RESOLUCIÓN DEL COMITÉ DE TRANSPARENCIA: CLASIFICACIÓN DE INFORMACIÓN COMO CONFIDENCIAL Y ELABORACIÓN DE VERSIÓN PÚBLICA

Mexicali, Baja California a 11 de mayo de 2023.

VISTOS, para resolver la **clasificación de información** como **confidencial, y su correspondiente versión pública,** respecto de la información contenida en los numerales 1.5, 2.5, 3.5, 4.5, 5.5. 6.5. 7.5, 8.5, 9.5, 10.5, 11.5, 12.5, 13.5, 14.5, 15.5, 16.5, 17.5, 18.5, 19.5, 20.5, 21.5, 22.5, 23.5, 24.5, 25.5, 26.5, 27.5, enlistados en el anexo 1, titulado *"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"* y, relativa a: "la ubicación de las bases de datos", que, en un momento posterior formará parte integral del *Documento de Seguridad*, conforme lo siguiente:

Con la finalidad de dar cumplimiento a la obligación de otorgar respuesta a la solicitud de información pública turnada a la Coordinación de Protección de Datos Personales del ITAIPBC, es que se procedió al escrutinio de la solicitud **SAIP 020067923000111**; la cual se transcribe a continuación:

> ***""[…] 1. Solicito en versión pública el documento de seguridad en los términos de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados. (de cualquier año). […]"(sic)***

Por lo anterior y con fundamento en los artículos 5, 16, fracción VI, 106, 107, 108 y 130 de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California, en concordancia con el Cuarto y Séptimo de los Lineamientos Generales en Materia de Clasificación y Desclasificación dela Información, así como para la Elaboración de Versiones Públicas, turno al Comité de Transparencia del ITAPBC para su análisis y determinación, lo siguiente:

Una vez analizada la solicitud que nos ocupa, se actualizan parcialmente los supuestos de confidencialidad previstos en los artículos 4, fracción XII y 106 de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California; 4, fracción VIII de la Ley de Protección de Datos Personales en Posesión de Sujeto Obligados para el Estado de Baja California; y, Trigésimo Octavo, fracción I de los Lineamientos Generales para la Clasificación

y Desclasificación de la Información Pública, así como para la elaboración de versiones públicas; consecuentemente, se solicita:

PRIMERO. Solicitud de acceso a la información: En fecha diecisiete de abril de dos mil veintitrés, se tuvo a la persona solicitante formulando una solicitud de acceso a la información pública identificada con el folio número **020067923000111** mediante la Plataforma Nacional de Transparencia, a través de la cual, entre otras cosas, solicitó lo siguiente: ***"[...] 1. Solicito en versión pública el documento de seguridad en los términos de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados. (de cualquier año). [...]" (Sic).***

SEGUNDO. Turno de la solicitud a la unidad administrativa competente: Con motivo de lo anterior, en la misma fecha, la 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. Clasificación 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 se identificó el *Documento de Seguridad* peticionado, mismo que, a su vez, se conforma con los siguientes anexos:

1. 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;
2. 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;
7. Programa de capacitaciones 2023 del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Baja California.

En ese sentido, tales anexos se encuentran en los archivos y bajo resguardo de esta Coordinación y, por lo que hace al anexo 1, relativo a los *Inventarios de Sistemas de Datos Personales del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Baja California,* este **SE CLASIFICA PARCIALMENTE COMO INFORMACIÓN CONFIDENCIAL,** 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 *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* que resulta del interés del particular, alberga información de acceso restringido y clasificada por las Leyes de la materia como confidencial, con base en lo dispuesto en los artículos 4 fracción XII de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California; 172 del Reglamento de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California y, el lineamiento Trigésimo Octavo fracción I de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas; mismos que son al tenor siguiente:

LEY DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA PARA EL ESTADO DE BAJA CALIFORNIA

Artículo 4*.- Para los efectos de la presente Ley se entenderá por:*
[…]
XII.- Información Confidencial: *La información en posesión de los sujetos obligados que refiera a datos personales; la que se refiere a los secretos bancario, fiduciario, industrial, comercial, fiscal, bursátil y postal cuya titularidad corresponda a particulares, sujetos de derecho internacional o a sujetos obligados cuando no involucren el ejercicio de recursos públicos; así como aquella que presenten los particulares a los sujetos obligados siempre que tengan el derecho a entregarla con ese carácter; por lo que no puede ser difundida, publicada o dada a conocer, excepto en aquellos casos en que así lo contemple la Ley General y la presente Ley..*
[…]

