RECURSO DE REVISIÓN

EXPEDIENTE: 1009/2023.

SUJETO OBLIGADO: AYUNTAMIENTO DE MÉRIDA, YUCATÁN.

COMISIONADO PONENTE: DOCTOR EN DERECHO, CARLOS FERNANDO PAVÓN DURÁN.

ANTECEDENTES:

- **Fecha de solicitud de acceso:** El día veintitrés de octubre de dos mil veintitrés, con folio número 310579123000821, en la que se requirió:

> **"A través del presente, solicito acceso a la siguiente información pública en cumplimiento de la Ley de Transparencia y Acceso a la Información Pública del Estado de Yucatán:**
> **1. Sistemas de Bases de Datos: Por favor, proporcione un listado detallado de todos los sistemas de bases de datos utilizados por el H. Ayuntamiento de Mérida. Incluya el nombre de cada sistema y cualquier información relevante, como el propósito de la base de datos. Una base de datos es una colección organizada de información o datos estructurados, que normalmente se almacena de forma electrónica en un sistema informático. Los datos de los tipos más comunes de bases de datos en funcionamiento actualmente se suelen utilizar como estructuras de filas y columnas en una serie de tablas para aumentar la eficacia del procesamiento y la consulta de datos. Así, se puede acceder, gestionar, modificar, actualizar, controlar y organizar fácilmente los datos. Normalmente, una base de datos está controlada por un sistema de gestión de bases de datos (DBMS). En conjunto, los datos y el DBMS, junto con las aplicaciones asociadas a ellos, reciben el nombre de sistema de bases de datos. La mayoría de las bases de datos utilizan un lenguaje de consulta estructurada (SQL) para escribir y consultar datos.**
> **2. Diccionarios de Datos: Solicito que se anexen los diccionarios de datos de cada una de las bases de datos mencionadas en el punto anterior. Los diccionarios de datos deben incluir información sobre la estructura de las tablas, los campos, los tipos de datos, las relaciones entre tablas y cualquier otra descripción que facilite la comprensión de la base de datos. Un diccionario de datos es un tipo de metadato que enlista de manera organizada los nombres, definiciones y características de cada uno de los campos o atributos de una base de datos y/o conjunto de datos. Es frecuente que cuando hablamos de diccionario de datos su significado se confunda con el de glosario de negocio o con el de vocabulario de datos, sin embargo, son conceptos distintos. Mientras que un glosario de negocio, o vocabulario de datos, trata de dar significado funcional a los indicadores o conceptos que se manejan para garantizar que se hable el mismo lenguaje, abstrayéndose del mundo técnico, un diccionario de datos trata de documentar los metadatos más ligados a su almacenamiento en la base de datos. Incluye aspectos técnicos como el tipo de dato, formato, longitud, posibles valores que puede tomar e, incluso, transformaciones sufridas, sin olvidar la definición de cada campo. La documentación de estas transformaciones nos proporcionará automáticamente el linaje del dato, entendido como la trazabilidad a lo largo de su ciclo de vida. Estos metadatos ayudan a los usuarios a entender los datos desde el punto de vista técnico para poder explotarlos adecuadamente. Por este motivo, cada base de datos debería contar con su diccionario de datos asociado. Para la**

cumplimentación de los metadatos solicitados en un diccionario de datos, existen guías y plantillas prediseñadas. Además, para poder estandarizar su contenido, es frecuente el uso de taxonomías y vocabularios controlados para codificar los valores de acuerdo a listados de códigos. Por último, un catálogo de datos actúa como directorio para localizar la información y ponerla a disposición de los usuarios, proporcionando a todos los usuarios un único punto de referencia para el acceso a los mismos. Un diccionario de datos debe incluir la siguiente información: 1. Descripción de Datos: Cada elemento de datos se describe en detalle. Esto incluye qué significa cada campo o variable. 2. Tipo de Datos: Debe especificar qué tipo de datos contiene cada campo o variable. 3. Formato y Longitud: Los detalles técnicos como el formato y la longitud de los datos. 4. Valores Posibles: Debe especificar qué valores puede tomar cada campo o variable, o si usa algún catálogo. 5. Relaciones entre Datos: Un diccionario de datos también muestra cómo se relacionan los datos entre sí. 6. Transformaciones Sufridas: Si los datos han sufrido alguna transformación, esto también debe documentarse. 7. Metadatos: Además de los detalles de los datos, un diccionario de datos puede incluir metadatos, como la fecha de creación, el autor y las actualizaciones más recientes."

- **Fecha en que se notificó el acto reclamado:** El día veintitrés de noviembre de dos mil veintitrés.
- **Acto reclamado:** La clasificación de información.
- **Fecha de interposición del recurso:** El día veintisiete de noviembre de dos mil veintitrés.

CONSIDERANDOS:

Normatividad Consultada:

Ley General de Transparencia y Acceso a la Información Pública.
Ley de Transparencia y Acceso a la Información Pública del Estado de Yucatán.
Ley de Gobierno de los Municipios del Estado de Yucatán.
Reglamento de la Administración Pública del Municipio de Mérida.

Área que resulta competente: Dirección de Tecnologías.

Conducta: En fecha veintitrés de noviembre de dos mil veintitrés, el Sujeto Obligado, puso a disposición de la parte recurrente, a través de la Plataforma Nacional de Transparencia, la respuesta recaída a la solicitud de acceso que nos ocupa, a través de la cual clasificó la información solicitada; inconforme con lo anterior, en fecha veintisiete del mes y año en cita, interpuso el medio de impugnación que nos ocupa contra la clasificación referida, resultando procedente en términos de la fracción I del artículo 143 de la Ley General de Transparencia y Acceso a la Información Pública.

