizados por la normativa.

5. Los titulares de las unidades administrativas que recaben datos personales serán responsables de elaborar y utilizar el aviso de privacidad, ya sea integral o simplificado. Este aviso deberá informar a los titulares sobre las finalidades y tratamiento de sus datos personales (incluyendo los sensibles), la posible transferencia de datos (especificando destinatarios y fines), y los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, así como las características principales del tratamiento.

6. Los avisos de privacidad deberán ser aprobados por el Comité de Transparencia y se difundirán a los titulares de datos tanto de manera física en las áreas correspondientes como electrónicamente en la página institucional de transparencia, en el apartado de Protección de Datos Personales.

7. El CIDE deberá solicitar al titular de los datos, ya sea de manera tácita o expresa, el consentimiento para la obtención y uso de sus datos personales, excepto en los casos previstos como excepciones por la Ley General.

8. En el caso de datos personales sensibles, el consentimiento para su tratamiento deberá ser expreso y por escrito, y deberá ser autenticado mediante un mecanismo autorizado que permita identificar al titular de manera plena.

9. En el tratamiento de datos personales, se deberá garantizar que dichos datos sean exactos, completos, correctos y actualizados para cumplir con los fines para los cuales fueron obtenidos.

10. Las áreas del CIDE deben borrar o eliminar la documentación y bases de datos que contengan datos personales una vez que estos ya no sean necesarios para las finalidades originales o haya vencido el plazo de conservación estipulado en el Catálogo de Disposición Documental vigente.

11. Las finalidades para las cuales se recaben los datos personales deben ser específicas y necesarias, informando claramente su uso y evitando en todo momento finalidades secundarias o no indispensables.

12. Las áreas del CIDE solo podrán solicitar datos personales que sean necesarios, adecuados y relevantes para cumplir con las facultades o atribuciones que la normativa aplicable les confiere, y procurarán solicitar el menor número de datos posibles.

13. Las personas servidoras públicas que recaben datos personales deberán estar plenamente identificadas ante los titulares.

14. Las áreas del CIDE deberán tener debidamente identificadas a las personas que, en el ejercicio de sus funciones, puedan realizar tratamiento de datos personales, garantizando la restricción de acceso a terceros no autorizados.

15. Las personas que, en virtud de su empleo, cargo o comisión, tengan acceso a datos personales en medios electrónicos deberán utilizar contraseñas seguras, las cuales no podrán ser compartidas con terceros.

16. Los datos personales contenidos en medios físicos deberán ser resguardados bajo llave en espacios que garanticen su adecuada conservación.

17. Los documentos de oficina que contengan datos personales no podrán ser utilizados como papel de doble uso.

18. Las personas que, en virtud de su empleo, cargo o comisión, tengan acceso a datos personales no podrán reproducirlos ni difundirlos por ningún medio, ya sea físico o electrónico, a menos que sea necesario para el desempeño de sus funciones.

19. Los datos personales deberán ser tratados con confidencialidad, lo que implica la obligación de mantener secreto, discreción y custodia por parte de quienes manejan, usan, recaban, utilizan o transfieren dichos datos. Estos no podrán difundirse ni compartirse con terceros, salvo que se cuente con el consentimiento del titular o exista una obligación normativa que requiera su difusión.

20. Cuando sea necesario remitir datos personales a otras áreas del CIDE, se deberá comunicar por escrito que la información corresponde a datos personales, especificar las finalidades de la entrega y subrayar la obligación de mantener la confidencialidad de dichos datos.

21. La transferencia de datos personales a otros sujetos obligados del sector público podrá realizarse siempre y cuando los datos se utilicen para el ejercicio de facultades propias, compatibles y análogas con la finalidad que motivó el tratamiento inicial. Esta transferencia deberá realizarse en estricta observancia de los preceptos establecidos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y sus Lineamientos.

22. Los datos personales en poder del CIDE podrán ser utilizados con fines estadísticos, asegurando la disociación de los datos para evitar la identificación de las personas involucradas en los informes generados.

23. Las personas servidoras públicas adscritas a las áreas del CIDE que participen en el tratamiento de datos personales, deberán cumplir con la capacitación en materia de protección de datos personales señalada en el Plan Anual de Capacitación en Materia de Datos Personales que apruebe el Comité de Transparencia.

24. Los titulares de las áreas que traten datos personales deberán informar al Titular de la Unidad de Transparencia sobre cualquier vulneración de seguridad que se presente, así como sobre las acciones tomadas en respuesta. De ser necesario se notificará al Comité de Transparencia y a los titulares afectados para que puedan tomar las medidas necesarias para la defensa de sus derechos.

DISPOSICIONES DE SEGURIDAD

Medidas de Seguridad Físicas:

a) Control de Acceso a Áreas Sensibles: Se deberá implementar controles físicos estrictos para evitar el acceso no autorizado a áreas donde se almacenan datos personales, tales como oficinas, salas de servidores y archivos.

b) Protección de Equipos y Soportes Físicos: Los equipos que almacenan datos personales, así como cualquier soporte físico (como discos duros y documentos en papel), deberán ser asegurados adecuadamente para prevenir daños, pérdida o robo.

c) Seguridad de Recursos Móviles y Portátiles: Los dispositivos móviles y portátiles que contienen datos personales deberán ser protegidos mediante medidas físicas como bloqueos de seguridad y controles de inventario para evitar su extravío o uso indebido.

d) Mantenimiento y Supervisión de Infraestructura: Los sistemas y equipos físicos que almacenan o procesan datos personales deberán recibir mantenimiento regular para garantizar su correcto funcionamiento. Se deberán realizar revisiones periódicas de las instalaciones físicas para identificar y corregir posibles vulnerabilidades en la infraestructura de seguridad.