[Énfasis añadido]

REGLAMENTO DE LA LEY DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA PARA EL ESTADO DE BAJA CALIFORNIA

> ***Artículo 172. Se consideran datos personales**, de manera enunciativa más no limitativa: la información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a una persona física o jurídica identificada o identificable, tales como el nombre, número telefónico, edad, sexo, registro federal de contribuyentes, clave única de registro de población, estado civil, domicilio, dirección de correo electrónico, origen racial o étnico, lugar y fecha de nacimiento, lugar de origen y nacionalidad, ideología, creencias o convicción religiosa, filosófica, política o de otro género; los referidos a características físicas, morales o emocionales, preferencias sexuales, vida afectiva o familiar, o cualquier otro referente al estado de salud físico o mental, datos laborales, idioma o lengua, escolaridad, patrimonio, títulos, certificados, cédula profesional, saldos bancarios, estados de cuenta, número de cuenta, bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, buró de crédito, seguros, afores, fianzas, tarjetas de crédito o de débito, contraseñas, huellas dactilares, firma autógrafa y electrónica, códigos de seguridad, etcétera.*
>
> ***[Énfasis añadido]***

LINEAMIENTOS GENERALES EN MATERIA DE CLASIFICACIÓN Y DESCLASIFICACIÓN DE LA INFORMACIÓN, ASÍ COMO PARA LA ELABORACIÓN DE VERSIONES PÚBLICAS

> *Trigésimo octavo.* ***Se considera información confidencial:***
>
> *I.* ***Los datos personales** en los términos de la norma aplicable;*
>
> ***[Énfasis añadido]***

En ese orden de ideas, resulta fundamental establecer la naturaleza jurídica del *Documento de Seguridad*, de conformidad con lo establecido en los artículos 4 fracciones III y XII, 16, 17 y 18 la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California, en relación con los artículos 2 fracción XXIV, 55, 57, 58, 70, 71 y 73 de los Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Baja California, los cuales, respectivamente señalan:

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:***
>
> *[...]*

III.- Bases de datos: *Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;*
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;*
[…]

Articulo 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.*

Articulo 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

Artículo 2. Además de las definiciones previstas en el artículo 4 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California, para efectos de los presentes Lineamientos se entenderá por:
[…]
XXIV. Sistema de datos personales: Conjunto organizado de archivos, registros, ficheros, bases o banco de datos personales de los Entes públicos, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso
[…]

Deber de seguridad
Artículo 55. *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 57*. 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 de 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. *Prevenir 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 el 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 58. *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.

Sistema de gestión
Artículo 70*.* ***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 71. *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.*

Vulneraciones a la seguridad
Artículo 73. *Para efectos de lo dispuesto en el artículo 19 de la Ley Estatal, se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:*

I. *La pérdida o destrucción no autorizada;*
II. *El robo, extravío o copia no autorizada;*
III. *El uso, acceso o tratamiento no autorizado; o,*
IV. *El daño, la alteración o modificación no autorizada.*

[Énfasis añadido]

Asimismo, por lo que respecta a las atribuciones del Comité de Transparencia del Sujeto Obligado en materia de protección de datos personales, la Ley en comento señala 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:*

[…]
V.- *Comité de Transparencia: Instancia a que hace referencia el artículo 53 de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California;*

Artículo 46.- El Comité de Transparencia tendrá las siguientes atribuciones:

I. Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con las disposiciones previstas en la presente Ley y en aquellas disposiciones que resulten aplicables en la materia;
II. *Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;*
III. *Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se niegue por cualquier causa el ejercicio de alguno de los derechos ARCO;*
IV. *Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la presente Ley y en aquellas disposiciones que resulten aplicables en la materia;*

> ***V. Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad;***
> ***VI.*** *Dar seguimiento y cumplimiento a las resoluciones emitidas por el Instituto Nacional y el Instituto, según corresponda;*
> *VII. Establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales, y*
> ***VIII.*** *Dar vista al órgano interno de control o instancia equivalente en aquellos casos*
> *en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto de determinado tratamiento de datos personales; particularmente en casos relacionados con la declaración de inexistencia que realicen los responsables.*
>
> ***[Énfasis añadido]***

En concordancia con el marco normativo previamente transcrito y, a la postre de la solicitud de acceso a la información pública, esta Coordinación advierte que la información relativa a *"la ubicación de las bases de datos"*, que obra en el anexo 1, relativo al *Inventario de Sistemas de Datos Personales*, se ajusta a las hipótesis contenidas en las disposiciones legales descritas, pues, de darse a conocer tal información, podrían vulnerarse las bases de datos, dejando susceptibles de ser identificadas o identificables a las personas titulares.