Admitido el medio de impugnación, se corrió traslado al Ayuntamiento de Mérida, Yucatán, para que dentro del término de siete días hábiles siguientes al de la notificación del referido acuerdo, manifestara lo que a su derecho conviniera, según dispone el artículo 150 fracciones II y III de la Ley de la Materia; siendo que, del análisis integral realizado a las documentales que obran en el expediente que nos compete, se advirtió que la autoridad presentó alegatos reiterando su respuesta inicial.

Del estudio efectuado a las constancias que integran en el presente medio de impugnación, se advierte que el Sujeto Obligado por conducto de la **Dirección de Tecnologías**, en cuanto a la información concerniente a:

1. **Un listado detallado de todos los sistemas de bases de datos utilizados por el H. Ayuntamiento de Mérida. Incluya el nombre de cada sistema y cualquier información relevante, como el propósito de la base de datos. Una base de datos es una colección organizada de información o datos estructurados, que normalmente se almacena de forma electrónica en un sistema informático.**
2. **Los diccionarios de datos de cada una de las bases de datos mencionadas en el punto anterior. Los diccionarios de datos deben incluir información sobre la estructura de las tablas, los campos, los tipos de datos, las relaciones entre tablas y cualquier otra descripción que facilite la comprensión de la base de datos.**

Por oficio número DTI/375/2023, de fecha nueve de noviembre de dos mil veintitrés, clasificó la información como reservada, cuya interpretación se inserta a continuación:

> Con fundamento en la Fracción I del artículo 113 de la Ley General de Transparencia y Acceso a la Información Pública; en lo que respecta a este Sujeto Obligado, y de acuerdo a las funciones de la Dirección a mi cargo, le comento que se ha realizado la búsqueda exhaustiva y razonable en los archivos físicos y electrónicos en todas y cada una de las áreas que lo conforman y a la fecha de la presente solicitud se informa respecto al **listado detallado de todos los sistemas de bases de datos utilizados por el H. Ayuntamiento de Mérida y los diccionarios de datos de cada una de las bases de datos señaladas,** lo siguiente:
>
> 1. Respecto al listado detallado de todos los sistemas de bases de datos utilizados por el H. Ayuntamiento de Mérida; que Incluya el nombre de cada sistema y cualquier información relevante, como el propósito de la base de datos; se informa que esta información se clasifica

como reservada; por lo que no puede ser entregada, ya que revelar información de nuestros sistemas de bases de datos puede facilitar un ataque informático mediante la explotación de alguna vulnerabilidad de seguridad no corregida por el fabricante del manejador DBMS o la explotación de alguna vulnerabilidad no corregida del lenguaje de programación de las aplicaciones asociadas a los sistemas del Ayuntamiento de Mérida.

2. Respecto a los Diccionarios de Datos: en donde se anexen los diccionarios de datos de cada una de las bases de datos utilizados por el H. Ayuntamiento de Mérida, se informa que esta información se clasifica como reservada; por lo que no puede ser entregada, ya que vulnera potencialmente la seguridad de los datos bajo el resguardo del Ayuntamiento, porque puede utilizarse sola o en combinación con la información solicitada en el Punto 1 de esta solicitud de información, para realizar un ataque informático capaz de obtener e incluso alterar datos personales, privados y confidenciales de terceros, como ciudadanos, empleados, proveedores y del mismo Ayuntamiento.

Por lo antes citado se realizó el acta de reserva 006/2023 de fecha ocho de ocho de noviembre del año en curso, en donde se clasifica como reservada la información antes mencionada con fundamento en los artículos 100, 104, 113 Fracción I; y artículo 114 de la Ley General de Transparencia y Acceso a la Información Pública.

Sin más por el momento me despido, enviándole un afectuoso saludo, quedando a sus órdenes para cualquier aclaración al respecto.

Así también, por Acta de reserva de información emitida por la Dirección de Tecnologías de la Información del Ayuntamiento de Mérida, Yucatán, con número de acta de clasificación: 006/2023, de fecha ocho de noviembre de dos mil veintitrés, se determinó la reserva de la información solicitada de conformidad a la fracción I del artículo 113 de la Ley General de Transparencia y Acceso a la Información Pública, la temporalidad de la reserva y se estableció la prueba de daño, en lo conducente de la forma siguiente:

SEGUNDO.- Es de considerarse reservar la información encontrada recae en el supuesto de la Fracción I del artículo 113 de la Ley General de Transparencia y Acceso a la Información Pública.

Artículo 113. Como información reservada podrá clasificarse aquella cuya publicación:

I. Comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable;

TERCERO.- En merito de lo anterior, se acreditó que, de entregar la documentación correspondiente, causaría daño presente, probable y especifico a la seguridad del Ayuntamiento, en razón de lo siguiente.

Daño presente: Esta información no puede ser entregada, ya que revelar información de nuestros sistemas de bases de datos puede facilitar un ataque informático mediante la explotación de alguna vulnerabilidad de seguridad no corregida por el fabricante del manejador DBMS o la explotación de alguna vulnerabilidad no corregida del lenguaje de programación de las aplicaciones asociadas a los sistemas del Ayuntamiento de Mérida.

Daño probable: Esta información no puede ser entregada, ya que vulnera potencialmente la seguridad de los datos bajo el resguardo del Ayuntamiento, porque puede utilizarse sola o en combinación con la información solicitada en el Punto 1 para realizar un ataque informático capaz de obtener e incluso alterar datos personales, privados y confidenciales de terceros, como ciudadanos, empleados, proveedores y del mismo Ayuntamiento.

Daño específico: Esta información no puede ser entregada, ya que revelar información de nuestros sistemas de bases de datos puede facilitaría un ataque informático mediante la explotación de alguna vulnerabilidad de seguridad no corregida por el fabricante del manejador DBMS o la explotación de alguna vulnerabilidad no corregida del lenguaje de programación de las aplicaciones asociadas a los sistemas vulnerando potencialmente la seguridad de los datos bajo el resguardo del Ayuntamiento.

