Resolución del Pleno del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios, con domicilio en Metepec, Estado de México, de fecha **dos de abril de dos mil veinticinco**.

Visto el expediente relativo al recurso de revisión **01299/INFOEM/IP/RR/2025**, interpuesto por **una persona usuaria del Sistema de Acceso a la Información Mexiquense que no proporcionó nombre** al cual en lo sucesivo se le denominará la parte **Recurrente**, en contra de la respuesta a su solicitud de información identificada con número de folio **00375/TOLUCA/IP/2025**, proporcionada por parte del **Ayuntamiento de Toluca**, en lo sucesivo el **Sujeto Obligado**; se procede a dictar la presente resolución, con base en los siguientes:

**I. A N T E C E D E N T E S**

1. **Solicitud de acceso a la información.** Con fecha **diecinueve de enero de dos mil veinticinco**, la parte **Recurrente** formuló solicitud de acceso a información pública al **Sujeto Obligado** a través del Sistema de Acceso a la Información Mexiquense, en adelante SAIMEX; sin embargo, al corresponder a un día inhábil se tuvo por presentada el día **veinte de enero de dos mil veinticinco**, misma a la que se le asignó el número **00375/TOLUCA/IP/2025**, mediante la cual se requirió la información siguiente:

*“Solicito todos los avisos de Privacidad Integrales y Simplificados de todas las áreas administrativas del Sujeto Obligado. Documentos de seguridad, número de bases de datos con registros, cédulas de cada base de datos. Responsable de cada base de datos actualizadas y las nuevas bases de datos dadas de alta en su administración actual” (Sic)*

**Modalidad elegida para la entrega de la información:** a través del Sistema de Acceso a la Información Mexiquense (SAIMEX).

1. **Respuesta.** Con fecha **once de febrero de dos mil veinticinco**, el **Sujeto Obligado** envió su respuesta a la solicitud de acceso a la información a través del SAIMEX, la cual versa como sigue:

*“…En atención a la solicitud con folio 0375/TOLUCA/IP/2025, me permito adjuntar al presente la respuesta correspondiente. Sin más por el momento, reciba un saludo.” (Sic)*

Asimismo, adjuntó a su respuesta el archivo electrónico que contiene la siguiente información:

* ***RESPUESTA 375. 2025.pdf:*** Oficio del 11 de febrero de 2025, a través del cual el Titular de la Unidad de Transparencia hizo del conocimiento de la persona solicitante, que derivado de la una búsqueda exhaustiva y razonable de la información, se informaba que lo requerido aún se encontraba en proceso de integración y por tanto no era posible hacer entrega de ello.
1. **Interposición del Recurso de Revisión**. La parte Solicitante, derivado de la respuesta del **Sujeto Obligado** interpuso Recurso de Revisión a través del **SAIMEX** en fecha **doce de febrero de dos mil veinticinco**, a través del cual expresó lo siguiente:

**Acto impugnado.** “*La respuesta de la unidad de transparencia*” (*Sic*)

**Razones o motivos de la inconformidad:** *“Informa que se está integrando y no dan lo que se pide pareciera que la están ocultando”* (*Sic*)

1. **Turno.** De conformidad con el artículo 185, fracción I de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, el recurso de revisión número **01299/INFOEM/IP/RR/2025**, se turnó por el sistema electrónico del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios, a la Comisionada Guadalupe Ramírez Peña para su análisis, estudio, elaboración del proyecto y presentación ante el Pleno de este Instituto.
2. **Admisión del recurso de revisión**: En fecha **diecisiete de febrero de dos mil veinticinco**, la Comisionada Ponente admitió a trámite el recurso de revisión que ahora se resuelve, dando un plazo máximo de siete días hábiles para que las partes manifestaran lo que a su derecho resultara conveniente, ofrecieran pruebas, formularan alegatos y el Sujeto Obligado presentara su informe justificado.
3. **Manifestaciones.** De las constancias que obran en el expediente electrónico aperturado con motivo del presente medio de impugnación, se advierte que el **Sujeto Obligado** en fecha **veintiséis de febrero de dos mil veinticinco** rindió su informe justificado a través del archivo electrónico denominado “[***RR-1299-2025.pdf***](https://saimex.org.mx/saimex/solicitud/downloadAttach/2371126.page)” que contiene un oficio de esa misma fecha, a través del cual el Titular de la Unidad de Transparencia rinde informe justificado, en el que **medularmente ratificó su respuesta inicial.**

Documento el anterior, que se hizo del conocimiento de la parte **Recurrente** a fin de que hiciera valer alegatos o manifestaciones que conforme a derecho resultaran procedentes; no obstante, fue omisa en ejercer dicha prerrogativa.

1. **Cierre de instrucción**. En fecha **veintiséis de marzo de dos mil veinticinco**, la Comisionada Ponente determinó el cierre de instrucción en términos de la fracción VI del artículo 185 de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios.

Debido a que fue debidamente sustanciado el expediente electrónico y no existe diligencia pendiente de desahogo, se emite la Resolución que conforme a Derecho proceda, de acuerdo con los siguientes:

**II. C O N S I D E R A N D O:**

**Primero. Competencia.** El Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios, es competente para conocer y resolver el presente recurso de revisión interpuesto por la parte recurrente, conforme a lo dispuesto en los artículos 6, apartado A de la Constitución Política de los Estados Unidos Mexicanos; 5, párrafos trigésimo séptimo, trigésimo octavo y trigésimo noveno fracciones IV y V de la Constitución Política del Estado Libre y Soberano de México; 1, 2, fracción II; 13, 29, 36, fracciones I y II; 176, 178, 179, 181 párrafo tercero y 185 de la Ley Transparencia y Acceso a la Información Pública del Estado de México y Municipios; 9, fracciones I y XXIII y 11 del Reglamento Interior del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios.

**Segundo. Oportunidad y Procedibilidad del Recurso de Revisión.** Previo al estudio del fondo del asunto, se procede a analizar los requisitos de oportunidad y procedibilidad que deben reunir el recurso de revisión interpuesto, previstos en los artículos 178 y 180 de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios.

El recurso de revisión fue interpuesto dentro del plazo de quince días hábiles previstos en el artículo 178 de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, toda vez que el **Sujeto Obligado** remitió la respuesta a la solicitud de información el **once de febrero de dos mil veinticinco**, mientras que el recurso de revisión interpuesto por la parte **Recurrente** se tuvo por presentado el **doce de febrero de dos mil veinticinco**, esto es al **primer** día hábil siguiente a aquel en que se tuvo conocimiento de la respuesta.

En este sentido, se concluye que el presente recurso de revisión se encuentra dentro de los márgenes temporales previstos en las disposiciones legales referidas.

Por otro lado, es de suma importancia mencionar que, si bien la parte **Recurrente** no **proporcionó nombre,** como se advierte en el detalle de seguimiento del SAIMEX; sin embargo, el no proporcionar un nombre no es motivo para archivar la solicitud de acceso a la información pública como concluida, conforme a lo previsto en el artículo 155, penúltimo párrafo de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios que establece lo siguiente:

*"****Las solicitudes anónimas,*** *con nombre incompleto o seudónimo****serán procedentes para su trámite por parte del sujeto obligado ante quien se presente****. No podrá requerirse información adicional con motivo del nombre proporcionado por el solicitante."*

Ahora bien, del análisis efectuado se advierte que resulta procedente la interposición del recurso y se concluye la acreditación plena de todos y cada uno de los elementos formales exigidos por el artículo 180 de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios en vigor, en atención a que fue presentado mediante el formato visible en **SAIMEX**.

Finalmente, se advierte que resulta procedente la interposición del recurso, según lo manifestado por **la parte** **Recurrente** en sus motivos de inconformidad, de acuerdo al artículo 179, fracción I del ordenamiento legal citado, que a la letra dice:

*“****Artículo 179.*** *El recurso de revisión es un medio de protección que la Ley otorga a los particulares, para hacer valer su derecho de acceso a la información pública, y procederá en contra de las siguientes causas:*

***I. La negativa a la información solicitada;****[…]”*

*(Énfasis añadido)*

**Tercero. Materia de la revisión.** De la revisión a las constancias y documentos que obran en el expediente electrónico se advierte que, el tema sobre el que este Organismo Garante de Transparencia y Acceso a la Información se pronunciará será: **verificar si la respuesta e informe justificado otorgados por el Sujeto Obligado son adecuados y suficientes para satisfacer el derecho de acceso a la información pública de la parte Recurrente,** o en su defecto, en caso de ser procedente, ordenar la entrega de la información oportuna.

