Cultura
Secretaría de Cultura

Centro Cultural Tijuana



PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES DE LA COMPAÑÍA OPERADORA DEL CENTRO CULTURAL Y TURÍSTICO DE TIJUANA S.A. DE C.V.

Unidad de Transparencia.

El presente documento fue aprobado por el Comité de Transparencia, en la Segunda Sesión Extraordinaria 2025, de fecha cinco de febrero de dos mil veinticinco.



2025 Año de La Mujer Indígena

CONTENIDO

INTRODUCCIÓN. 3
OBJETIVO GENERAL. 3
OBJETIVOS ESPECÍFICOS. 3
MARCO JURÍDICO. 4
POLÍTICAS PARA EL TRATAMIENTO DE DATOS PERSONALES. 4
Principios Generales para la Obtención y Uso de Datos Personales. 4
Cumplimiento del Principio de Responsabilidad. 6
Acciones para la implementación de Medidas de Seguridad. 6
Documento de Seguridad. 7
Inventario de Datos Personales 8
Seguridad de Datos Personales. 8
Transferencia de Datos Personales. 9
Interpretación de las políticas 10

INTRODUCCIÓN.

En apego a lo dispuesto por la Constitución Política de los Estados Unidos Mexicanos, en su artículo 6, Apartado A, fracciones I y II la información que posea la Compañía Operadora del Centro Cultural y Turístico de Tijuana S.A. de C.V. (CECUT) es de máxima publicidad, mientras que la información concerniente a los datos personales será protegida en los términos y excepciones que fijen las leyes, por lo tanto, y de conformidad con lo establecido por los artículos 29, 30, 33 y 35 de la Ley General de Datos de Personales en Posesión de Sujetos Obligados (LGPDPPSO o Ley General), cuyo objeto es establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados.

El CECUT, atiende a los principios de accesibilidad a la información, transparencia, objetividad e independencia, y tiene como obligación, el realizar acciones que deberán llevar a cabo las Unidades Administrativas correspondientes en la protección, tratamiento y conservación de los datos personales; así como aquellas que coadyuven a identificar y adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos de carácter personal; su adopción es de carácter obligatorio para las Unidades Administrativas, las cuales conforme a sus funciones, facultades y atribuciones dan tratamiento a datos personales y, en su caso, de las personas encargadas del tratamiento.

Es por ello que se establece el presente Programa de Protección de Datos Personales, como un instrumento necesario para asegurar el adecuado tratamiento de los datos personales en posesión del CECUT.

OBJETIVO GENERAL.

Determinar el procedimiento que deberá seguir la Compañía Operadora del Centro Cultural y Turístico de Tijuana S.A. de C.V. (CECUT) para asegurar la protección de los datos personales que posee esta entidad.

OBJETIVOS ESPECÍFICOS.

1. Proveer el marco de trabajo necesario para la protección de los datos personales en posesión del CECUT;

2. Cumplir con las obligaciones que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales, así como la normatividad que derive de los mismos;

3. Establecer los elementos y actividades de dirección, operación y control de los procesos que impliquen el tratamiento de datos personales, a efecto de protegerlos de manera sistemática y continua, y

4. Promover la adopción de mejores prácticas en la protección de datos personales, de manera preferente una vez que el programa se haya implementado de manera integral en la entidad, o bien, cuando se estime pertinente la implementación de buenas prácticas en tratamientos específicos.

ALCANCE.

El Programa de Protección de Datos Personales es aplicable al tratamiento de datos personales de personas físicas en posesión del CECUT y son de observancia general para las Unidades Administrativas del CECUT que resguardan datos personales.

MARCO JURÍDICO.

- Constitución Política de los Estados Unidos Mexicanos.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley General de Transparencia y Acceso a la Información Pública.
- Ley Federal de Transparencia y Acceso a la Información Pública.
- Lineamientos generales de protección de datos personales para el sector público.

POLÍTICAS PARA EL TRATAMIENTO DE DATOS PERSONALES.

Principios Generales para la Obtención y Uso de Datos Personales.

1. En el tratamiento de datos personales, las Unidades Administrativas y las personas servidoras públicas vinculados deberán observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, en términos de la Ley General de Datos de Personales y demás disposiciones normativas aplicables.

2. Las Unidades Administrativas deberán tratar los datos personales que resulten estrictamente necesarios para el ejercicio de sus funciones, facultades y atribuciones que la normatividad aplicable les confiera, observando las disposiciones aplicables en materia de datos personales.

3. Todo tratamiento de datos personales que efectúen la Unidades Administrativas y las personas servidoras públicas vinculadas, deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera. Se podrán tratar datos personales para finalidades distintas a las inicialmente informadas mediante el aviso de privacidad, siempre y cuando las Unidades Administrativas cuenten con atribuciones conferidas en la Ley y medie el consentimiento del titular.