Por lo expuesto anteriormente y con fundamento en el artículo 100 y 113 Fracción I de la Ley General de Transparencia y Acceso a la Información Pública, se:

ACUERDA

PRIMERO.- Emítase la presente acta, mediante la cual se reserva totalmente la información que posee el área responsable denominada Subdirección de Ingeniería de Software, respecto a los Sistemas de Bases de Datos y Diccionarios de Datos del Ayuntamiento de Mérida, en virtud de que se acredito los supuestos daños presentes y probables que se puedan originar con la publicación y difusión de la información solicitada, encuadrándose de esta manera con el supuesto de la Fracción I del artículo 113 de la Ley General de Transparencia y Acceso a la Información Pública, que a la letra dice:

> ***Artículo 113.*** *Como información reservada podrá clasificarse aquella cuya publicación:*
>
> *Comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable.*

SEGUNDO.- La información reservada estará sujeta a una temporalidad limitada correspondiente al periodo comprendido del 8 de noviembre de 2023 al 8 de noviembre de 2028, por lo que vencido el plazo o cumplida la condición que la origino, la información de referencia deberá ser objeto de libre acceso. Para ello la Dirección de Tecnologías de la Información deberá informar a la Unidad de Transparencia del Ayuntamiento de Mérida, al momento en que se tenga la evidencia de que no subsisten las causas que dieron origen a la reserva.

Por su parte, el comité de transparencia del Ayuntamiento de Mérida, Yucatán, en fecha veintitrés de noviembre del año próximo pasado, emitió el acta número: 215/EXTRAORD/23-11-2023, correspondiente al Acta de la Bicentésima Décima Quinta Sesión Extraordinaria, correspondiente a la administración 2021-2024, a través de la cual el citado Comité de Transparencia, en la página 4, en la parte medular Confirmó la reserva de la información de la forma siguiente:

En ese contexto, este Comité considera que la Dirección de Tecnologías de la Información, clasifica como RESERVADA, toda vez que hacer del dominio público los sistemas de bases de datos y el diccionario de datos, puede comprometer la seguridad pública, por lo cual habría que considerar si se otorga su publicación debido a que recae en el supuesto descrito de esta manera en lo establecido en la fracción I del artículo 113 de la Ley General de Transparencia y Acceso a la Información Pública, puesto que, de divulgar esa información se podría facilitar un ataque informático mediante la explotación de alguna vulnerabilidad de seguridad no corregida por el fabricante del manejador DBMS o la explotación de alguna vulnerabilidad no corregida del lenguaje de programación de las aplicaciones asociadas a los sistemas del Ayuntamiento de Mérida.

En ese sentido debe arribarse a una conclusión que permita el derecho de acceso a la información, conforme al oficio mencionado anteriormente, conforme a lo solicitado por el ciudadano en cuanto a los sistemas de bases de datos y diccionarios de datos. Por cuanto, se le informa que revelar información de nuestros sistemas de bases de datos puede facilitar un ataque informático mediante la explotación de alguna vulnerabilidad de seguridad no corregida por el fabricante del manejador DBMS o la explotación de alguna vulnerabilidad no corregida del lenguaje de programación de las aplicaciones asociadas a los sistemas del Ayuntamiento de Mérida, de igual manera, en lo que respecta a la información contenida en el diccionario de datos puede utilizarse sola o en combinación con la información solicitada en el Punto 1 para realizar un ataque informático capaz de obtener e incluso alterar datos privados y confidenciales de personas terceras, como ciudadanos, empleados, proveedores y del mismo Ayuntamiento, por lo que la información generada que fue solicitada se considera como reservada, ya que de divulgar esa información se podría ocasionar una afectación a la seguridad pública.

En esas condiciones, previo análisis y valoración del oficio y del acta de clasificación No. 0006/2023 de fecha ocho de noviembre del año dos mil veintitrés anteriormente mencionados de la Dirección de Tecnologías de la Información, con apoyo y fundamento en los artículos 44, fracción II y 137 de la Ley General de Transparencia y Acceso a la Información Pública; 54 y 55 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Yucatán; 15 y 16 del Reglamento de Transparencia y Acceso a la Información Pública del Municipio de Mérida y artículo 2 del Manual Interno de Organización y Funcionamiento del Comité de Transparencia del Municipio de Mérida, y por encontrarse debidamente fundada la clasificación de información, por unanimidad de votos de todos los integrantes del Comité se **CONFIRMÓ** la clasificación de **información reservada**, realizada por la Dirección de Tecnologías de la Información.

Con base en lo anterior, a continuación, el Pleno de este Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales, Procederá a valorar la reserva realizada por el Sujeto Obligado, resultando indispensable para ello exponer lo siguiente:

La Ley General de Transparencia y Acceso a la Información Pública, dispone:

"Artículo 2. Son objetivos de esta Ley:

I. Distribuir competencias entre los Organismos garantes de la Federación y las Entidades Federativas, en materia de transparencia y acceso a la información;

II. Establecer las bases mínimas que regirán los procedimientos para garantizar el ejercicio del derecho de acceso a la información;

…

VII. Promover, fomentar y difundir la cultura de la transparencia en el ejercicio de la función pública, el acceso a la información, la participación ciudadana, así como la rendición de cuentas, a través del establecimiento de políticas públicas y mecanismos que garanticen la publicidad de información oportuna, verificable, comprensible, actualizada y completa, que se difunda en los formatos más

adecuados y accesibles para todo el público y atendiendo en todo momento las condiciones sociales, económicas y culturales de cada región;

…

Artículo 4. El derecho humano de acceso a la información comprende solicitar, investigar, difundir, buscar y recibir información. Toda la información generada, obtenida, adquirida, transformada o en posesión de los sujetos obligados es pública y accesible a cualquier persona en los términos y condiciones que se establezcan en la presente Ley, en los tratados internacionales de los que el Estado mexicano sea parte, la Ley Federal, las leyes de las Entidades Federativas y la normatividad aplicable en sus respectivas competencias; sólo podrá ser clasificada excepcionalmente como reservada temporalmente por razones de interés público y seguridad nacional, en los términos dispuestos por esta Ley.