**Cuarto. Estudio del asunto.** Antes de entrar al análisis de los pronunciamientos del **Sujeto Obligado** en la respuesta proporcionada, es necesario mencionar que el derecho de acceso a la información está consagrado en instrumentos internacionales de los cuales el Estado Mexicano se ha adherido, sin oponer reserva alguna sobre lo que nos interesa, adoptando dichas disposiciones al Derecho Interno, específicamente a nivel Constitucional, tal y como lo prevén los arábigos 1 párrafos primero, segundo y tercero y 6 apartado A fracciones I, II, III, IV, V, VI y VII que a la letra señalan:

***Artículo 1o. En los Estados Unidos Mexicanos todas las personas gozarán de los derechos humanos reconocidos en esta Constitución y en los tratados internacionales de los que el Estado Mexicano sea parte****, así como de las garantías para su protección, cuyo ejercicio no podrá restringirse ni suspenderse, salvo en los casos y bajo las condiciones que esta Constitución establece.*

***Las normas relativas a los derechos humanos se interpretarán de conformidad con esta Constitución y con los tratados internacionales de la materia favoreciendo en todo tiempo a las personas la protección más amplia.***

***Todas las autoridades, en el ámbito de sus competencias, tienen la obligación de promover, respetar, proteger y garantizar los derechos humanos de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad.*** *En consecuencia, el Estado deberá prevenir, investigar, sancionar y reparar las violaciones a los derechos humanos, en los términos que establezca la ley*

*[…]*

***“Artículo 6o.***

*[...]*

***A. Para el ejercicio del derecho de acceso a la información, la Federación y las entidades federativas,*** *en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:*

***I. Toda la información en posesión de cualquier autoridad, entidad, 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 federal, estatal y municipal,* ***es pública y sólo podrá ser reservada temporalmente por razones de interés público y seguridad nacional,*** *en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad. Los sujetos obligados deberán documentar todo acto que derive del ejercicio de sus facultades, competencias o funciones, la ley determinará los supuestos específicos bajo los cuales procederá la declaración de inexistencia de la información.*

***II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes. Para tal efecto, los sujetos obligados contarán con las facultades suficientes para su atención.***

*[]*

***III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública,*** *a sus datos personales o a la rectificación de éstos.*

***IV. Se establecerán mecanismos de acceso a la información y procedimientos de revisión expeditos que se sustanciarán ante las instancias competentes en los términos que fija esta Constitución y las leyes.***

***V.*** *Los sujetos obligados deberán preservar sus documentos en archivos administrativos actualizados y publicarán, a través de los medios electrónicos disponibles, la información completa y actualizada sobre el ejercicio de los recursos públicos y los indicadores que permitan rendir cuenta del cumplimiento de sus objetivos y de los resultados obtenidos.*

***VI.*** *Las leyes determinarán la manera en que los sujetos obligados deberán hacer pública la información relativa a los recursos públicos que entreguen a personas físicas o morales.*

***VII.*** *La inobservancia a las disposiciones en materia de acceso a la información pública será sancionada en los términos que dispongan las leyes. [...]”*

Esto es, que cualquier persona tiene el derecho al acceso de la información pública, información que consiste en aquella que sea generada, obtenida, adquirida, transformada, administrada o en posesión de los Sujetos Obligados, como así también lo señala la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios en su artículo 4, que toda la información generada, obtenida, adquirida, transformada, administrada o en posesión de los sujetos obligados, es pública y accesible, de manera permanente a cualquier persona, privilegiando el principio de máxima publicidad, como así lo establece dicha determinación, que a continuación se transcribe para un mejor entendimiento:

*“****Artículo 4****. El derecho humano de acceso a la información pública es la prerrogativa de las personas para buscar, difundir, investigar, recabar, recibir y solicitar información pública, sin necesidad de acreditar personalidad ni interés jurídico.*

***Toda la información generada, obtenida, adquirida, transformada, administrada o en posesión de los sujetos obligados es pública y accesible de manera permanente a cualquier persona****, en los términos y condiciones que se establezcan en los tratados internacionales de los que el Estado mexicano sea parte, en la Ley General, la presente Ley y demás disposiciones de la materia, privilegiando el principio de máxima publicidad de la información. Solo podrá ser clasificada excepcionalmente Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios 29 como reservada temporalmente por razones de interés público, en los términos de las causas legítimas y estrictamente necesarias previstas por esta Ley.*

***Los sujetos obligados deben poner en práctica, políticas y programas de acceso a la información que se apeguen a criterios de publicidad, veracidad, oportunidad, precisión y suficiencia en beneficio de los solicitantes****.”*

Esto es, que los Sujetos Obligados tiene la obligación o deber de atender las solicitudes de acceso a la información pública que se les hagan de su conocimiento y proporcionar la información pública que obren en su poder conforme el estado que se encuentra y no hacer un procesamiento de la misma, ni presentarla conforme al interés del solicitante; como así lo establece el artículo 12 de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, que a la letra dice:

***“Artículo 12.-*** *Quienes generen, recopilen, administren, manejen, procesen, archiven o conserven información pública serán responsables de la misma en los términos de las disposiciones jurídicas aplicables.*

***Los sujetos obligados sólo proporcionarán la información pública que se les requiera y que obre en sus archivos y en el estado en que ésta se encuentre****.* ***La obligación de proporcionar información no comprende el procesamiento de la misma, ni el presentarla conforme al interés del solicitante; no estarán obligados a generarla, resumirla, efectuar cálculos o practicar investigaciones”.***

Es decir, que todo sujeto obligado que genere, recopile, administre, procese, archive, posea o conserven, son responsables de la misma teniendo a su vez la obligación de proporcionar la información que se les requiera sin necesidad de resumirla, efectuar procedimientos para obtenerla, calcular y practicar investigaciones; en otras palabras, que los Sujetos Obligados sólo se concretaran a proporcionar la información solicitada que tengan en su poder en el estado que se encuentran, sin necesidad de concretarse al interés o términos específicos del solicitante.

Sirve de apoyo a lo anterior, el criterio orientador 03-17, expuesto por el entonces Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, que dice:

*“****No existe obligación de elaborar documentos ad hoc para atender las solicitudes de acceso a la información.*** *Los artículos 129 de la Ley General de Transparencia y Acceso a la Información Pública y 130, párrafo cuarto, de la Ley Federal de Transparencia y Acceso a la Información Pública, señalan que los sujetos obligados deberán otorgar acceso a los documentos que se encuentren en sus archivos o que estén obligados a documentar, de acuerdo con sus facultades, competencias o funciones, conforme a las características físicas de la información o del lugar donde se encuentre. Por lo anterior, los sujetos obligados deben garantizar el derecho de acceso a la información del particular, proporcionando la información con la que cuentan en el formato en que la misma obre en sus archivos; sin necesidad de elaborar documentos ad hoc para atender las solicitudes de información”.*

En esa tesitura, el artículo 24 en su último párrafo de la Ley de la Materia, dispone que los Sujetos Obligados sólo proporcionarán la información pública que generen, administren o posean en el ejercicio de sus atribuciones; por consiguiente, la información pública se encuentra a disposición de cualquier persona, lo que implica que es deber de los Sujetos Obligados, garantizar el Derecho de Acceso a la Información Pública.

Siempre y cuando no se trate de información reservada o clasificada, que difundirla pondría en riesgo la seguridad jurídica y física del titular de la información, debiendo tener audacia los Sujetos Obligados para cuidar esta información a través del acuerdo clasificatorio del comité de transparencia y la versión pública que emita el servidor público habilitado de cada Sujeto Obligado; como así se establece en la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios.

En conclusión, el derecho de acceso a la información pública, consiste en que la información solicitada conste en un documento en cualquiera de sus formas, a saber: expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro que documente el ejercicio de las facultades, funciones y competencias de los Sujetos Obligados; los que, podrán estar en cualquier medio, sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico de conformidad con el artículo 3, fracción XI de la Ley de la materia, el cual señala lo siguiente:

*“****Artículo 3.*** *Para los efectos de la presente Ley se entenderá por:*

*…*

***XI. Documento:*** *Los expedientes, reportes, estudios, actas****,*** *resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro que documente el ejercicio de las facultades, funciones y competencias de los sujetos obligados, sus servidores públicos e integrantes, sin importar su fuente o fecha de elaboración. Los documentos podrán estar en cualquier medio, sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico…”*

Siendo aplicable, el Criterio de interpretación en el orden administrativo número 0002-11, emitido por Acuerdo del Pleno del Instituto de Transparencia y Acceso a la Información Pública del Estado de México y Municipios; publicado en el Periódico Oficial del Gobierno del Estado Libre y Soberano de México “Gaceta del Gobierno”, el diecinueve de octubre de dos mil once, cuyo rubro y texto refieren lo siguiente:

**“*CRITERIO 0002-11. INFORMACIÓN PÚBLICA, CONCEPTO DE, EN MATERIA DE TRANSPARENCIA. INTERPRETACIÓN SISTEMÁTICA DE LOS ARTÍCULOS 2°, FRACCIÓN V, XV, Y XVI, 3°, 4°, 11 Y 41.*** *De conformidad con los artículos antes referidos, el derecho de acceso a la información pública, se define en cuanto a su alcance y resultado material, el acceso a los archivos, registros y documentos públicos, administrados, generados o en posesión de los órganos u organismos públicos, en virtud del ejercicio de sus funciones de derecho público, sin importar su fuente, soporte o fecha de elaboración.*