Es así que, esta Coordinación con fundamento en lo dispuesto en los artículos 4 fracción XII, 5, 16 fracción VI, 106, 107, y 130 de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California; en concordancia con los artículos 171, 172, 175 Y 177 del Reglamento de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California; así como los numerales Cuarto, Séptimo fracción I y, Trigésimo Octavo fracción I, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, y demás relativos y aplicables en el ejercicio de sus facultades, propone la presente **CLASIFICACIÓN COMO CONFIDENCIAL** respecto de la información contenida en los numerales 1.5, 2.5, 3.5, 4.5, 5.5. 6.5. 7.5, 8.5, 9.5, 10.5, 11.5, 12.5, 13.5, 14.5, 15.5, 16.5, 17.5, 18.5, 19.5, 20.5, 21.5, 22.5, 23.5, 24.5, 25.5, 26.5, 27.5, enlistados en el anexo 1, titulado *"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"* y, relativa a: "la ubicación de las bases de datos", que, en un momento posterior formará parte integral del solicitado *Documento de Seguridad*.

II. MOTIVACIÓN. Es evidente que existe un inconveniente legal que impide otorgar de manera completa la información peticionada al particular, ya que por disposición expresa de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California y su Reglamento, dicha información reviste el carácter de confidencial, pues, como ya se afirmó, de otorgar la ubicación de las bases de datos, podrían verse afectados los interés de los particulares y vulnerarse su derecho fundamental a la protección de sus datos personales, contraviniendo los principios de licitud, lealtad, consentimiento y calidad, así como los deberes de seguridad y confidencialidad que deben regir el tratamiento de los datos personales, y que deben observarse por las personas que integran este Instituto en los procesos y procedimientos que lleva a cabo, en su carácter de sujeto obligado.

En tal virtud, de conformidad con el numeral Trigésimo Octavo de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, una vez confirmada la clasificación, dicha información no estará sujeta a temporalidad alguna, y solo podrán tener acceso a ella, las personas titulares de los datos personales ahí resguardados o sus representantes, así como las personas servidoras públicas de este Instituto, facultadas para ello.

III. PRUEBA DE DAÑO. En coherencia con lo anterior, se establece que la prueba de daño para clasificar como confidencial la información referida y no proporcionarla al solicitante, se sustenta justamente en el hecho de que la *ubicación de las bases de datos de este Instituto* se encuentra relacionada directamente con las medidas de seguridad implementadas para proteger los datos personales contra daño, pérdida, acceso, alteración, destrucción o su uso o acceso no autorizados, así como para garantizar su confidencialidad, integridad y disponibilidad, de conformidad con el artículo 55 de la los Lineamientos de protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Baja California. De tal suerte que, al proporcionar dicha información, se ocasionaría un efecto contrario y, se estaría en el supuesto de causar un perjuicio a la esfera personal de quienes integran dichas bases de datos, dejándoseles más bien, en una situación vulnerable, poniendo en riesgo su seguridad, y dejándoles susceptibles de ser identificadas o identificables.

De lo anterior, se advierte que la entrega y/o difusión de la información peticionada podría traer como consecuencia alguna de las conductas a las que se refiere el artículo 73 de los

citados Lineamientos, con lo cual se podrían vulnerar las medidas de seguridad para la protección de los datos personales, materializándose un daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado sobre los datos personales.

En ese orden de ideas, resulta prudente que la información en cuestión sea clasificada como confidencial, pues hacerla del conocimiento público o difundirla, atenta contra la debida protección de los datos personales que este Instituto debe observar en cumplimiento y, como sujeto obligado de la citada Ley de Protección de datos Personales.

En este mismo sentido, se estima evidente que la difusión de la información podría causar un daño presente, probable y específico a los principios jurídicos tutelados por la Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California, así como por aquellos que rigen la protección de los datos personales.

IV. EL DAÑO PROBABLE, PRESENTE Y ESPECÍFICO QUE PODRÍA PRODUCIR LA PUBLICIDAD DE LA INFORMACIÓN SEÑALADA, SEA MAYOR QUE EL INTERÉS PÚBLICO.