…

Artículo 7. El derecho de acceso a la información o la clasificación de la información se interpretarán bajo los principios establecidos en la Constitución Política de los Estados Unidos Mexicanos, los tratados internacionales de los que el Estado mexicano sea parte y la presente Ley.

En la aplicación e interpretación de la presente Ley deberá prevalecer el principio de máxima publicidad, conforme a lo dispuesto en la Constitución Política de los Estados Unidos Mexicanos, en los tratados internacionales de los que el Estado mexicano sea parte, así como en las resoluciones y sentencias vinculantes que emitan los órganos nacionales e internacionales especializados, favoreciendo en todo tiempo a las personas la protección más amplia.

…

I. Certeza: Principio que otorga seguridad y certidumbre jurídica a los particulares, en virtud de que permite conocer si las acciones de los Organismos garantes son apegadas a derecho y garantiza que los procedimientos sean completamente verificables, fidedignos y confiables;

…

V. Legalidad: Obligación de los Organismos garantes de ajustar su actuación, que funde y motive sus resoluciones y actos en las normas aplicables;

VI. Máxima Publicidad: Toda la información en posesión de los sujetos obligados será pública, completa, oportuna y accesible, sujeta a un claro régimen de excepciones que deberán estar definidas y ser además legítimas y estrictamente necesarias en una sociedad democrática;

…

Artículo 44. Cada Comité de Transparencia tendrá las siguientes funciones:

…

II. Confirmar, modificar o revocar las determinaciones que en materia de ampliación del plazo de respuesta, clasificación de la información y declaración de inexistencia o de incompetencia realicen los titulares de las Áreas de los sujetos obligados;

…

Artículo 100. La clasificación es el proceso mediante el cual el sujeto obligado determina que la información en su poder actualiza alguno de los supuestos de reserva o confidencialidad, de conformidad con lo dispuesto en el presente Título.

Los supuestos de reserva o confidencialidad previstos en las leyes deberán ser acordes con las bases, principios y disposiciones establecidos en esta Ley y, en ningún caso, podrán contravenirla.

Los titulares de las Áreas de los sujetos obligados serán los responsables de clasificar la información, de conformidad con lo dispuesto en esta Ley, la Ley Federal y de las Entidades Federativas.

…

Artículo 103. En los casos en que se niegue el acceso a la información, por actualizarse alguno de los supuestos de clasificación, el Comité de Transparencia deberá confirmar, modificar o revocar la decisión.

Para motivar la clasificación de la información y la ampliación del plazo de reserva, se deberán señalar las razones, motivos o circunstancias especiales que llevaron al sujeto obligado a concluir que el caso particular se ajusta al supuesto previsto por la norma legal invocada como fundamento. Además, el sujeto obligado deberá, en todo momento, aplicar una prueba de daño. Tratándose de aquella información que actualice los supuestos de clasificación, deberá señalarse el plazo al que estará sujeto la reserva.

Artículo 104. En la aplicación de la prueba de daño, el sujeto obligado deberá justificar que:

I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional;

II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda, y

III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio.

Artículo 105. Los sujetos obligados deberán aplicar, de manera restrictiva y limitada, las excepciones al derecho de acceso a la información prevista en el presente Título y deberán acreditar su procedencia.

La carga de la prueba para justificar toda negativa de acceso a la información, por actualizarse cualquiera de los supuestos de reserva previstos, corresponderá a los sujetos obligados.

Artículo 106. La clasificación de la información se llevará a cabo en el momento en que:

I. Se reciba una solicitud de acceso a la información;

II. Se determine mediante resolución de autoridad competente, o

III. Se generen versiones públicas para dar cumplimiento a las obligaciones de transparencia previstas en esta Ley.

…

Artículo 108. Los sujetos obligados no podrán emitir acuerdos de carácter general ni particular que clasifiquen Documentos o información como reservada. La clasificación podrá establecerse de manera parcial o total de acuerdo al contenido de la información del Documento y deberá estar acorde con la actualización de los supuestos definidos en el presente Título como información clasificada. En ningún caso se podrán clasificar Documentos antes de que se genere la información.

La clasificación de información reservada se realizará conforme a un análisis caso por caso, mediante la aplicación de la prueba de daño.

Artículo 109. Los lineamientos generales que emita el Sistema Nacional en materia de clasificación de la información reservada y confidencial y, para la elaboración de versiones públicas, serán de observancia obligatoria para los sujetos obligados.

Artículo 110. Los documentos clasificados serán debidamente custodiados y conservados, conforme a las disposiciones legales aplicables y, en su caso, a los lineamientos que expida el Sistema Nacional.

Artículo 111. Cuando un Documento contenga partes o secciones reservadas o confidenciales, los sujetos obligados, para efectos de atender una solicitud de información, deberán elaborar una Versión Pública en la que se testen las partes o secciones clasificadas, indicando su contenido de manera genérica y fundando y motivando su clasificación.

…

Artículo 137. En caso de que los sujetos obligados consideren que los Documentos o la información deba ser clasificada, se sujetará a lo siguiente:

El Área deberá remitir la solicitud, así como un escrito en el que funde y motive la clasificación al Comité de Transparencia, mismo que deberá resolver para:

a) Confirmar la clasificación;

b) Modificar la clasificación y otorgar total o parcialmente el acceso a la información, y

c) Revocar la clasificación y conceder el acceso a la información.

El Comité de Transparencia podrá tener acceso a la información que esté en poder del Área correspondiente, de la cual se haya solicitado su clasificación. La resolución del Comité de Transparencia será notificada al interesado en el plazo de respuesta a la solicitud que establece el artículo 132 de la presente Ley.