*En consecuencia el acceso a la información se refiere a que se cumplan cualquiera de los siguientes tres supuestos:*

*1) Que se trate de información registrada en cualquier soporte documental, que en ejercicio de las atribuciones conferidas, sea generada por los Sujetos Obligados;*

***2) Que se trate de información registrada en cualquier soporte documental, que en ejercicio de las atribuciones conferidas, sea administrada por los Sujetos Obligados, y***

***3) Que se trate de información registrada en cualquier soporte documental, que en ejercicio de las atribuciones conferidas, se encuentre en posesión de los Sujetos Obligados.”***

De ahí que el **Sujeto Obligado** cuenta con el deber de satisfacer las solicitudes de acceso a la información que le sean formuladas y entregar la información pública que obre en sus archivos pudiendo ser de manera electrónica; más aún si la misma se trata de información relativa a obligaciones de transparencia, la cual se relaciona con aquella que se genere de acuerdo con sus facultades, atribuciones y obligaciones señaladas por la Ley en la materia[[1]](#footnote-1), así como de interés público, es decir, aquella que resulta relevante o beneficiosa para la sociedad y no simplemente de interés individual, y cuya divulgación resulta útil para que el público comprenda las actividades que llevan a cabo los Sujetos Obligados[[2]](#footnote-2), como pudiera tratarse de aquella relacionada con las obligaciones de transparencia señaladas en los artículos 92 y 100 de la Ley de la Materia.

Para ello, conviene iniciar el presente estudio señalando que, del análisis a la solicitud de información se advierte que la persona solicitante requirió al **Sujeto Obligado,** lo siguiente:

*“…todos los avisos de Privacidad Integrales y Simplificados de todas las áreas administrativas del Sujeto Obligado. Documentos de seguridad, número de bases de datos con registros, cédulas de cada base de datos. Responsable de cada base de datos actualizadas y las nuevas bases de datos dadas de alta en su administración actual” (Sic)*

En respuesta, el **Sujeto Obligado** por conducto del Titular de la Unidad de Transparencia hizo del conocimiento de la persona solicitante, que derivado de la una búsqueda exhaustiva y razonable de la información, se informaba que lo requerido aún se encontraba en proceso de integración y por tanto no era posible hacer entrega de ello.

Inconforme con la respuesta, la parte **Recurrente** promovió el recurso de revisión que nos ocupa, en el que se inconformó medularmente de la **negativa a la entrega de la información requerida.**

Admitido el presente recurso de revisión, en términos del artículo 185 fracción II[[3]](#footnote-3) de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, se integró el expediente y se puso a disposición de las partes para que, en un plazo máximo de siete días hábiles, manifestaran lo que a su derecho resultara conveniente.

Cabe resaltar que, durante la etapa de manifestaciones**,** el **Sujeto Obligado** rindió su informe justificado en el que medularmente ratificó su respuesta inicial.

Por su lado, **la parte Recurrente** fue omisa en hacer valer manifestaciones o rendir alegatos que conforme a derecho resultaran procedentes con relación al informe justificado rendido por el **Sujeto Obligado.**

Una vez establecidas las posturas de las partes, previo al análisis de fondo, resulta necesario aclarar que, por cuanto hace al requerimiento relativo a “***las nuevas bases de datos dadas de alta en su administración actual***” se entiende que lo que el particular solicita no son todos los expedientes y registros de datos personales, sino, que se le entregue el nombre de cada una de las bases de datos con las que cuenta el Ayuntamiento a la fecha de la solicitud, de tal suerte que pueda identificarlas, por lo que, dicho dato, se colmará con la entrega que se haga del documento de seguridad, como se abordará más adelante.

Asimismo, por lo que corresponde a los requerimientos relativos a ***“número de bases de datos con registros”*** y “***responsable de cada base de datos***”; se advierte que la pretensión del particular es acceder al número de bases de datos registradas, así como a los servidores públicos responsables de las bases de datos; datos que de igual manera, como se precisará más adelante podrán colmarse con la entrega del documento de seguridad, al ser la documental en cuyo contenido se desprende dicha información.

Precisado lo anterior, se considera que para mayor proveer, el análisis del presente asunto debe versar en la siguiente información requerida:

**Con vigencia a la fecha de la solicitud -20 de enero de 2025-:**

1. Documentos de seguridad actualizados.
2. Cédulas de las bases de datos que se tienen registradas.
3. Todos los avisos de privacidad (integrales y simplificados) de todas las áreas administrativas del Sujeto Obligado.

Al respecto, en el caso resulta necesario recordar que quien se pronunció fue el Titular de la Unidad de Transparencia, área que conforme el artículo 114, fracción II, del Bando Municipal de Toluca, dos mil veinticinco, en relación con el artículo 5.41 fracción I, del Código Reglamentario Municipal, se encuentra bajo la estructura orgánica del Ayuntamiento de Toluca y es la encargada de conocer todo lo relacionado a garantizar el derecho de acceso a la información, y la protección de datos personales de la Administración Municipal.

Así, se advierte que fue la propia Unidad de Transparencia en su calidad de Servidor Público Habilitado quien atendió la solicitud, que ve las cuestiones relacionadas con el derecho de acceso a la información y la protección de datos personales del Ayuntamiento de Toluca.

Ahora bien, dicha área tanto en respuesta, como en informe justificado, indicó que la información se encontraba en proceso de integración, por lo que no podía hacer entrega de lo peticionado. Así, con base en dichas manifestaciones, el área competente no negó que genera y administra la información solicitada, sino que, a la fecha de la solicitud, esta se encontraba en proceso de integración.

Por tanto, al haberse turnado la solicitud a la Unidad de Transparencia, se dio cumplimiento al procedimiento para la atención a las solicitudes de acceso a la información que se encuentra establecido en los artículos 151, 159, 160, 162, 163, 164, 165 y 166, de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, el cual es el siguiente:

* Las Unidades de Transparencia de los Sujetos Obligados deben garantizar las medidas y condiciones de accesibilidad para que toda persona puede ejercer el derecho de acceso a la información; por lo que, son las responsables de hacer las notificaciones correspondientes, además de llevar a cabo de todas las gestiones necesarias para facilitar el acceso de la información;
* Los Sujetos Obligados podrán requerirle a los Solicitantes, que complementen, corrijan o amplíen su solicitud de información, cuando resulten los datos proporcionados insuficientes, incorrectos, incompletos o erróneos; solicitar dicha aclaración, interrumpirá el plazo para dar respuesta y comenzará a computarse el día siguiente al desahogo de esta;
* Las respuestas a los requerimientos informativos deberán notificarse al interesado en el menor tiempo posible, que no podrá exceder **quince días, contados a partir del día siguiente a la presentación de ésta.** Excepcionalmente, el plazo referido podrá ampliarse por siete días hábiles más, cuando existan razones fundadas y motivadas, a través del Comité de Transparencia;
* **Las Unidades de Transparencia garantizarán que las solicitudes se turnen a todas las áreas competentes que cuenten con la información o deban tenerla de acuerdo con sus facultades, funciones y atribuciones, para que realicen una búsqueda exhaustiva y razonable de la documentación solicitada, con el fin de que proporcionen las expresiones documentales que se encuentren en sus archivos o que estén constreñidos a elaborar;**
* El acceso se dará en la modalidad de entrega y en su caso, de envío elegido por el solicitante, cuando no pueda entregarse en dicha modalidad, el Sujeto Obligado deberá ofrecer otras; por lo cual, deberá fundamentar y motivar la necesidad de modificar el medio de entrega, y
* Las Unidades de Transparencia, tendrán disponible la información requerida durante un plazo mínimo de sesenta días hábiles, contados a partir de que el solicitante hubiere realizado, en su caso, el pago respectivo, el cual deberá efectuarse en un plazo no mayor a treinta días hábiles; por lo que, una vez transcurrida dicha temporalidad, los Sujetos Obligados darán por concluida la solicitud y procederán de ser el caso, a la destrucción del material.