4. Las Unidades Administrativas deberán abstenerse de tratar los datos personales a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la confianza depositada por éste de que sus datos serán tratados conforme la Ley General de Datos Personales.

5. Previo al tratamiento de los datos personales, las Unidades Administrativas y los servidores públicos vinculados deberá obtener el consentimiento del titular, de manera libre, específica e informada, salvo que se actualice alguna de las causales de excepción previstas en el artículo 22 de la Ley General de Datos Personales. El consentimiento del titular podrá manifestarse de forma expresa o tácita, por regla general será válido el consentimiento tácito, salvo que una ley exija que la voluntad del titular se manifieste de manera expresa.

El consentimiento expreso se recabará por las Unidades Administrativa a través de las funciones, facultades y atribuciones con que cuenten, para lo cual deberá elaborarse un acta o notificación que permita garantizar la certeza de su obtención. Todo tratamiento de datos personales para finalidades distintas a las establecidas en el aviso de privacidad, deberá contar con el consentimiento expreso o tácito de su titular, en términos de lo previsto Ley General de Datos Personales.

6. Las Unidades Administrativas deberán adoptar las medidas necesarias para mantener exactos, completos, pertinentes, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos, para lo cual deberán atender lo siguiente:

I. Los datos personales son exactos cuando reflejan la realidad de la situación de su titular, es decir, son verdaderos o fieles;

II. Los datos personales están completos cuando no falta ninguno de los que se requiera para las finalidades para las cuales se obtuvieron y son tratados;

III. Los datos personales son pertinentes cuando corresponden efectivamente al titular y no a una homonimia;

IV. Los datos personales están actualizados cuando corresponden a la situación presente de su titular; y

V. Los datos personales son correctos cuando cumplen con todas las características anteriores, es decir, son exactos, completos, pertinentes y actualizados.

Se presume que se cumple con la calidad en los datos personales cuando son proporcionados directamente por el titular y hasta que éste no manifieste y acredite lo contrario.

7. Las Unidades Administrativas deberán tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

8. Para informar al titular de los datos personales que obren en bases o sistemas de datos personales que las Unidades Administrativas del CECUT resguarden en ejercicio de atribuciones y funciones relativas a información correspondiente a su gestión administrativa, deberá ponerse a su disposición el Aviso de Privacidad en dos modalidades: simplificado e integral.

Los avisos de privacidad deberán contener lo establecido en los artículos 27 y 28 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Cumplimiento del Principio de Responsabilidad.

9. Para adoptar los mecanismos previstos en el artículo 3 de la Ley General, se atenderá a lo siguiente:

I. El Comité de Transparencia, a propuesta de la Unidad de Transparencia, aprobará el programa de capacitación en materia de protección de datos personales;

II. La Unidad de Transparencia establecerá un sistema de supervisión de vigilancia para comprobar el cumplimiento de las políticas en materia de datos personales;

III. La Unidad de Transparencia, en el ámbito de sus facultades, recibirá y atenderá las dudas y quejas de los titulares de los datos personales.

Acciones para la implementación de Medidas de Seguridad.

10. Para adoptar los mecanismos previstos en el artículo 33 de la Ley General, se atenderá a lo siguiente:

I. Los titulares de las Unidades Administrativas deberán definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;

II. Los titulares de las Unidades Administrativas que con motivo del ejercicio de sus funciones cuenten con uno o varios sistemas de datos, deberán informar a la

Unidad de Transparencia a efecto de integrar el inventario de datos personales respectivo;

III. Los titulares de las Unidades Administrativas por cada uno de los sistemas de datos con que cuentan deberán elaborar los análisis de riesgo y de brecha, los cuales deberán remitir a la Unidad de Transparencia.

IV. Los titulares de las Unidades Administrativas deberán elaborar un plan de trabajo con apoyo de la Unidad Administrativa Correspondiente, en el que se definan las acciones a implementar conforme a los resultados de los análisis de riesgo y de brecha, para que la Unidad de Transparencia los integre al plan de trabajo del responsable; y

V. La Unidad de Transparencia 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, para lo cual se podrá auxiliar de la Gerencia de Informática o la Unidad Administrativa pertinente.

Documento de Seguridad.

11. La Unidad de Transparencia elaborará el documento de seguridad a que se refiere el artículo 35 de la Ley General, el cual se integrará con la información que señala el artículo señalado.

