"2024, Año de los Pueblos Yumanos, Pueblos Originarios y de las Personas Afromexicanas"

COMITÉ DE TRANSPARENCIA

INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE BAJA CALIFORNIA

RESOLUCIÓN DE COMITÉ DE TRANSPARENCIA: DECLARACIÓN DE INEXISTENCIA
NO. DE SOLICITUD: 020067924000049

Mexicali, Baja California a 07 de marzo del 2024.

VISTOS, para resolver la declaración de inexistencia de la solicitud de acceso a la información 020067924000049, formulada a este Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Baja California.

ANTECEDENTES

PRIMERO. Solicitud de acceso a la información: En fecha veintisiete de febrero de dos mil veinticuatro, se formuló mediante la Plataforma Nacional de Transparencia, la solicitud de acceso a la información pública identificada con el folio número **020067924000049**, a través de la cual, entre otras cosas, la persona solicitante manifestó su interés en que se la proporcionara lo siguiente: *el **Documento de seguridad para proteger los datos personales del sujeto obligado** y, las **Medidas de Seguridad de carácter administrativo, físico y técnico para proteger los datos personales.***

SEGUNDO. Turno de la solicitud a la unidad administrativa competente: Con motivo de lo anterior, en la misma fecha, el Titular de la Unidad de Transparencia tuvo a bien requerir a esta Coordinación de Protección de Datos Personales, como área responsable de generar, poseer o administrar la información, para que, de acuerdo a las facultades y atribuciones previstas en el Reglamento Interior, localizara y remitiera la información requerida en la solicitud, para estar en aptitud de notificar la respuesta correspondiente.

TERCERO. Declaración de inexistencia de la información por parte de la unidad administrativa competente: La Coordinación de Protección de Datos Personales, de conformidad con lo dispuesto en los artículos 122 y 124 de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California, se avocó a la búsqueda de la información solicitada, tras lo cual identificó el documento denominado *Documento de Seguridad* del Instituto de Transparencia, Acceso a la

Información Pública y Protección de Datos Personales del Estado de Baja California, con los siguientes anexos:

I. Inventario de sistemas de datos personales del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Baja California;
II. Funciones y obligaciones del personal que trata datos personales en la organización del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Baja California;
VII. Programa de capacitaciones 2024 del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Baja California.

En ese sentido, se advierte que el multicitado Documento de Seguridad se encuentra en los archivos y bajo resguardo de esta Coordinación; sin embargo, resulta imperativo señalar que, si bien el *Documento de Seguridad del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Baja California* cuenta con los anexos I, II y VII, en un análisis comparativo respecto de los elementos que por mandato de Ley debe contener, se tiene que dicho *Documento de Seguridad* se encuentra incompleto, siendo necesario que se confirme la inexistencia de los anexos III, IV, V y VI del mismo, en razón de los siguientes:

CONSIDERANDOS

I. **FUNDAMENTACIÓN**. Del estudio de la solicitud de acceso a la información que nos ocupa, se advierte que el *Documento de* Seguridad *del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Baja California* que resulta del interés del particular, de conformidad con el artículo 18 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California, en relación con lo establecido en los artículos 35 y 36 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, se encuentra incompleto, pues el primero señala que *el responsable debe elaborar un documento de seguridad y actualizarlo conforme a los supuestos que enmarca la Ley General.*

En ese tenor, para una mejor comprensión de los elementos que debe contener tal documento, a continuación se transcriben los artículos citados:

LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS PARA EL ESTADO DE BAJA CALIFORNIA

Artículo 18.- *El responsable debe elaborar un documento de seguridad y actualizarlo conforme a los supuestos que enmarca la Ley General.*

LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS

Artículo 35. *De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:*

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.*

Artículo 36. *El responsable deberá actualizar el 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.*

Así, en concordancia con los anteriores preceptos normativos, se establece el siguiente cuadro comparativo, en el que se reflejan los elementos pendientes:

Contenido del Documento de Seguridad por disposición legal	**Documentos que conforman el Documento de Seguridad del ITAIPBC**
I. El inventario de datos personales y de los sistemas de tratamiento;	**I.** El inventario de datos personales y de los sistemas de tratamiento del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Baja California;
II. Las funciones y obligaciones de las personas que traten datos personales;	**II.** Las funciones y obligaciones de las personas que tratan datos personales en la organización del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Baja California;
III. El análisis de riesgos;	**III.**
IV. El análisis de brecha;	**IV.**
V. El plan de trabajo;	**V.**
VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad; y	**VI.**
VII. El programa general de capacitación	**VII.** Programa de capacitaciones 2024 del Instituto de Transparencia, Acceso a la Información Pública y Protección de

	Datos Personales del Estado de Baja California

Ahora bien, respecto a las *"medidas de seguridad de carácter administrativo, físico y técnico para proteger los datos personales"* a que hace referencia la persona solicitante, es necesario establecer la naturaleza jurídica de las mismas, así como su relación con el multicitado Documento de Seguridad.