En ese sentido, se tiene que, **el procedimiento de búsqueda de la información se tiene por atendido.**

Precisado lo anterior, en cuanto a la naturaleza de la información y procedencia de la entrega de la misma, resulta necesario abordar el estudio del presente asunto bajo los siguientes apartados:

**a) Documentos de seguridad:**

Bajo este orden de ideas, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, señala en sus artículos 4, fracción XVIII, 43, 44, 45, 46, 47, 48, 49 y 50, sobre el tema en comento, lo siguiente:

*“Artículo 4. Para los efectos de esta Ley se entenderá por*

*…*

***XVIII. Documento de seguridad:******al instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de la información contenida en los sistemas y bases de datos personales.***

***…***

*Naturaleza de las medidas de seguridad y registro del nivel de seguridad*

***Artículo 43****. Las medidas de seguridad previstas en este capítulo constituyen mínimos exigibles, por lo que el sujeto obligado adoptará las medidas adicionales que estime necesarias para brindar mayor garantía en la protección y resguardo de los sistemas y bases de datos personales.*

***Por la naturaleza de la información, las medidas de seguridad que se adopten serán consideradas confidenciales y únicamente se comunicará al Instituto, para su registro, el nivel de seguridad aplicable.***

*El responsable y el encargado establecerán medidas para garantizar que cualquier persona que actúe bajo la autoridad de éstos y que tenga acceso a datos personales sólo pueda tratarlos siguiendo las instrucciones del responsable y observando lo previsto en la normatividad aplicable.*

*Las medidas de seguridad que al efecto se establezcan indicarán el nombre y cargo del administrador o usuaria o usuario, según corresponda. Cuando se trate de usuarias o usuarios se incluirán los datos del acto jurídico mediante el cual, el sujeto obligado otorgó el tratamiento del sistema de datos personales.*

*En el supuesto de actualización de estos datos, la modificación respectiva se notificará al Instituto en sus oficinas o en el portal que para tal efecto se cree, dentro de los treinta días hábiles siguientes a la fecha en que se efectuó.*

*El responsable o el encargado, designarán a una o un administrador, quien tendrá bajo su responsabilidad directa la base y sistema de datos personales.*

*Tipos y Niveles de Seguridad*

***Artículo 44****. El responsable adoptará las medidas de seguridad, conforme a lo siguiente:*

*A. Tipos de seguridad:*

*I. Física: a la medida orientada a la protección de instalaciones, equipos, soportes, sistemas o bases de datos para la prevención de riesgos por caso fortuito o causas de fuerza mayor.*

*II. Lógica: a las medidas de seguridad administrativas y de protección que permiten la identificación y autenticación de las usuarias y los usuarios autorizados para el tratamiento de los datos personales de acuerdo con su función.*

*III. De desarrollo y aplicaciones: a las autorizaciones con las que contará la creación o tratamiento de los sistemas o bases de datos personales, según su importancia, para garantizar el adecuado desarrollo y uso de los datos, previendo la participación de las usuarias y usuarios, la separación de entornos, la metodología a seguir, ciclos de vida y gestión, así como las consideraciones especiales respecto de aplicaciones y pruebas.*

*IV. De cifrado: a la implementación de algoritmos, claves, contraseñas, así como dispositivos concretos de protección que garanticen la seguridad de la información.*

*V. De comunicaciones y redes: a las medidas de seguridad técnicas, así como restricciones preventivas y de riesgos que deberán observar los usuarios de datos o sistemas de datos personales para acceder a dominios o cargar programas autorizados, así como para el manejo de telecomunicaciones.*

*B. Niveles de seguridad:*

*I. Básico: a las medidas generales de seguridad cuya aplicación es obligatoria para todos los sistemas y bases de datos personales. Dichas medidas corresponden a los siguientes aspectos:*

***a) Documento de seguridad.***

 *b) Funciones y obligaciones del personal que intervenga en el tratamiento de las bases o sistemas de datos personales.*

*c) Registro de incidencias.*

*d) Identificación y autenticación.*

*e) Control de acceso.*

*f) Gestión de soportes.*

*g) Copias de respaldo y recuperación.*

*II. Medio: a la adopción de medidas de seguridad cuya aplicación corresponde a bases o sistemas de datos relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, datos patrimoniales, así como a los que contengan datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo.*

*Este nivel de seguridad, de manera adicional a las medidas calificadas como básicas, considera los aspectos siguientes:*

*a) Responsable de seguridad.*

*b) Auditoría.*

*c) Control de acceso físico.*

*d) Pruebas con datos reales.*

*III. Alto: a las medidas de seguridad aplicables a bases o sistemas de datos concernientes a la ideología, religión, creencias, afiliación política, origen racial o étnico, salud, biométricos, genéticos o vida sexual, así como los que contengan datos recabados para fines policiales, de seguridad pública, prevención, investigación y persecución de delitos.*

*En estos casos, además de incorporar las medidas de nivel básico y medio, deberán completar las que se detallan a continuación:*

*a) Distribución de soportes.*

*b) Registro de acceso.*

*c) Telecomunicaciones.*

*Los diferentes niveles de seguridad serán establecidos atendiendo a las características propias de la información. Elementos a considerar para la adopción de medidas de seguridad y su naturaleza*

***Artículo 45****. Las medidas de seguridad adoptadas por el responsable considerarán: I. El riesgo inherente a los datos personales tratados.*

*II. La sensibilidad de los datos personales tratados.*

*III. El desarrollo tecnológico.*

*IV. Las posibles consecuencias de una vulneración para las y los titulares.*

*V. Las transferencias de datos personales que se realicen.*

*VI. El número de titulares.*

*VII. Las violaciones a la seguridad previas ocurridas en los sistemas de tratamiento.*

*VIII. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión. Actividades interrelacionadas para establecer y mantener las medidas de seguridad.*

***Artículo 46****. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable realizará, al menos, las actividades interrelacionadas siguientes:*

*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 las bases y o 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, así como las medidas 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 vulnerabilidades a las que están sujetos los datos personales.*

*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.*

***Exigibilidad de Documentos y Registros derivados de un Sistema de Gestión de la Protección de Datos.***

***Artículo 47.*** *Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales serán documentadas y contenidas en un sistema de gestión.*

*Se entenderá por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en la presente Ley y las demás disposiciones legales aplicables.*

***Obligatoriedad del Documento de Seguridad***

***Artículo 48. Los sujetos obligados elaborarán y aprobarán un documento que contenga las medidas de seguridad aplicables a las bases y sistemas de datos personales, tomando en cuenta los estándares internacionales de seguridad, la presente Ley así como los lineamientos que se expidan.***

***El documento de seguridad será de observancia obligatoria para los responsables, encargados y demás personas que realizan algún tipo de tratamiento a los datos personales. A elección del sujeto obligado, éste podrá ser único e incluir todos los sistemas y bases de datos personales que posea, por unidad administrativa en que se incluyan los sistemas y bases de datos personales en custodia, individualizado para cada sistema, o mixto.***

***Contenido del Documento de Seguridad***

***Artículo 49. El documento de seguridad deberá contener como mínimo lo siguiente:***

*I. Respecto de los sistemas de datos personales:*

*a) El nombre.*

 *b) El nombre, cargo y adscripción del administrador de cada sistema y base de datos.*

 *c) Las funciones y obligaciones del responsable, encargado o encargados y todas las personas que traten datos personales.*

***d) El folio del registro del sistema y base de datos.***

***e) El inventario o la especificación detallada del tipo de datos personales contenidos****.*

***f) La estructura y descripción de los sistemas y bases de datos personales, lo cual consiste en precisar y describir el tipo de soporte, así como las características del lugar donde se resguardan****.*

*II. Respecto de las medidas de seguridad implementadas deberá incluir lo siguiente:*

*a)* ***Transferencia y remisiones.***

***b) Resguardo de soportes físicos y electrónicos.***

***c) Bitácoras para accesos, operación cotidiana y violaciones a la seguridad de los datos personales.***

***d) El análisis de riesgos.***

***e) El análisis de brecha.***

***f) Gestión de incidentes.***

 ***g) Acceso a las instalaciones.***

***h) Identificación y autenticación.***

***i) Procedimientos de respaldo y recuperación de datos****.*

*j) Plan de contingencia.*

***k) Auditorías.***

***l) Supresión y borrado seguro de datos.***

***m) El plan de trabajo****.*

***n) Los mecanismos de monitoreo y revisión de las medidas de seguridad****.*

*o) El programa general de capacitación. Revisión y actualización del documento de seguridad.*

 *Artículo 50. El responsable revisará el documento de seguridad de manera periódica y actualizarlo cuando ocurran los eventos siguientes:*

*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.*

 *IV. Implementación de acciones correctivas y preventivas ante una violación de la seguridad de los datos personales.”*

*(Énfasis añadido)*

Preceptos legales en donde se establece, que el documento de seguridad es el instrumento en donde se establecen las medidas de seguridad adoptadas por el responsable del tratamiento de los datos personales, con la finalidad de avalar el secreto, probidad y tratamiento de los datos personales contenida en los sistemas y base de datos creados por los Sujetos Obligados en el cumplimiento de sus obligaciones.

Asimismo, conforme el artículo 48 de la Ley de Protección de Datos Personales Local, el documento de seguridad es de observancia obligatoria para los responsables, encargados y demás personas que realizan algún tipo de tratamiento a los datos personales, **y a elección del sujeto obligado, éste podrá ser único e incluir todos los sistemas y bases de datos personales que posea,** por unidad administrativa en que se incluyan los sistemas y bases de datos personales en custodia, individualizado para cada sistema, o mixto.

De ahí que los Sujetos Obligados pueden tener un documento de seguridad único en el que se incluyan todos los sistemas y bases de datos que posean por unidad administrativa.