…”

De los preceptos transcritos, es posible concluir que, entre los objetivos de la Ley General de Transparencia y Acceso a la Información pública, se encuentran el de promover, fomentar y difundir la cultura del acceso a la información, a través de la fijación de mecanismos que garanticen la publicidad de la información, de manera oportuna, verificable, comprensible, actualizada y completa, en los formatos accesibles para todo público.

Asimismo, se establece que el derecho de acceso a la información comprende solicitar, investigar, difundir, buscar y recibir toda la información, y debe interpretarse bajo los principios de la Constitución Política de los Estados Unidos Mexicanos y de los tratados internacionales.

En dicha normativa se indica que toda la información generada, obtenida, adquirida, transformada o en posesión de los sujetos obligados, es pública y accesible a cualquier persona, salvo algunas excepciones a causa de la calificación.

Ahora bien, los Organismos garantes, conforme a la normativa en comento deberán regir su comportamiento de acuerdo a los principios de certeza, legalidad y máxima publicidad.

Es obligación de los Organismos Garantes ajustar su actuación, que funde y motive sus resoluciones y actos en las normas aplicables; y por último, deberá regir su funcionamiento en virtud de que toda la información en posesión de los sujetos obligados será pública, completa, oportuna y accesible, sujeta a un claro régimen de excepciones que deberán estar definidas y ser además legítimas y estrictamente necesarias en una sociedad democrática.

Establecido lo anterior, se debe señalar que, en tanto a la clasificación de la información, esta es una excepción al derecho de acceso a la información, pues se trata de un proceso mediante el cual el sujeto obligado determina que la información que obra en su poder actualiza alguno de los supuestos de reserva o confidencialidad, misma que debe aplicarse de manera restrictiva y limitada, debiendo acreditar su procedencia.

En ese sentido, cuando se trate de información clasificada, el Comité de Transparencia resolverá, de manera fundada y motivada, ya sea confirmando, modificando o revocando la clasificación invocada por el área administrativa, señalando las razones, motivos o circunstancias especiales que llevaron al sujet6o obligado a concluir que el caso particular se ajusta a alguna causal de clasificación, realizando en todo momento una prueba de daño.

La prueba de daño que deben señalar los sujetos obligados a fin de comprobar la clasificación de la información, se debe justificar que:

- La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público a la seguridad nacional.
- El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda.
- La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio.

En todo momento, corresponde al sujeto obligado realizar un análisis caso por caso a fin de justificar la negativa de acceso a la información cuando se reciba una solicitud de acceso a la

información, mediante resolución de autoridad competente o en su caso, determinar que se generen versiones públicas para dar atención a las obligaciones de transparencia prevista en la Ley general de la Materia.

La normativa en comento, establece que no podrá emitir acuerdos de carácter general ni particular que clasifiquen documentos o información como reservada, por lo que en ningún caso se podrán clasificar documentos antes de que se genere la información.

Asimismo, se establece que los documentos clasificados serán debidamente custodiados y conservados, conforme a las disposiciones legales aplicables sin que esto sea en demerito que cuando un documento contenga partes o secciones reservadas o confidenciales, los sujetos obligados, para efectos de atender una solicitud de información, deberán elaborar una versión pública en la que se testen las partes o secciones clasificadas, indicando su contenido de manera genérica y fundando y motivando su clasificación.

En concatenación con lo anterior, la Ley de Transparencia y Acceso a la Información Pública del Estado de Yucatán, establece lo siguiente:

"Artículo 6. Acceso efectivo a la información

El Estado garantizará el efectivo acceso de toda persona a la información en posesión de cualquier entidad, autoridad, órgano y organismo de los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos; así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito del estado y los municipios.

…

Artículo 54. Objeto

Los comités de transparencia tienen por objeto garantizar que los sujetos obligados, en los procedimientos de generación de la información, clasificación o desclasificación, y declaración de inexistencia de la información, así como en las determinaciones de ampliación de respuesta, se apeguen a los principios de esta ley y a las disposiciones legales y normativas aplicables.

Artículo 55. Funciones

Los comités de transparencia, para el cumplimiento del objeto de la ley, tendrán las funciones establecidas en el artículo 44 de la Ley general, así como la de identificar las obligaciones que le corresponde cumplir al sujeto obligado y las áreas responsables específicamente de proporcionar la información.

…

Artículo 78. Clasificación

La clasificación es el proceso mediante el cual el sujeto obligado determina que la información en su poder se encuentra en alguno de los supuestos de reserva o confidencialidad. Para tal efecto, los titulares de las áreas de los sujetos obligados serán los responsables de realizar la clasificación de la información, con base en las disposiciones y el procedimiento previsto en el título sexto de la Ley general y los lineamientos generales que emita el sistema nacional.

Artículo 79. Acceso a la información

Cualquier persona, directamente o a través de su representante, podrá ejercer su derecho de acceso a la información, sin que acredite interés alguno o justifique su utilización, mediante la presentación de la solicitud respectiva, a través del procedimiento establecido en el título séptimo de la ley general.

No obstante lo anterior, se entenderá que el plazo previsto en el párrafo primero del artículo 132 de la Ley general, para dar respuesta a la solicitud de acceso, no podrá exceder de diez días hábiles.
…

Artículo 80. Presentación de la solicitud

La solicitud de información pública debe presentarse ante la unidad de transparencia del sujeto obligado.

Cuando se presente una solicitud de información pública ante un área distinta a la unidad de transparencia del sujeto obligado, el titular de dicha área la remitirá a la unidad respectiva y lo notificará al solicitante, dentro de los tres días hábiles siguientes a su recepción.
…”

De conformidad con la normativa en cita, se tiene que los Comités de Transparencia tienen por objeto garantizar que los sujetos obligados, en procedimientos de generación de la información, clasificación o desclasificación y declaración de inexistencia de la información, así como en las determinaciones de ampliaciones de respuesta, se apeguen a los principios de la Ley y demás ordenamientos aplicables.

Las funciones del Comité de Transparencia están establecidas en el artículo 44 de la Ley General, así como identificar las obligaciones que le corresponden cumplir al sujeto obligado y a las áreas responsables.

