

SISTEMA DE SUPERVISIÓN Y VIGILANCIA.

INTRODUCCIÓN.

La Compañía Operadora del Centro Cultural y Turístico de Tijuana S.A. de C.V. (CECUT), tiene el deber de evaluar y medir el resultado de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de datos personales, de conformidad con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el Sector Público y de más normatividad aplicable.

Asimismo, deberá contar con un sistema de gestión de seguridad de datos personales que permita planificar, establecer, implementar, operar, monitorear, mantener, revisar y mejorar las medidas de seguridad de carácter administrativo, físico y técnico aplicadas a los datos personales.

Corresponderá a la Unidad de Transparencia y a la Gerencia de Informática en el ámbito de sus respectivas competencias, llevar a cabo, de manera coordinada y en conjunto con las unidades administrativas del CECUT; el diseño, la implementación y la mejora continua del sistema de gestión de seguridad de datos personales, con base en las necesidades institucionales. La elaboración y actualización periódica del documento de seguridad previsto en el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) estará a cargo, de manera coordinada, de la Unidad de Transparencia y con la participación de las unidades administrativas de la entidad. En dicho documento deberán mencionarse, además, las medidas de seguridad implementadas para la protección de los datos personales.

NORMATIVIDAD.

- Artículo 30, fracción V, artículo 33 fracción VII y 35 fracción VI de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
- Artículo 63 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales).

El artículo 30, fracción V, de la LGPDPPSO, establece que entre los mecanismos que se deberán adoptar para cumplir con el principio de responsabilidad, se encuentra el de:

> *"Artículo 30.- (…)*
>
> *V.- Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales; (…)"*



SISTEMA DE SUPERVISIÓN Y VIGILANCIA.

Por su parte el artículo 33 fracción VII de la misma Ley señala que, para establecer y mantener las medidas de seguridad para la protección de los datos personales se debe "*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.*"

Con relación al artículo 35 fracción VI de la LGPDPPSO señala que los sujetos obligados deben elaborar un documento de seguridad, el cual deberá contener, entre otras cosas, los mecanismos de monitoreo y revisión de las medidas de seguridad.

Respecto a los Lineamientos Generales, el artículo 63 establece lo siguiente:

> "***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.*"

MECANISMOS DE MONITOREO Y SUPERVISIÓN.

La Unidad de Transparencia del CECUT 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:





SISTEMA DE SUPERVISIÓN Y VIGILANCIA.

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, contestación al siguiente cuestionario:

Pregunta	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, a fin de identificar si 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, obligaciones y cadena de mando de cada persona servidora pública que trata datos personales, por unidad administrativa?		
4. ¿Se ha comunicado a cada persona servidora pública 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 personas servidoras públicas que tienen acceso a los sistemas de tratamiento; • En su caso, el nombre completo o denominación o razón social de la persona encargada 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;		





SISTEMA DE SUPERVISIÓN Y VIGILANCIA.

• 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.		
9. ¿Se ha elaborado el plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales, a partir del análisis de riesgo y brecha realizado, y		





SISTEMA DE SUPERVISIÓN Y VIGILANCIA.

priorizando las medidas de seguridad más relevantes e inmediatas a establecer?		
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.		

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.

MECANISMOS DE ACTUACIÓN ANTE VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES.

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 de la Gerencia de Informática, de la Subdirección de Administración y de las demás áreas que se consideren pertinentes.

Además, es importante contar con un mecanismo que permita monitorear las alertas de seguridad de los datos personales, como posibles incidentes de seguridad, las cuales se realizarán a través de:



SISTEMA DE SUPERVISIÓN Y VIGILANCIA.

1. Verificar si el hecho o evento podía dar como consecuencia una vulneración a la seguridad (posible incidente de seguridad). De manera enunciativa mas no limitativa, se entenderá por vulneración de seguridad:

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

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, datos personales involucrados, datos de identificación y de contacto de la persona servidora pública responsable del tratamiento de los datos personales y las actuaciones que pueden evitar la explotación de 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, así como informarlo al Comité de Transparencia.

MECANISMOS DE AUDITORÍA EN MATERIA DE DATOS PERSONALES.

Cuando así se considere pertinente, podrán realizarse auditorías en materia de datos personales, las cuales tendrán la finalidad de verificar el debido cumplimiento de los principios y deberes, así como de los controles establecidos para proteger los datos personales en apego a lo establecido en la Ley General de Protección de Datos Personales en posesión de Sujetos Obligados y los Lineamientos generales.

Esto permitirá identificar las acciones y mejoras que habrán de implementarse para el adecuado manejo y protección de los datos personales que maneja la Compañía Operadora del Centro Cultural y Turístico de Tijuana S.A. de C.V.

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.