Por otra parte, la Ley de Protección de Datos Personales, referida, señala como obligatoriedad por parte de los Sujetos Obligados el de **emitir y aprobar su documento de seguridad para el tratamiento de los datos personales que recabe en cumplimiento de sus funciones que se encuentren contenidos en sus sistemas o bases de datos**; asimismo, dicho soporte documental, contendrá las medidas de seguridad aplicables a las bases y sistemas de datos personales, en ese contexto, por cuanto hace a esta parte resulta aplicable lo dispuesto por el artículo 43 de la Ley de Protección de Datos Personales local, que en su penúltimo párrafo de la misma Ley, refiere lo siguiente:

*“****Artículo 143.*** *…*

*…*

*La información confidencial no estará sujeta a temporalidad alguna y sólo podrán tener acceso a ella los titulares de la misma, sus representantes y los servidores públicos facultados para ello.”(Sic)*

En concordancia con expuesto, el numeral Trigésimo Octavo, párrafo segundo de los “Lineamientos Generales en materia de Clasificación y Desclasificación de la información, así como para la elaboración de Versiones Públicas”, señala lo siguiente:

*“****Trigésimo octavo.*** *…*

*La información confidencial no estará sujeta a temporalidad alguna y sólo podrán tener acceso a ella los titulares de la misma,* *sus representantes y los integrantes de los sujetos obligados facultados para ello.” (Sic)*

Bajo lo previo, resulta importante señalar que las medidas de seguridad aplicables a las bases de datos personales por parte del responsable es **información de carácter confidencial** por mandato expreso del artículo 43 de la Ley, razón por la cual las políticas y procedimientos de seguridad en materia de protección de datos personales, no pueden ser proporcionados, toda vez que la puesta a disposición de las mismas pudiesen causar un daño, alteración, pérdida, destrucción, o el uso, transferencia, acceso o cualquier tratamiento no autorizado o ilícito a la información que se encuentra en tratamiento en bases y sistemas de datos personales.

Asimismo, es pertinente mencionar que conforme a lo dispuesto en el artículo 49 de la Ley de Protección de Datos Personales supraindicada, el documento de seguridad debe contener, como mínimo, lo referente a:

1. **Sistemas de Datos Personales**: a) el nombre, **b) el nombre, cargo y adscripción del administrador de cada sistema y base de datos, c) las funciones y obligaciones del responsable o encargados y todas la personas que traten datos personales, d) el folio del registro del sistema y base de datos,** e) el inventario o especificación detallada del tipo de datos personales y f) la estructura y descripción de los sistemas y bases de datos personales, en las que deberá precisar y describir el tipo de soporte y características del lugar donde se resguardan.
2. **Las Medidas de Seguridad implementadas**, como son: a) transferencia y remisiones, b) resguardo de soportes físicos y electrónicos, c) bitácoras para accesos, operación cotidiana y violaciones a la seguridad de los datos personales, d) el análisis de riesgos, e) el análisis de brecha, f) Gestión de incidentes, g) acceso a las instalaciones, h) Identificación y autenticación, i) procedimientos de respaldo y recuperación de datos, j) plan de contingencia, k) auditorías, l) supresión y borrado seguro de datos, m) plan de trabajo, n) los mecanismos de monitoreo y revisión de las medidas de seguridad y o) el programa general de capacitación.

Como se desprende de lo anterior, la fracción I del artículo 49 de la Ley de Protección de Datos Personales de la Entidad, prevé que el documento de seguridad debe contener, como mínimo, información relativa a los sistemas de datos personales; de la cual es de precisar que por lo que corresponde a la indicada en los **incisos del a) al e), se trata de información pública,** en virtud de relacionarse con el nombre del sistema o base de datos; el nombre, cargo y adscripción del administrador de cada sistema y base de datos; las funciones y obligaciones del responsable o encargados y todas la personas que traten datos personales; el folio del registro del sistema y base de datos; así como, el inventario o especificación detallada del tipo de datos personales.

Sin embargo, **en el caso del inciso f) de la fracción I** del artículo 49 de la Ley de Protección de Datos Personales en cita, relativo a la estructura y descripción de los sistemas y bases de datos personales, en las que deberá precisar y describir el tipo de soporte y características del lugar donde se resguardan; su publicidad queda sujeta al análisis pormenorizado que realice el **Sujeto Obligado**, ya que si dicho ente arriba a la conclusión de que dicho inciso que debe contener el documento de seguridad contiene medidas de seguridad detalladas, el mismo deberá clasificarse como información confidencial.

Por otro lado, en el caso resulta relevante los incisos a), b) y d) de la fracción I del artículo 49 de la Ley de Protección de Datos Personales de la Entidad, que prevén, que el documento de seguridad debe contener, entre otra información el nombre del sistema o base de datos; el nombre, cargo y adscripción del administrador de cada sistema y base de datos; así como el folio del registro del sistema y base de datos.

Lo anterior, pues es de recordar que la parte **Recurrente** en el presente asunto pretende tener acceso al nombre de cada una de las bases de datos con las que cuenta el Ayuntamiento a la fecha de la solicitud, al número de bases de datos que se tienen registradas y al nombre de los servidores públicos responsables de cada base de datos.

Por lo que, con la entrega que, en su caso, proceda del o los documentos de seguridad con que cuente el Ayuntamiento de Toluca actualizados a la fecha de la solicitud, también se atendería lo relativo al nombre de las bases de datos y el número de bases de datos que se tienen registradas, asimismo, con la entrega del documento o documentos de seguridad se atendería lo relativo a los nombres de los servidores públicos responsables de cada base de datos.

Se afirma lo anterior, pues si bien conforme el artículo 4°, fracción XLI, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, se establece que los Sujetos Obligados son los **responsables** que deciden del tratamiento de los datos personales; del análisis a la solicitud de información se desprende que el particular pretende tener acceso al nombre de los servidores públicos nombrados para llevar a cabo el tratamiento de datos personales y que a su vez son los responsables de los sistemas y bases de datos personales, siendo estos los administradores, como se desprende de la fracción I del artículo 4 de la Ley en cita, que dispone lo siguiente:

*“Artículo 4. Para los efectos de esta Ley se entenderá por:*

*[…]*

***I. Administrador:******a la servidora o el servidor público*** *o persona física facultada y nombrada por el Responsable para llevar a cabo tratamiento de datos* ***personales y que tiene bajo su responsabilidad los sistemas y bases de datos personales.****[…]”*

*(Énfasis añadido)*

Por lo tanto, con la entrega del documento de seguridad, **también se colmaría lo relativo a los nombres de los servidores públicos responsables de las bases de datos que tiene el Ayuntamiento de Toluca a la fecha de la solicitud.**

Precisado lo anterior, ahora por lo que corresponde a la información que debe contener el documento de seguridad, prevista en la fracción II del artículo 49 de la Ley de Protección de Datos Personales de la Entidad, es de indicar que la misma, por cuanto hace a los incisos a) al n), se encuentra relacionada con las medidas de seguridad implementadas, las cuales son susceptibles de clasificarse como información confidencial.

Lo anterior, tiene sustento en atención a que el **análisis de riesgo** contiene las consideraciones relacionadas con las amenazas y vulnerabilidades existentes.

El **resguardo es el espacio destinado para almacenar o resguardar datos personales** que han recibido el tratamiento correspondiente, para que formen parte integral de uno o más Sistemas de Datos Personales en soporte electrónico.

Las **bitácoras** registran los accesos autorizados e incidencias para cada una de ellas. Asimismo, deberá establecer los procedimientos para el uso de bitácoras respecto de las acciones cotidianas llevadas a cabo en los SDPS.

El **análisis de brecha**, contiene la comparación de las medidas de seguridad existentes y las medidas de seguridad faltantes en la organización del responsable del tratamiento de datos personales.

La **gestión de incidentes** son acciones que adoptan el titular del Sujeto Obligado y el responsable de los Sistemas de Datos Personales, a efecto de dar a conocer a las autoridades competentes, a los titulares de los datos y, en su caso, al público en general, los actos deliberados (intrusión, robo, etcétera) y los acontecimientos de caso fortuito o de fuerza mayor (desastres naturales, incendios, huelgas, etcétera) que hubieran ocasionado la pérdida total o parcial de los datos personales bajo su custodia;

El **acceso a instalaciones** donde se encuentren los Sistemas de Datos Personales, ya sea en soporte físico o electrónico, se permite únicamente a quienes estén expresamente autorizados en el documento de seguridad, por lo que dar a conocer esta información compromete la seguridad de los datos personales.

Por cuanto hace a la **identificación y autenticación**, el responsable tendrá a su cargo la elaboración de una relación actualizada de los servidores públicos que tengan acceso autorizado a los Sistemas de Datos Personales y del establecimiento de procedimientos que permitan la correcta identificación y autenticación para dicho acceso. El responsable establecerá un mecanismo que permita la identificación, de forma inequívoca y personalizada, de toda persona que intente acceder a los Sistemas de Datos Personales y la verificación de que está autorizada.