Para ello, resulta fundamental señalar el contenido de los artículos 4 fracción XII, 16, 17 y 18 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California, en relación con los artículos 57, 59, 60, 68, 72 y 73 de los Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Baja California, los cuales, respectivamente, estipulan lo siguiente:

LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS PARA EL ESTADO DE BAJA CALIFORNIA

Artículo 4.- Para los efectos de la presente Ley se entenderá por:

[...]
XII.- Documento de Seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable *para garantizar de la confidencialidad, integridad y disponibilidad de los datos personales que posee;*
[...]

Artículo 16.- El responsable debe establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico *para proteger los datos personales.*

Artículo 17.- El responsable debe implementar su sistema de gestión que contenga las acciones relacionadas con las medidas de seguridad *para el tratamiento de los datos personales.*

Artículo 18.- El responsable debe elaborar un documento de seguridad *y actualizarlo conforme a los supuestos que enmarca la Ley General.*

[Énfasis añadido]

LINEAMIENTOS DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DEL ESTADO DE BAJA CALIFORNIA

Deber de seguridad

Artículo 57. *Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe,* ***el responsable deberá establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales****, que le permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad, de conformidad con lo previsto en el artículo 16 de la Ley Estatal, con el objeto de impedir, que cualquier tratamiento de datos personales contravenga las disposiciones de dicho ordenamiento, la Ley General y los presentes Lineamientos.*

Medidas de seguridad

Artículo 59. Las medidas de seguridad a que se refiere el artículo 16 de la Ley Estatal son el conjunto de acciones, actividades, controles y/o mecanismos administrativos, técnicos y físicos que le permiten al responsable proteger los datos personales.

Para efectos de lo dispuesto en dicho ordenamiento y en los presentes Lineamientos se entenderá por:

I. Medidas de seguridad administrativas: Políticas y procedimientos *para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la* ***sensibilización y capacitación*** *del personal, en materia de protección de datos personales.*

II. Medidas de seguridad físicas: Conjunto de acciones y mecanismos *para proteger el entorno físico de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:*
a. *Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;*
b. *Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;*
c. *Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización; y,*
d. *Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.*

III. Medidas de seguridad técnicas: Conjunto de acciones y mecanismos *que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:*
a. *Prever que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;*

***b.** Generar un esquema de privilegios para que cada usuario lleve a cabo las actividades que requiere con motivo de sus funciones;*
***c.** Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware; y,*
***d.** Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.*

Medidas de seguridad para la protección de los datos personales
Artículo 60. Para establecer y mantener las medidas de seguridad para la protección de los datos personales a que se refiere el artículo 16 de la Ley Estatal, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:

***I.** Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;*
II. Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;
III. Elaborar un inventario de datos personales y de los sistemas de tratamiento;
***IV. Realizar un análisis de riesgo de los datos personales,** considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;*
V. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;
***VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad** faltantes y para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;*
***VII. 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; y,*
***VIII. Diseñar y aplicar diferentes niveles de capacitación del personal** bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.*

Análisis de brecha
Artículo 68.** Con relación a la fracción V del artículo 60 de los presentes Lineamientos, **en la realización del análisis de brecha el responsable deberá considerar lo siguiente:

I. Las medidas de seguridad existentes y efectivas;
II. Las medidas de seguridad faltantes, y
III. La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.

Sistema de gestión
***Artículo 72.** El responsable deberá **implementar un sistema de gestión de seguridad de los datos personales** a que se refiere el artículo 17 de la Ley Estatal, **el cual 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; tomando en consideración los estándares nacionales e internacionales en materia de protección de datos personales y seguridad.

Documento de Seguridad
Artículo 73. *Para dar cumplimiento a lo establecido en el artículo 18 de la Ley Estatal y 35 de la Ley General,* ***el responsable deberá elaborar, difundir e implementar normas internas para la seguridad y protección de los datos personales mediante el documento de seguridad.***

El documento de seguridad será de observancia obligatoria para todos los servidores públicos de la organización, así como para los encargados que, conforme al artículo 4, fracción XIII de la Ley Estatal, tengan acceso a los sistemas de datos personales y/o al sitio donde se ubican los mismos; ***Dicho documento de seguridad deberá contener, como mínimo, lo siguiente:***

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.

[Énfasis añadido]

Es así que, con fundamento en lo dispuesto en los artículos 13 segundo párrafo, 54 fracción II y, 131 fracción I de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California; 191 del Reglamento de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California; 4 fracción XII, 16 17 y 18 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California; 35 y 36 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en relación con los artículos 57, 59, 60, 68, 72 y 73 de los Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Baja California, esta Coordinación **solicita la confirmación de la declaración de inexistencia respecto de los anexos III, IV, V y VI del *Documento de* Seguridad *del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Baja California.***

II. MOTIVACIÓN: En concordancia con el marco normativo previamente transcrito, como resultado de lo que señala el artículo 16 de la Ley estatal de datos, en relación con el 59 de los Lineamientos estatales, puede advertirse que las *medidas de seguridad de carácter administrativo, físico y técnico para proteger los datos personales* a que refiere la persona solicitante, consisten en todas aquellas acciones, actividades, controles y mecanismos administrativos, técnicos y físicos que el responsable deba implementar con el objetivo de proteger los datos personales.