Respecto a la clasificación, la norma la define como el proceso mediante el cual el Sujeto Obligado determina que la información en su poder se encuentra en alguno de los supuestos de reserva o confidencialidad, para tal efecto, los titulares de las áreas de los sujetos obligados serán los responsables de realizar la clasificación de la información.

La Ley local a través de los artículos 63 y 78, prevé que la clasificación de la información se rige con base en lo establecido en la Ley general, considerando tanto los principios como los casos de excepción previstos en la misma.

El artículo 113 de la Ley General de Transparencia y Acceso a la Información Pública, establece que se podrá clasificar como reservada aquella información cuya publicación:

- **Comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable;**
- **Pueda menoscabar la conducción de las negociaciones y relaciones internacionales;**
- **Se entregue al Estado mexicano expresamente con ese carácter o el de confidencial por otro u otros sujetos de derecho internacional, excepto cuando se trate de violaciones graves de derechos humanos o delitos de lesa humanidad de conformidad con el derecho internacional;**
- **Pueda afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; pueda poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país, pueda comprometer la seguridad en la provisión de moneda nacional al país, o pueda incrementar el costo de operaciones financieras que realicen los sujetos obligados del sector público federal;**
- **Pueda poner en riesgo la vida, seguridad o salud de una persona física;**
- **Obstruya las actividades de verificación, inspección y auditoría relativas al cumplimiento de las leyes o afecte la recaudación de contribuciones;**
- **Obstruya la prevención o persecución de los delitos;**
- **La que contenga las opiniones, recomendaciones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos, hasta en tanto no sea adoptada la decisión definitiva, la cual deberá estar documentada;**
- **Obstruya los procedimientos para fincar responsabilidad a los Servidores Públicos, en tanto no se haya dictado la resolución administrativa;**
- **Afecte los derechos del debido proceso;**
- **Vulnere la conducción de los Expedientes judiciales o de los procedimientos administrativos seguidos en forma de juicio, en tanto no hayan causado estado;**
- **Se encuentre contenida dentro de las investigaciones de hechos que la ley señale como delitos y se tramiten ante el Ministerio Público, y**
- **Las que por disposición expresa de una ley tengan tal carácter, siempre que sean acordes con las bases, principios y disposiciones establecidos en esta Ley y no la**

contravengan; así como las previstas en tratados internacionales.

Así las causales de reserva se deberán fundar y motivar, a través de la aplicación de la prueba de daño. Asimismo, no podrá invocarse el carácter de reservado, de conformidad al numeral 115 de la norma General, cuando se trate de violaciones graves de derechos humanos o delitos de la humanidad, o se trate de información relacionada con actos de corrupción de acuerdo con las leyes aplicables.

Una vez precisado lo anterior, a continuación, el Pleno de este Instituto estima necesario hacer un análisis respecto de las causales invocadas por el Sujeto Obligado, al reservar la información del interés del ciudadano, siendo estas las fracciones XII y XIII del artículo 113 de la Ley General de la Materia.

El artículo 113, fracción I de la Ley General de Transparencia y Acceso a la Información Pública, establece que se considerará como información reservada aquélla que comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un defecto demostrable.

En relación con lo anterior, los Lineamientos Generales establecen lo siguiente:

Décimo noveno. De conformidad con el artículo 113, fracción I de la Ley General, podrá considerarse como información reservada que compromete la defensa nacional, aquella que difunda, actualice o potencialice un riesgo o amenaza que ponga en peligro las misiones generales del Ejército, Fuerza Aérea Mexicana o Armada de México, relacionadas con la defensa del Estado mexicano, para salvaguardar la soberanía y defender la integridad, y permanencia del territorio nacional.

Asimismo, podrá considerarse como reservada aquella que revele datos que pudieran ser aprovechados para conocer la capacidad de reacción del Estado, sus planes, o uso de tecnología, información y producción de los sistemas de armamento y otros sistemas militares incluidos los sistemas de comunicaciones.

Valorando, el proceder de la autoridad, se observa que el Director de Tecnologías de a Información, clasificó como reservada la información relacionada con los sistemas de bases de datos y los diccionarios de datos, toda vez que al otorgar los sistemas de bases de datos se podría facilitar un ataque informático mediante la explotación de alguna vulnerabilidad de seguridad no corregida por el fabricante del manejador DMBS o la explotación de alguna vulnerabilidad no corregida del lenguaje de programación de las aplicaciones asociadas a los sistemas del Ayuntamiento de Mérida, y al suministrar los diccionarios de datos de cada una

de las bases de datos utilizados por el propio Ayuntamiento, se vulneraría potencialmente la seguridad de los datos bajo resguardo del Sujeto Obligado, pues podría utilizarse sola o en combinación con los sistemas de bases de datos, para realizar un ataque informático capaz de obtener e incluso alterar datos personales, privados y confidenciales de terceros, como ciudadanos, empleados, proveedores y del mismo Ayuntamiento.

Cabe señalar que un sistema de gestión de bases de datos (SGDB) es software que permite crear, almacenar, manipular y recuperar datos en una o más bases de datos. Los SGBD facilitan la interacción entre los usuarios y las aplicaciones con los datos, mediante una interfaz que utiliza un lenguaje de consulta específico. Los SGBD también se encargan de garantizar la seguridad, la integridad, la consistencia y el rendimiento de los datos.

Existen diferentes tipos de SGBD según el modelo de datos que utilizan, como los relacionales, los documentales, los columnares o los orientados a objetos. Cada tipo de SGBD tiene sus ventajas y desventajas, y se adapta mejor a ciertos escenarios y necesidades.

Así también, es necesario referir que un diccionario de datos es un componente esencial en la gestión de bases de datos y sistemas de información. Es una herramienta que describe de manera detallada, los elementos que componen una base de datos, proporcionando información sobre su estructura, significado, relaciones y otros atributos.