Cuando el mecanismo de autenticación se base en la existencia de contraseñas, se establecerá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

Respecto al procedimiento de **respaldo y recuperación de datos**, se advierte que dar a conocer los medios de almacenamiento no volátil autorizados para la generación y almacenamiento de copias de seguridad o respaldos compromete los tres pilares de la organización: confidencialidad, disponibilidad e integridad.

En la **supresión de datos personales**, los Sujetos Obligados deberán establecer las políticas, métodos y técnicas, por lo que el responsable deberá considerar, al menos, los siguientes atributos y el o los medios de almacenamiento, físicos y/o electrónicos en los que se encuentren los datos personales:

Irreversibilidad: que el proceso utilizado no permita recuperar los datos personales; Seguridad y confidencialidad: que en la eliminación definitiva de los datos personales se consideren los deberes de confidencialidad y seguridad, y Favorable al medio ambiente: que el método utilizado produzca el mínimo de emisiones y desperdicios que afecten el medio ambiente. Divulgar esta información pudiera representar que los datos personales no puedan ser reutilizados o susceptibles de un mal uso por terceros.

Por lo que hace al **plan de contingencia**, éste se relaciona con una eventual “situación de emergencia”[[4]](#footnote-4) respecto al tratamiento de datos personales de los titulares, caso en el que se concreta una excepción al Principio de Consentimiento previsto en el artículo 21, fracción VI de la Ley de protección de Datos Personales en Posesión de Sujetos Obligados aplicable en la Entidad, que al respecto establece:

*“****Artículo 21.*** *El responsable no estará obligado a recabar el consentimiento de la o el titular para el tratamiento de sus datos personales en los casos siguientes:*

 *…*

***VI.******Exista una situación de emergencia*** *que pueda dañar a un individuo en su persona o en sus bienes.” (Sic)*

El **Plan de trabajo** contiene lo relacionado con la implementación de las medidas de seguridad faltantes y las que dan complimiento cotidiano de las políticas de gestión y tratamiento de los datos personales.

Finalmente, **por lo que respecta al inciso o) de la fracción II que corresponde al Programa General de Capacitación**, no puede ser clasificado, pues si bien corresponde a acciones de seguridad, esta información no permite acceder a los datos personales protegidos; por el contrario rinde cuentas de que se capacitó al personal y que las capacitaciones corresponden con las necesidades de protección que tenga el Sujeto Obligado.

De lo expuesto, se advierte que los incisos de la fracción II del artículo 49 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México, **a excepción del inciso o),** contienen concretamente, la información relacionada con la vulnerabilidad concerniente a las medidas de seguridad que en el caso concreto debe proteger el **Sujeto Obligado**,pues se reitera, la puesta a disposición de la información referida en los incisos expuestos, pudiese causar un daño, alteración, pérdida, destrucción, o el uso, transferencia, acceso o cualquier tratamiento no autorizado o ilícito a la información que se encuentra en tratamiento en bases y sistemas de datos personales.

Por lo tanto, derivado del presente estudio se concluye que todo lo concerniente a la **fracción I** del artículo 49 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios **si deberá entregarse,** mientras que lo previsto en la **fracción II, con excepción del inciso o) que es información pública,** de la citada normatividad no es susceptible de entrega, por las razones previamente expuestas en líneas argumentativas anteriores.

Asimismo, es de agregar que, el documento de seguridad debe ser actualizado, cuando se considere así por el Sujeto Obligado, Responsables y/o administradores, de tal suerte que, en el presente asunto, lo que se solicita es la información que se tiene a la fecha de la solicitud, ya que los documentos de seguridad se crean sólo para bases de datos personales nuevas y para el resto sólo se actualizan.

Por lo tanto, el pronunciamiento del servidor público habilitado competente, en el sentido de que la información estaba en proceso de integración, resulta insuficiente para tener por colmado el derecho de acceso a la información del particular, pues conforme lo expuesto el **Sujeto Obligado** tiene la obligación de contar con un documento de seguridad de las bases o sistemas de datos personales.

En consecuencia, resulta procedente ordenar que en cumplimiento a la presente resolución, se entregue, previa búsqueda exhaustiva y razonable, en versión pública, **el o los documentos de seguridad de las bases o sistemas de datos personales vigentes al veinte de enero de dos mil veinticinco.**

**b) Cédulas de las bases de datos que se tienen registradas.**

Al respecto, se procede a contextualizar la información solicitada, relacionada con las Cédulas de Bases de Datos Personales, por lo que, es pertinente señalar lo siguiente:

***LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DEL ESTADO DE MÉXICO Y MUNICIPIOS.***

***Artículo 4.*** *Para los efectos de esta Ley se entenderá por:*

*I. Administrador: a la servidora o el servidor público o persona física facultada y nombrada por el Responsable para llevar a cabo tratamiento de datos personales y que tiene bajo su responsabilidad los sistemas y bases de datos personales.*

*V. Aviso de Privacidad: al documento físico, electrónico o en cualquier formato generado por el responsable que es puesto a disposición del Titular con el objeto de informarle los propósitos del tratamiento al que serán sometidos sus datos personales.*

***VI. Base de Datos: al conjunto de archivos, registros, ficheros, condicionados a criterios determinados con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento, organización y acceso.***

*XXX. Medidas de seguridad: a las acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.*

*XLIII. Sistema de datos personales: a los datos personales contenidos en los archivos de un sujeto obligado que puede comprender el tratamiento de una o diversas bases de datos para el cumplimiento de una o diversas finalidades.*

*…*

*Artículo 35. Corresponde a cada sujeto obligado determinar, a través de su titular, órgano competente o Comité de Transparencia, la creación, modificación o supresión de sistemas y bases de datos personales, conforme a su respectivo ámbito de competencia.*

*“Artículo 36. La integración, tratamiento y tutela de los sistemas de datos personales se regirán por las disposiciones siguientes:*

*I. Cada sujeto obligado deberá informar al Instituto sobre la creación, modificación o supresión de sus sistemas de datos personales.*

*II. En caso de creación o modificación de sistemas de datos personales, se incluirá en el registro, los datos previstos la presente Ley.*

*II. En las disposiciones que se dicten para la supresión de los sistemas de datos personales, se establecerá el destino de los datos contenidos en los mismos o, en su caso, las previsiones que se adopten para su destrucción.*

*IV. De la destrucción de los datos personales podrán ser excluidos aquellos que, con finalidades estadísticas o históricas, sean previamente sometidos al procedimiento de disociación.*

*El registro de Sistemas de Datos Personales deberá realizarse a más tardar dentro de los seis meses siguientes al inicio del tratamiento por parte del responsable.*

***Artículo 37.*** *Los sujetos obligados registrarán ante el Instituto los sistemas de datos personales que posean. El registro deberá indicar por lo menos los datos siguientes:*

*I. El sujeto obligado que tiene a su cargo el sistema de datos personales.*

*II. La denominación del sistema de datos personales, la base de datos y el tipo de datos personales objeto de tratamiento.*

*III. El nombre y cargo del administrador, así como el área o unidad administrativa a la que se encuentra adscrito.*

*IV. El nombre y cargo del encargado.*

*V. La normatividad aplicable que dé fundamento al tratamiento en términos de los principios de finalidad y licitud.*

*VI. La finalidad del tratamiento.*

*VII. El origen, la forma de recolección y actualización de datos.*

*VIII. Datos transferidos, lugar de destino e identidad de los destinatarios, en el caso de que se registren transferencias.*

*IX. El modo de interrelacionar la información registrada, o en su caso, la trazabilidad de los datos en el sistema de datos personales.*

*X. El domicilio de la Unidad de Transparencia, así como de las áreas o unidades administrativas ante las que podrán ejercitarse de manera directa los derechos ARCO.*

*XI. El tiempo de conservación de los datos.*

*XII. El nivel de seguridad.*

*XIII. En caso de que se hubiera presentado una violación de la seguridad de los datos personales se indicará la fecha de ocurrencia, la de detección y la de atención.*

*Dicha información deberá permanecer en el registro un año calendario posterior a la fecha de su atención.*

Bajo esta línea de pensamiento, se tiene que efectivamente las bases de datos generadas para almacenar los datos personales, deberá registrarse ante este Instituto y dicho registro deberá contener una serie de elementos, de entre los cuales destaca la denominación de la base de datos, tipo de datos personales objeto del tratamiento, finalidad del tratamiento, tiempo de conservación de los datos, nivel de seguridad, etc.

Los Sujetos Obligados, se tienen que guiar bajo las bases, principios y procedimientos para tutelar y garantizar el derecho que tiene toda persona a la protección de sus datos personales, mediante bases de datos, documentos de seguridad y avisos de privacidad a efecto de tratar los datos personales.