12. Cada Unidad Administrativa designará una persona servidora pública vinculada a las bases de datos personales, quién será el encargado de apoyar al Titular de la Unidad Administrativa de su adscripción para realizar lo establecido en las presentes Políticas y tendrá las siguientes funciones:

I. Adoptar las medidas de seguridad para el resguardo del o los sistemas de datos personales bajo su responsabilidad, en soporte físico, de manera que se evite su alteración, pérdida o acceso no autorizado;

II. Autorizar expresamente, en los casos en que no esté previsto por un instrumento jurídico o disposición normativa, a los usuarios, y llevar una relación actualizada de las personas que tengan acceso a las bases o los sistemas de datos personales que se encuentran en soporte físico, y

III. Aplicar y vigilar el cumplimiento de las medidas y estándares de seguridad para la conservación y resguardo de las bases o sistemas de datos personales del CECUT, que para tal efecto determine el Comité, a través de las disposiciones normativas específicas de observancia general para las Unidades Administrativas que cuenten con los referidos sistemas o bases.

Inventario de Datos Personales

13. Las Unidades Administrativas, con la asesoría de la Unidad de Transparencia, deberán elaborar un inventario con la información básica de cada tratamiento de datos personales en posesión del CECUT, considerando, al menos, los siguientes elementos:

I. Fundamento jurídico que habilita el tratamiento;

II. Las facultades, atribuciones y funciones que la normatividad aplicable les confiera para dar tratamiento a datos personales;

III. Listado de datos personales sujetos a tratamiento, en su caso, aquellos sensibles;

IV. Los medios a través de los cuales se obtienen los datos personales;

V. Las finalidades de cada tratamiento de datos personales;

VI. Los formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;

VII. Los servidores públicos que tienen acceso a las bases o sistemas de tratamiento y;

VIII. En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas.

La actualización del inventario de datos personales deberá realizarse por las Unidades Administrativas responsables de su administración, el Titular de éstas, remitirá a la Unidad de Transparencia en el formato que establezca para tal efecto la modificación, actualización o cancelación de dichas bases.

Seguridad de Datos Personales.

14. Corresponderá al Titular de cada Unidad Administrativa responsable establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar su relación con el mismo. Lo anterior, sin menoscabo de lo establecido en las disposiciones de acceso a la información pública.

Con independencia del tipo de sistema en el que se encuentren los Datos Personales o el tipo de tratamiento que se efectúe, el Titular de la Unidad Administrativa responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico pudiendo solicitar apoyo de la Unidad Administrativa competente 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.

De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

I. Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
II. Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
III. Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización;
IV. Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.
V. Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
VI. Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
VII. Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware,
VIII. Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales que implementen las Unidades Administrativas responsables de las bases de datos personales deberán estar documentadas y contenidas en el sistema de que se trate, en términos de lo dispuesto por la Ley General de Datos de Personales y demás disposiciones administrativas aplicables.

Corresponderá a las Unidades Administrativas, con la asesoría de la Unidad de Transparencia, llevar una bitácora de las vulneraciones a la seguridad, a que hace referencia el artículo 39 de la Ley General de Datos de Personales, en la que se describa la fecha en la que ocurrió, el motivo y las acciones correctivas implementadas de forma inmediata y definitiva.

Transferencia de Datos Personales.

15. Toda transferencia de datos personales se encontrará sujeta al consentimiento de su titular, salvo las excepciones previstas en los artículos 22, 66 y 70 de la Ley General de Datos de Personales.

Toda transferencia de datos personales que realicen las Unidades Administrativas del CECUT en ejercicio de sus atribuciones o funciones, deberán ser formalizadas mediante convenios de colaboración o cualquier otro instrumento jurídico en el que se incluyan cláusulas que permitan demostrar el alcance del tratamiento de los datos personales,

así como las obligaciones y responsabilidades asumidas por las partes atendiendo a lo establecido en el Aviso de Privacidad correspondiente.

El instrumento que formalice la transferencia deberá contener al menos, lo siguiente:

I. Identificación del Sistema de Datos Personales, del transmisor y del destinatario de estos;
II. Finalidad de la transferencia, así como el tipo de datos que son objeto de esta;
III. Las medidas de seguridad y custodia que fueron adoptadas por la Unidad o Área Administrativa y el destinatario;
IV. Plazo por el que conservará el destinatario los datos que le hayan sido transmitidos, el cual podrá ser ampliado mediante aviso al CECUT, y
V. Señalar si una vez concluidos los propósitos de la transmisión, los datos personales deberán ser destruidos o devueltos al CECUT, al igual que cualquier soporte o documento en que conste algún Dato Personal objeto de la transmisión.

Interpretación de las políticas

16. Las Unidades Administrativas podrán solicitar asesoría sobre la aplicación de la Ley General de Datos de Personales y del presente Programa, la cual será proporcionada por la Unidad de Transparencia, sin menoscabo de la interpretación que del presente documento realice el Comité de Transparencia, quien es la autoridad máxima en materia de protección de datos personales, acorde a lo dispuesto en los artículos 83 y 84 de la Ley General de Datos de Personales.