Medidas de Seguridad Administrativas:

a) Confidencialidad del Usuario: La persona usuaria deberá garantizar la confidencialidad de los datos personales que se encuentren bajo su custodia o aquellos que tenga acceso debido a su empleo, cargo o comisión, y no deberá comunicar dicha información a terceros no autorizados, incluso después de la finalización de la relación laboral con el Instituto.

b) **Resguardo de Documentos:** Se deberá asegurar que cualquier documento que contenga datos personales esté adecuadamente resguardado en todo momento para evitar el acceso no autorizado por parte de terceros.

c) **No Reutilización de Documentos:** No se deberá reutilizar hojas o documentos que contengan datos personales, para evitar la posible divulgación accidental de información confidencial.

d) Uso de Dispositivos Personales: No se deberá utilizar dispositivos personales, tales como celulares, cámaras fotográficas u otros, para captar, reproducir o difundir datos personales.

e) Acceso Restringido: Solo el personal autorizado podrá acceder a documentos que contengan datos personales.

f) Registro de Accesos: Se deberá registrar quién accede a los archivos bajo custodia de cualquier persona servidora pública para garantizar el control de acceso.

g) Bloqueo y Apagado de Equipos: Los equipos deberán ser bloqueados cuando la persona servidora pública se ausente y apagados al finalizar la jornada laboral para proteger la información.

h) Retiro de Documentos: Se deberán retirar de impresoras, escáneres y fotocopiadoras los documentos que contengan datos personales inmediatamente después de su uso.

i) Resguardo de Documentos y Dispositivos: Los documentos y dispositivos que contengan datos personales deberán ser resguardados bajo llave para prevenir accesos no autorizados.

j) Contraseñas Seguras: Se deberán generar contraseñas complejas, combinando letras y números, y mantenerlas en secreto por parte de los usuarios que manejan datos personales.

k) Protección de Datos Fuera del Trabajo: Se deberá evitar llevar datos personales fuera del lugar de trabajo en dispositivos electrónicos o papel. Si es necesario, la información deberá ser protegida con contraseñas o guardada en sobres debidamente cerrados.

l) Protección de Dispositivos Móviles: Se deberá evitar dejar dispositivos móviles o portátiles que contengan datos personales desatendidos en lugares públicos. Si es necesario separarse del dispositivo, este deberá ser bloqueado, siguiendo el mismo procedimiento aplicado a los equipos en el área.

m) Cumplimiento de Normas: Se deberá cumplir con todas las medidas de seguridad y normas internas establecidas para la protección de datos personales.

n) Comunicación de Incidencias: Cualquier incidencia detectada en el tratamiento de datos personales deberá ser comunicada de inmediato a la persona superior inmediata para asegurar una gestión adecuada de la situación.

o) Remisión de Datos a Otras Áreas: Al remitir datos personales a otras áreas del Instituto, se deberá comunicar por escrito que dichos datos forman parte de un sistema de protección de datos personales, especificando las finalidades para las cuales pueden ser tratados y la obligación de mantener la confidencialidad respecto a los mismos.

SANCIONES

Las sanciones por incumplimiento de estas políticas serán aplicadas de conformidad con lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como en la normatividad vigente en la materia. En particular, se tendrán en cuenta las causales de sanción establecidas en el artículo 163 de dicha Ley.

De acuerdo con el artículo 163 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, se considerarán causas de sanción las siguientes:

1. **Violación de Principios y Obligaciones:** El incumplimiento de los principios y obligaciones establecidos por la Ley General para el tratamiento de datos personales, incluyendo la falta de transparencia, la ausencia de consentimiento adecuado, y el manejo indebido de la información.
2. **Incumplimiento de Medidas de Seguridad:** La falta de implementación o el incumplimiento de las medidas de seguridad requeridas para proteger los datos personales contra accesos no autorizados, pérdida o daño.
3. **Transgresión de Derechos ARCO:** La negativa o ineficacia en la atención de las solicitudes de acceso, rectificación, cancelación u oposición por parte de los titulares de datos personales.
4. **Deficiencias en la Gestión de Incidencias:** La falta de comunicación oportuna y adecuada de incidencias relacionadas con la seguridad de los datos personales a las autoridades competentes o a los titulares afectados.

5. **Transferencia y Remisión Inadecuada:** La transferencia de datos personales a terceros sin el consentimiento adecuado o sin cumplir con las normativas que regulan la remisión de datos dentro o fuera del Instituto.

El Comité de Transparencia tomará las medidas necesarias para asegurar que las sanciones sean aplicadas de manera justa y proporcional, en concordancia con los procedimientos establecidos por la Ley General y la normativa aplicable.

Unidad de Transparencia CIDE

05 de diciembre de 2024