***Artículo 38.*** *Con independencia del tipo de sistema y base de datos en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable adoptará, establecerá, mantendrá y documentará las medidas de seguridad administrativas, físicas y técnicas para garantizar la integridad, confidencialidad y disponibilidad de los datos personales, a través de controles y acciones que eviten su daño, alteración, pérdida, destrucción, o el uso, transferencia, acceso o cualquier tratamiento no autorizado o ilícito, de conformidad con lo dispuesto en los lineamientos que al efecto se expidan.*

*Artículo 40. Confidencialidad a la propiedad o característica consistente en que la información no se pondrá a disposición, ni se revelará a individuos, entidades o procesos no autorizados, por consiguiente, el responsable, el administrador, el encargado o en su caso las usuarias y los usuarios autorizados son los únicos que pueden llevar a cabo el tratamiento de los datos personales, mediante los procedimientos que para tal efecto se establezcan.*

*El responsable, el encargado, las usuarias o los usuarios o cualquier persona que tenga acceso a los datos personales están obligados a guardar el secreto y sigilo correspondiente, conservando la confidencialidad aún después de cumplida su finalidad de tratamiento.*

*El administrador, el encargado o en su caso las usuarias y los usuarios autorizados son los únicos que pueden llevar a cabo el tratamiento de los datos personales, mediante los procedimientos que para tal efecto se establezcan.*

*El responsable establecerá controles o mecanismos que tengan por objeto que las personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el sujeto obligado en los mismos términos que operen las prescripciones en materia de responsabilidades, salvo disposición legal en contrario.*

*En caso de contravención al deber de confidencialidad se estará a lo dispuesto por los ordenamientos administrativos correspondientes, independientemente de las acciones penales o civiles que en su caso procedan.*

***Artículo 43.*** *Las medidas de seguridad previstas en este capítulo constituyen mínimos exigibles, por lo que el sujeto obligado adoptará las medidas adicionales que estime necesarias para brindar mayor garantía en la protección y resguardo de los sistemas y bases de datos personales. Por la naturaleza de la información, las medidas de seguridad que se adopten serán consideradas confidenciales y únicamente se comunicará al Instituto, para su registro, el nivel de seguridad aplicable.*

*El responsable y el encargado establecerán medidas para garantizar que cualquier persona que actúe bajo la autoridad de éstos y que tenga acceso a datos personales sólo pueda tratarlos siguiendo las instrucciones del responsable y observando lo previsto en la normatividad aplicable.*

*Las medidas de seguridad que al efecto se establezcan indicarán el nombre y cargo del administrador o usuaria o usuario, según corresponda. Cuando se trate de usuarias o usuarios se incluirán los datos del acto jurídico mediante el cual, el sujeto obligado otorgó el tratamiento del sistema de datos personales.*

*En el supuesto de actualización de estos datos, la modificación respectiva se notificará al Instituto en sus oficinas o en el portal que para tal efecto se cree, dentro de los treinta días hábiles siguientes a la fecha en que se efectuó. El responsable o el encargado, designarán a una o un administrador, quien tendrá bajo su responsabilidad directa la base y sistema de datos personales.*

El responsable de los datos personales, adoptará, establecerá, mantendrá y documentará las medidas de seguridad administrativas, físicas y técnicas para garantizar la integridad, confidencialidad y disponibilidad de los datos personales, a través de controles y acciones que eviten su daño, alteración, pérdida, destrucción, o el uso, transferencia, acceso o cualquier tratamiento no autorizado o ilícito, por lo que no se pondrá a disposición, ni se revelará a individuos, entidades o procesos no autorizados, por consiguiente, el responsable, el administrador, el encargado o en su caso las usuarias y los usuarios autorizados son los únicos que pueden llevar a cabo el tratamiento de los datos personales, mediante los procedimientos, por lo que se adoptarán las medidas adicionales que estime necesarias para brindar mayor garantía en la protección y resguardo de los sistemas y bases de datos personales.

Dicho esto, las cédulas de bases de datos es información que debe obrar en los archivos del Sujeto Obligado.

Como referencia de lo anterior, se procede a citar un ejemplo de las cédulas de bases de datos personales:







Por lo tanto, respecto del punto en análisis, se considera que el pronunciamiento del servidor público habilitado competente, en el sentido de que la información estaba en proceso de integración, también resulta insuficiente para tener por colmado el derecho de acceso a la información del particular, pues conforme lo expuesto en los archivos del **Sujeto Obligado** debe obrar las cédulas requeridas, máxime que el ente público no manifestó lo contrario.

En consecuencia, resulta procedente ordenar que en cumplimiento a la presente resolución, se entregue, previa búsqueda exhaustiva y razonable, en versión pública, **las cédulas de las bases o sistemas de datos personales vigentes al veinte de enero de dos mil veinticinco.**

**c) Avisos de privacidad (integrales y simplificados) de las áreas administrativas del Sujeto Obligado.**

De conformidad con la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, el **aviso de privacidad** es el documento físico, electrónico o en cualquier formato generado por el responsable que es puesto a disposición del titular con el objeto de informarle los propósitos del tratamiento al que serán sometidos sus datos personales.

La Ley establece que los responsables pondrán a disposición de la o el titular en formatos impresos, digitales, visuales, sonoros o de cualquier otra tecnología, **el aviso de privacidad en las modalidades simplificado e integral**, siendo que a través de este aviso, el responsable tiene la obligación de información de modo expreso, preciso e inequívoco a las o los titulares, la información que se recaba de ellos y con qué fines, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que puedan tomar decisiones informadas al respecto, tal como se observa a continuación:

***“Principio de Información***

***Artículo 23.*** *El responsable tendrá la obligación de informar a través del aviso de privacidad de modo expreso, preciso e inequívoco a las y los titulares, la información que se recaba de ellos y con qué fines, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que puedan tomar decisiones informadas al respecto.*

*El aviso de privacidad estará redactado y estructurado de manera clara precisa y sencilla, será difundido por los medios electrónicos y físicos con que cuente el responsable. Cuando resulte imposible dar a conocer a la o el titular el aviso de privacidad, de manera directa o ello exija esfuerzos desproporcionados, el responsable instrumentará medidas compensatorias de comunicación masiva de acuerdo con los criterios que para tal efecto emita el Sistema Nacional.”*

En el mismo orden de ideas, es de destacar que se entiende como **aviso de privacidad integral** a aquel que es entregado cuando los datos son proporcionados directamente por el titular de estos, este debe ser facilitado en el momento de forma clara e incuestionable, a través de los formatos establecidos por el sujeto obligado, por otro lado, el **aviso de privacidad simplificado** es aquel que es entregado cuando los datos son obtenidos por cualquier medio electrónico, óptimo, sonoro, visual o a través de cualquier otra tecnología, el aviso de privacidad debe ser puesto a disposición en un lugar visible, considerando los medios o mecanismos para que se conozca el texto completo del aviso.

Por otro lado, de conformidad con los artículos 31 y33 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, se establece que:

***“Contenido del Aviso de Privacidad Integral***

***Artículo 31.*** *El aviso de privacidad integral contendrá la información siguiente:*

*I. La denominación del responsable.*

*II. El nombre y cargo del administrador, así como el área o unidad administrativa a la que se encuentra adscrito.*

*III. El nombre del sistema de datos personales o base de datos al que serán incorporados los datos personales.*

*IV. Los datos personales que serán sometidos a tratamiento, identificando los que son sensibles.*

*V. El carácter obligatorio o facultativo de la entrega de los datos personales.*

*VI. Las consecuencias de la negativa a suministrarlos.*

*VII. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieran el consentimiento de la o el titular.*

*VIII. Cuando se realicen transferencias de datos personales se informará:*

*a) Destinatario de los datos.*

*b) Finalidad de la transferencia.*

*c) El fundamento que autoriza la transferencia.*

*d) Los datos personales a transferir.*

*e) Las implicaciones de otorgar, el consentimiento expreso.*

*Cuando se realicen transferencias de datos personales que requieran consentimiento, se acreditará el otorgamiento.*

*IX. Los mecanismos y medios estarán disponibles para el uso previo al tratamiento de los datos personales, para que la o el titular, pueda manifestar su negativa para la finalidad y transferencia que requieran el consentimiento de la o el titular.*

*X. Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO, indicando la dirección electrónica del sistema para presentar sus solicitudes.*

*XI. La indicación por la cual la o el titular podrá revocar el consentimiento para el tratamiento de sus datos, detallando el procedimiento a seguir para tal efecto.*

*XII. Cuando aplique, las opciones y medios que el responsable ofrezca a las o los titulares para limitar el uso o divulgación, o la portabilidad de datos.*

*XIII. Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad,*

*XIV. El cargo y domicilio del encargado, indicando su nombre o el medio por el cual se pueda conocer su identidad.*

*XV. El domicilio del responsable, y en su caso, cargo y domicilio del encargado, indicando su nombre o el medio por el cual se pueda conocer su identidad.*

*XVI. El fundamento legal que faculta al responsable para llevar a cabo el tratamiento.*

*XVII. El procedimiento para que se ejerza el derecho a la portabilidad.*

*XVIII. El domicilio de la Unidad de Transparencia.*

*XIX. Datos de contacto del Instituto, incluidos domicilio, dirección del portal informativo, correo electrónico y teléfono del Centro de Atención Telefónica, para que la o el titular pueda recibir asesoría o presentar denuncias por violaciones a las disposiciones de la Ley.*

***Contenido del Aviso de Privacidad Simplificado***

***Artículo 33.*** *El aviso de privacidad simplificado deberá contener, al menos, la información a que se refieren las fracciones I, VII, VIII y IX del artículo relativo al contenido del aviso de privacidad integral.”*

Como se logra advertir, el aviso de privacidad es de suma importancia en el tratamiento de datos personales, ya que permite informar a sus titulares del tratamiento que se les da a los mismos, por lo que, es **obligatorio** que los sujetos obligados cuenten con los avisos de privacidad correspondientes, cuando algunas de sus unidades administrativas procesen datos personales.