Del estudio que precede, se pone de manifiesto que no es factible proporcionarle al solicitante el acceso a la *ubicación de las bases de datos* antes citada, ya que de hacer pública tal información se causaría un serio perjuicio a la privacidad de los particulares cuya información confidencial integra tales bases de datos.

Asimismo, de conformidad del artículo 7, Apartado C de la Constitución Política del Estado Libre y Soberano de Baja California, los numerales 7, y 15 fracción VI de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California, así como el artículo 2 segundo párrafo, 16, 17, 18, y demás relativos y aplicables de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California, este Instituto, como sujeto obligado, tiene la obligación y es responsable de proteger los datos personales que obran en su poder, mediante la implementación de medidas de seguridad de tipo administrativo, físico y técnico y, la aplicación y observancia de todos los principios y deberes establecidos en dicha Ley de protección de datos personales, entre los que se destacan la licitud, la lealtad y el consentimiento del titular para el uso de sus datos, así como el deber de confidencialidad que debe observarse por todas aquellas personas que intervienen en los tratamientos de datos personales.

Por ello, entregar el acceso a la información relacionada con la *ubicación de las bases de datos* de este Instituto, supone un daño **presente** y **especifico**, con lo que se amenaza el interés público protegido por la Ley, ya que haría nugatoria su facultad para garantizar la protección de datos personales de las personas que acuden al mismo; máxime, que se trata del Órgano Garante encargado, precisamente, de velar y garantizar ejercicio de los derechos fundamentales relacionados con la protección de los datos personales.

Además, de difundirse la información aludida, podemos hablar de un daño **probable** puesto que se podría materializar la pérdida o destrucción; el robo, extravío o copia; el uso, acceso o tratamiento; o bien, el daño, la alteración o modificación no autorizados de datos personales, afectándose la privacidad, integridad y seguridad de las personas.

V.- INFORMACIÓN QUE SE CLASIFICA COMO CONFIDENCIAL. La *ubicación de las bases de datos* referida en los numerales 1.5, 2.5, 3.5, 4.5, 5.5. 6.5. 7.5, 8.5, 9.5, 10.5, 11.5, 12.5, 13.5, 14.5, 15.5, 16.5, 17.5, 18.5, 19.5, 20.5, 21.5, 22.5, 23.5, 24.5, 25.5, 26.5, 27.5, enlistados en el anexo 1, titulado "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" (anexo 1) el cual formará parte integral del solicitado *Documento de Seguridad*.

VI. ELABORACIÓN DE LA VERSIÓN PÚBLICA. Una vez realizado lo anterior, de conformidad con el procedimiento descrito en los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, esta Coordinación se avocó a realizar la versión pública del documento en cuestión, mismo que se adjunta al presente.

R E S U E L V E

PRIMERO. - Se **CONFIRMA** la Clasificación como Confidencial, respecto de la ubicación de las bases de datos referida en los numerales 1.5, 2.5, 3.5, 4.5, 5.5. 6.5. 7.5, 8.5, 9.5, 10.5, 11.5, 12.5, 13.5, 14.5, 15.5, 16.5, 17.5, 18.5, 19.5, 20.5, 21.5, 22.5, 23.5, 24.5, 25.5, 26.5, 27.5, enlistados en el anexo 1, titulado "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" (anexo 1) el cual formará parte integral del solicitado *Documento de*

Seguridad, solicitada por la Coordinación de Protección de Datos Personales del ITAIPBC, en consecuencia se instruye notificar a la Unidad de Transparencia del ITAIPBC, a la Coordinación de Protección de Datos Personales del ITAIPBC, y al solicitante, la presente Resolución.

SEGUNDO. - Se **APRUEBA LA VERSIÓN PÚBLICA DEL DOCUMENTO MENCIONADO EN EL RESOLUTIVO PRIMERO** de 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; **MICHELLE CORONA NÁJERA**, 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 SECRETARIA TÉCNICA DEL COMITÉ DE TRANSPARENCIA DEL ITAIPBC; **CHRISTIAN JESUS AGUAYO BECERRA**, COORDINADOR SE 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

MICHELLE CORONA NÁJERA
TITULAR DE LA UNIDAD DE TRANSPARENCIA
SECRETARIO TÉCNICO DEL COMITÉ DE
TRANSPARENCIA DEL ITAIPBC

COMITÉ DE TRANSPARENCIA

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

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