Ahora bien, el artículo 60 de los Lineamientos indica que, entre las actividades mínimas que el sujeto obligado debe realizar para establecer y mantener las medidas de seguridad para la protección de los datos personales, se encuentra la de llevar a la práctica un análisis de brecha, entendido este como un proceso que le permitirá comparar las medidas de seguridad con que cuenta, contra aquellas faltantes y que requiere implementar para estar en aptitud de proteger los datos personales.

Lo anterior se concatena con el contenido del artículo 68 de los mismos Lineamientos, en el que se advierte que, para dar cuenta y generar evidencia de los resultados del análisis de brecha, así como para facilitar su seguimiento, es necesario registrar y documentar las medidas de seguridad existentes y efectivas, las medias de seguridad faltantes, así como las nuevas medidas de seguridad necesarias en la organización. En ese sentido, es posible considerar que las *medidas de seguridad de carácter administrativo, físico y técnico para proteger los datos personales* a que refiere la persona solicitante estarán contenidas y se plasmarán como resultado del análisis de brecha.

Finalmente, el artículo 4 fracción XII de la Ley estatal de datos señala que el Documento de Seguridad es el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable; en ese sentido, habiendo establecido que dichas medidas se documentarán durante la ejecución del análisis de brecha, es posible concluir que la información relativa a las ***medidas de seguridad de carácter administrativo, físico y técnico para proteger los datos personales*** solicitada por la persona interesada, le deberían ser entregadas en el documento que resulte del **análisis de brecha** que, en su momento se realice.

Lo anterior se confirma con el contenido del artículo 73 fracción IV de los multicitados Lineamientos, en el que se estipula que el análisis de brecha constituye uno de los elementos mínimos de dicho Documento de Seguridad.

Por todo lo anteriormente expuesto, se declara que después de realizar una búsqueda exhaustiva, no fue posible localizar la información requerida por la persona solicitante, por lo que es necesario declarar la inexistencia de los siguientes elementos del *Documento de Seguridad*:

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;*

Consecuentemente, de conformidad con lo establecido en los artículos 54 fracción II y 131 fracción II de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California, así como el 191 del Reglamento de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California, se solicita al H. Comité de Transparencia, tenga a bien **CONFIRMAR** la **INEXISTENCIA DE LOS ANEXOS III, IV, V Y VI DEL DOCUMENTO DE SEGURIDAD.**

R E S U E L V E

PRIMERO. - Se confirma la **INEXISTENCIA DE LOS ANEXOS III, IV, V Y VI DEL DOCUMENTO DE SEGURIDAD** de la solicitud de acceso a la información pública, identificada con el número de folio **020067924000049**, solicitada por la Coordinación de Protección de Datos Personales del ITAIPBC.

SEGUNDO. - Notifíquese a la Unidad de Transparencia, a la Coordinación de Protección de Datos Personales del ITAIPBC, y al solicitante, la presente **RESOLUCIÓN**.

TERCERO. - Publíquese la presente **RESOLUCIÓN** en el Portal de Obligaciones de Transparencia de este Instituto.

ASÍ LO RESOLVIERON POR UNANIMIDAD DE VOTO DE LOS INTEGRANTES DE ESTE COMITÉ DE TRANSPARENCIA, **JIMENA JIMÉNEZ MENA**, SECRETARIA EJECUTIVA DEL INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE BAJA CALIFORNIA Y PRESIDENTA DEL COMITÉ DE TRANSPARENCIA DEL ITAIPBC; **JESÚS GABRIEL RODRÍGUEZ AGUILAR**, TITULAR DE LA UNIDAD DE TRANSPARENCIA DEL INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE BAJA CALIFORNIA Y SECRETARIO TÉCNICO DEL COMITÉ DE TRANSPARENCIA DEL ITAIPBC; **CHRISTIAN JESUS AGUAYO BECERRA**, COORDINADOR DE VERIFICACIÓN Y SEGUIMIENTO DE ESTE INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE BAJA CALIFORNIA Y VOCAL DEL COMITÉ DE TRANSPARENCIA DE ESTE INSTITUTO.

JIMENA JIMÉNEZ MENA
SECRETARIA EJECUTIVA
PRESIDENTA DEL COMITÉ DE TRANSPARENCIA
DEL ITAIPBC

JESÚS GABRIEL RODRÍGUEZ AGUILAR
TITULAR DE LA UNIDAD DE TRANSPARENCIA
SECRETARIO TÉCNICO DEL COMITÉ DE
TRANSPARENCIA DEL ITAIPBC

CHRISTIAN JESUS AGUAYO BECERRA
COORDINADOR DE VERIFICACIÓN Y SEGUIMIENTO
VOCAL DEL COMITÉ DE TRANSPARENCIA DEL ITAIPBC

COMITÉ DE TRANSPARENCIA
ESTADOS UNIDOS MEXICANOS
INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE BAJA CALIFORNIA