Un diccionario de datos es una herramienta crucial para entender y documentar la estructura de una base de datos, facilitando el desarrollo, la administración y el mantenimiento del sistema de información.

Ahora bien, la autoridad señala que la reserva de la información tiende a evitar ataques cibernéticos, como consecuencia de estos ataques, los criminales informáticos pueden:

- Apropiarse de información del Ayuntamiento de Mérida, Yucatán.
- Explotar alguna vulnerabilidad de seguridad no corregida por el fabricante del manejador DMBS.
- Explotar alguna vulnerabilidad no corregida del lenguaje de programación de las aplicaciones asociadas a los sistemas del Ayuntamiento de Mérida.

A mayor abundamiento, se distingue los siguientes tipos de ataques a sistemas informáticos según la Comisión de las Comunidades Europeas:

1. Acceso no autorizado a sistemas de información: esto incluye el concepto de piratería informática, la cual consiste en tener acceso de manera no autorizada a una computadora o

una red de computadoras. Puede tomar distintas formas que van desde el uso de informaciones internas a ataques directos y la intercepción de contraseñas.

2. La perturbación de los sistemas de información: existen distintas maneras de perturbar los sistemas de información mediante ataques malintencionados. Uno de los medios más conocidos de denegar o deteriorar los servicios ofrecidos es el ataque tipo denegación de servicio (DdS). Este ataque es en cierta medida similar al hecho de inundar las máquinas de faz con mensajes largos y repetidos. Los ataques del tipo denegación de servicio tienen por objeto sobrecargar los servidores o los proveedores de servicios de internet con mensajes generados automáticamente.
3. Ejecución de programas informáticos perjudiciales que modifican o destruyen datos: el tipo más conocido de programa informático malintencionado es el virus. Algunos dañan a la propia computadora, mientras que otros utilizan el PC para atacar otros elementos de la red.
4. Intervención de las comunicaciones: La intervención malintencionada de comunicaciones afecta los requisitos de confidencialidad e integridad de los usuarios.
5. Declaraciones falsas: Los sistemas de información ofrecen nuevas posibilidades de declaraciones faltas y de fraude. El hecho de usurpar la identidad de otra persona en internet y de utilizarla con fines malintencionados se llama spoofing.

Respecto de la naturaleza del riesgo, la Comisión de las Comunidades Europeas señala lo siguiente: existe la necesidad de desarrollar estudios confiables sobre la amplitud y la naturaleza de los ataques contra los sistemas informáticos. los ataques más graves contra los sistemas de información se dirigen a los operadores de redes de comunicaciones electrónicas y a los servidores de servicios o a las sociedades de comercio electrónico. Los ámbitos más tradicionales pueden también verse afectados seriamente debido al nivel de interconexión cada vez mayor en las comunicaciones modernas; las fábricas, los servicios, hospitales, organismos del sector público y gobiernos. Existe una preocupación creciente de que las bandas de delincuencia organizada utilicen las redes de comunicación para lanzar ataques contra los sistemas de información. En los últimos tiempos, las tensiones a escala internacional han supuesto un recrudecimiento de los ataques contra los sistemas de información y, de manera concreta, contra sitios de Internet. Unos ataques más graves podrían no sólo tener serias consecuencias financieras, sino, además, en algunos casos, implicar la pérdida de vidas humanas (sistemas hospitalarios, sistemas de control de tráfico aéreo, por ejemplo).

En este orden de ideas, se tiene que el Código Penal del Estado de Yucatán, en vigor, prevé el tipo de conductas antijurídicas que deben sancionarse como delitos informáticos y cibernéticos, a saber, los dispuestos en sus artículos 243 Bis 5, 243 Bis 6, 243 Bis 7, 243 Bis 8, 243 Bis 9, 243 Bis 10, 243 Bis 11, 243 Bis 12, que refieren el acceso ilícito a sistemas y equipos de informática, conductas que pueden considerarse como hacking informático; mismas que consisten en la modificación, destrucción, la provocación a perder, el conocer o copiar información que esté contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, sean de particulares o del Estado.

De lo anteriormente señalado se advierte que los delitos informáticos permiten acceder a información sensible de las personas, pero también a información de carácter restringido de una institución, con la cual personas ajenas puedan dañar o generar afectaciones a la vida privada de las personas, así como el funcionamiento habitual de las instituciones públicas, generando con ello daños morales y materiales, respectivamente.

Derivado de lo anterior, se advierten elementos establecidos en el artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, en razón de que se funda y motiva la reserva mediante la prueba de daño, en los términos siguientes:

- **Daño presente:** Esta información no puede ser entregada, ya que revelar información de los sistemas de bases de datos del Ayuntamiento de Mérida, Yucatán, puede facilitar un ataque informático mediante la explotación de alguna vulnerabilidad de seguridad no corregida por el fabricante del manejador DBMS o la explotación de alguna vulnerabilidad no corregida del lenguaje de programación de las aplicaciones asociadas a los sistemas del propio Ayuntamiento.

- **Daño probable:** Esta información no puede ser entregada, toda vez que pondría en riesgo potencial la seguridad de los datos bajo el resguardo del Sujeto Obligado, pues podría utilizarse sola o en combinación (sistemas de bases de datos y diccionarios de datos), para realizar un ataque informático capaz de obtener y alterar datos personales, privados y confidenciales de terceros, como ciudadanos, empleados, proveedores y del mismo Ayuntamiento.

- **Daño específico:** la Información solicitada no puede ser divulgada, pues darla a conocer vulneraría la protección de los sistemas de bases de datos, los diccionarios de datos, y con ello la información que con ellos resguarda el Ayuntamiento de Mérida, Yucatán, en tanto que se podrían acceder a la información inmersa en aquellos y con esto, se potencializaría el nivel de vulnerabilidad de un ataque cibernético, lo que deviene en un riesgo contra la seguridad informática del Sujeto Obligado al tener la posibilidad de tener un daño irreversible en los sistemas de bases de datos y diccionarios de datos, como consecuencia de la posible comisión de un delito, que le constituye delitos informáticos y cibernéticos tipificados en el Código Penal del Estado de Yucatán, en vigor, pues la publicación de la información podría vulnerar o contrarrestar las acciones que tiene implementado el Ayuntamiento de Mérida, Yucatán en materia de seguridad informática y que permite proteger el funcionamiento de los sistemas de bases de datos y diccionarios de datos del Ayuntamiento. Esto es, daría cuenta de posibles vulnerabilidades que potencializarían el robo de información o cualquier ataque a ésta,

afectando la seguridad de los datos bajo el resguardo del Ayuntamiento de Mérida, Yucatán.

Ahora bien, en la Ley General de Transparencia y Acceso a la Información Pública, en su artículo 101, segundo párrafo establece que la información clasificada como reservada, según el ordinal 113 de la propia Ley, podrá permanecer con tal carácter hasta por un periodo de cinco años. Asimismo, señala que los documentos reservados serán desclasificados cuando extingan la causa que dio origen a su clasificación.

A efecto de procurar que el periodo de reserva sea el estrictamente necesario, este Órgano Garante considera que la información solicitada y que se propone reservar debe permanecer con este carácter por el periodo de cinco años, tal como lo manifestó el Sujeto Obligado por conducto de la Dirección de Tecnologías de la Información.

Posteriormente, el Comité de Transparencia del Ayuntamiento de Mérida, Yucatán, a través del Acta de la Bicentésima Décima Quinta sesión extraordinaria correspondiente a la administración 2021-2024, de fecha veintitrés de noviembre de dos mil veintitrés, consideró procedente CONFIRMAR la clasificación de la información referida en la solicitud de acceso con folio 310579123000821, como reservada realizada por la Dirección de Tecnologías de la Información.

Finalmente, el Pleno de este Órgano Garante, como refuerzo de lo anterior, tiene a bien citar el oficio de respuesta de la Coordinación de Tecnologías de la Información y Administración de Sistemas perteneciente a la Dirección de Asuntos Jurídicos y Plenarios del Instituto Estatal de Transparencia, Acceso a la Información Pública y Protección de Datos Personales de este Instituto, el cual contiene el respectivo **pronunciamiento técnico**, presentado ante la Oficialía de Partes de este Organismo Autónomo el día ocho de marzo del año en curso, con motivo del requerimiento que se le hiciere por acuerdo de fecha veintisiete de febrero de dos mil veinticuatro, con la finalidad de recabar mayores elementos para resolver e impartir una justicia completa y efectiva, acorde a los artículos 6 y 17 de la Constitución Política de los Estados Unidos Mexicanos, con fundamento en los artículos 61 de la Ley de Actos y Procedimientos Administrativos del Estado de Yucatán, aplicado de manera supletoria de conformidad al diverso 8, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Yucatán, y 46 fracción XVIII del Reglamento Interior del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, vigente, para efectos que emitiera el **pronunciamiento técnico** respecto a la respuesta brindada por el Sujeto Obligado por conducto de la Dirección de Tecnologías de la Información, a través del oficio número DTI/375/2023, de fecha nueve de noviembre de dos mil veintitrés, a la solicitud de acceso con número de folio 310579122000821, así también, en cuanto a la contestación de la autoridad realizada por oficio número DTI/043/2024, de fecha veintitrés de febrero de dos mil veinticuatro, signado por el Director de Tecnologías de la Información del

Ayuntamiento de Mérida, Yucatán, derivado del requerimiento que el Comisionado Ponente en el recurso de revisión que nos compete, por acuerdo de fecha nueve de febrero del año en curso; lo anterior, bajo el apercibimiento que en caso de no realizar manifestación alguna, se acordaría conforme a derecho correspondiera.

No pasa inadvertido para el Cuerpo Colegiado de este Instituto, las constancias remitidas por el Ayuntamiento de Mérida, Yucatán, con motivo del requerimiento que le fuere realizado mediante proveído de fecha nueve de febrero del año en curso, mismas que fueran enviadas al secreto de este Órgano Garante.

Al respecto, en la presente definitiva con motivo de la confirmación de la reserva en la información objeto de estudio, se determina que las citadas documentales sean devueltas en su integridad al Ayuntamiento de Mérida, Yucatán, a través del Titular de la Unidad de Transparencia del propio Ayuntamiento, a partir del día posterior a la fecha en que se efectúe la notificación de la resolución que nos compete, en el día y hora que así le sea factible al Sujeto Obligado, y en consecuencia, el secreto en cuestión dejará de subsistir en el recurso de recurso de revisión en que se actúa.

Consecuentemente, se considera que la Clasificación con carácter de reservada realizada por el Ayuntamiento de Mérida, Yucatán, Sí resulta ajustada a derecho, pues se advierte que la reserva estuvo debidamente fundada y motivada a través de la aplicación de la prueba de daño, en la cual el Sujeto Obligado justificó que la divulgación de la información representa un daño presente, probable y específico de perjuicio significativo e irreparable a las acciones que tiene implementado el Ayuntamiento de Mérida, Yucatán en materia de seguridad informática y que permite proteger el funcionamiento de los sistemas de bases de datos y diccionarios de datos del propio Ayuntamiento. Esto es, daría cuenta de posibles vulnerabilidades que potencializarían el robo de información o cualquier ataque a ésta, afectando la seguridad de los datos bajo el resguardo del Sujeto Obligado. Por todo lo anterior, el agravio en estudio resulta infundado.

SENTIDO: Se **CONFIRMA** la clasificación de la información requerida en la solicitud de acceso con folio 310579123000821 como reservada, realizada por el Ayuntamiento de Mérida, Yucatán.

Plazo para cumplir e informar lo ordenado: No resulta aplicable.

KAPC/JAPC/HNM.
SESIÓN DEL 14/MARZO/2024