Por lo tanto, respecto del punto en análisis, se considera que el pronunciamiento del servidor público habilitado competente, en el sentido de que la información estaba en proceso de integración, también resulta insuficiente para tener por colmado el derecho de acceso a la información del particular, pues conforme lo expuesto el **Sujeto Obligado** debe contar con los avisos de privacidad correspondientes, máxime que en respuesta no se manifestó lo contrario.

En consecuencia, resulta procedente ordenar que en cumplimiento a la presente resolución, se entregue, previa búsqueda exhaustiva y razonable, **los avisos de privacidad integrales y simplificados, con los que se cuente al veinte de enero de dos mil veinticinco.**

**Quinto. Versión Pública.** Finalmente para la entrega del soporte documental que deberá proporcionar el **Sujeto Obligado** para dar satisfacción de la derecho humano de acceso a la información de la persona solicitante, deberá considerar que ello no es absoluto, sino que encuentra como excepciones que la información sobre la cual se peticiona el acceso, contenga datos que deban ser clasificados en los términos que la misma Ley de la Materia señala, el **Sujeto Obligado** tendrá que elaborar la versión pública de los documentos que vaya entregar para dar cumplimiento a esta resolución, a fin de satisfacer el derecho de acceso a la información pública de la recurrente sin menoscabar el derecho a la protección de los datos personales de terceros.

Lo anterior, de conformidad a lo que señalan los artículos 3 fracciones IX, XX, XXI y XLV, 91, 132 fracciones II y III, y 143 fracción I de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios que establecen:

*“****Artículo 3****. Para los efectos de la presente Ley se entenderá por:*

*[…]*

***IX. Datos personales:*** *La información concerniente a una persona, identificada o identificable según lo dispuesto por la Ley de Protección de Datos Personales del Estado de México;*

***XX. Información clasificada****: Aquella considerada por la presente Ley como reservada o confidencial;*

***XXI. Información confidencial:*** *Se considera como información confidencial 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;*

***XLV. Versión pública:*** *Documento en el que se elimine, suprime o borra la información clasificada como reservada o confidencial para permitir su acceso.*

*[…]*

***Artículo 91.*** *El acceso a la información pública será restringido excepcionalmente, cuando ésta sea clasificada como reservada o confidencial.*

***Artículo 132.*** *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 143****. Para los efectos de esta Ley se considera información confidencial, la clasificada como tal, de manera permanente, por su naturaleza, cuando:*

***I.*** *Se refiera a la información privada y los datos personales concernientes a una persona física o jurídico colectiva identificada o identificable;*

***II.*** *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; y*

***III****. La que presenten los particulares a los sujetos obligados, de conformidad con lo dispuesto por las leyes o los tratados internacionales.*

*La información confidencial no estará sujeta a temporalidad alguna y sólo podrán tener acceso a ella los titulares de la misma, sus representantes y los servidores públicos facultados para ello.*

*No se considerará confidencial la información que se encuentre en los registros públicos o en fuentes de acceso público, ni tampoco la que sea considerada por la presente ley como información pública.”*

Igualmente, los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas, emitidos por el Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, publicados en el Diario Oficial de la Federación el día quince de abril de dos mil dieciséis, que se encontraban vigentes a la fecha de la solicitud, tienen por objeto establecer los criterios con base en los cuales los sujetos obligados clasificarán como reservada o confidencial la información que posean, desclasificarán y generarán, en su caso, versiones públicas de expedientes o documentos que contengan partes o secciones clasificadas.

Entorno a lo que aquí nos interesa, los Lineamientos Quincuagésimo, Quincuagésimo primero, Quincuagésimo segundo, Quincuagésimo cuarto y Quincuagésimo quinto, vigentes a la fecha de la solicitud, señalan las formalidades que deberá llevar el acuerdo de clasificación que deberá emitir el **Sujeto Obligado**, siendo estas las siguientes:

*“CAPÍTULO VIII*

*DE LOS ELEMENTOS PARA LA CLASIFICACIÓN*

***Quincuagésimo.*** *Los titulares de las áreas de los sujetos obligados podrán establecer sus propios modelos o formatos para la elaboración de versiones públicas de documentos o expedientes, siempre y cuando cumplan lo establecido en los presentes Lineamientos, así como en las correspondientes Leyes Generales.*

***Quincuagésimo primero.*** *Toda acta del Comité de Transparencia deberá contener:*

*I. El número de sesión y fecha;*

*II. El nombre del área que solicitó la clasificación de información;*

*III. La fundamentación legal y motivación correspondiente;*

*IV. La resolución o resoluciones aprobadas; y*

*V. La rúbrica o firma digital de cada integrante del Comité de Transparencia.*

*[…]*

*En los casos de resoluciones del Comité de Transparencia en las que se* ***confirme la clasificación de información confidencial solo se deberán de identificar los tipos de datos protegidos, de conformidad con el lineamiento trigésimo octavo.***

***Quincuagésimo segundo.*** *Para la clasificación y elaboración de versiones públicas de documentos que contengan información clasificada como reservada o* ***confidencial,*** *las áreas de los sujetos obligados deberán tomar las medidas pertinentes tendientes a asegurar que el espacio utilizado para testar la información no podrá ser empleado para la sobreposición de contenido distinto al autorizado por el Comité.*

*En el caso específico de la clasificación y elaboración de versiones públicas de documentos que contengan información confidencial, las áreas de los sujetos obligados deberán:*

***I. Fijar la fecha en que se elaboró la versión pública y la fecha en la cual el Comité de Transparencia confirmó dicha versión;***

***II. Señalar dentro del documento el tipo de información confidencial que fue testada en cada caso específico, de conformidad con el lineamiento trigésimo octavo; y***

***III. Señalar las personas o instancias autorizadas a acceder a la información clasificada.***

*En los documentos de difusión electrónica, señalar en la primera hoja y en el nombre del archivo, que la versión pública corresponde a un documento que contiene* ***información confidencial.***

***[…]***

***Quincuagésimo cuarto.*** *Cuando el Comité de Transparencia confirme la clasificación de documentos reservados y/o* ***confidenciales****, sea total o parcialmente; se deberá anexar al expediente la resolución que determinó la clasificación o, en su defecto, identificar en la carátula del expediente del cual formen parte, la fecha y sesión del Comité de Transparencia en la que se confirmó dicha clasificación.*

***Quincuagésimo quinto.*** *Cada área del sujeto obligado podrá designar formalmente a una o más personas como responsables del testado, que sean encargadas de la adecuada elaboración o supervisión de las versiones públicas de los documentos o expedientes, verificando que cumplan con los requisitos señalados en las Leyes Generales, los presentes Lineamientos y demás normativa aplicable antes de su confirmación por el Comité de Transparencia.” (Énfasis añadido)*

Entorno a lo que aquí nos interesa, los Lineamientos Quincuagésimo sexto, Quincuagésimo séptimo y Quincuagésimo octavo, establecen lo siguiente:

*“****Quincuagésimo sexto.*** *La versión pública del documento o expediente que contenga partes o secciones reservadas o confidenciales, será elaborada por los sujetos obligados, previo pago de los costos de reproducción, a través de sus áreas y deberá ser aprobada por su Comité de Transparencia*

***Quincuagésimo séptimo.*** *Se considera, en principio, como información pública y no podrá omitirse de las versiones públicas la siguiente:*

***I.*** *La relativa a las Obligaciones de Transparencia que contempla el Título V de la Ley General y las demás disposiciones legales aplicables;*

***II.*** *El nombre de los servidores públicos en los documentos, y sus firmas autógrafas, cuando sean utilizados en el ejercicio de las facultades conferidas para el desempeño del servicio público, y*

***III.*** *La información que documente decisiones y los actos de autoridad concluidos de los sujetos obligados, así como el ejercicio de las facultades o actividades de los servidores públicos, de manera que se pueda valorar el desempeño de los mismos.*

*Lo anterior, siempre y cuando no se acredite alguna causal de clasificación, prevista en las leyes o en los tratados internaciones suscritos por el Estado mexicano.*

***Quincuagésimo octavo****. Los sujetos obligados garantizarán que los sistemas o medios empleados para eliminar la información en las versiones públicas no permitan la recuperación o visualización de la misma.”*

De esta manera, en la versión pública de los documentos que se ordenan se deben testar aquellos elementos señalados en la presente resolución, en el entendido de que debe ser pública toda la demás información relacionada que no encuadre en los supuestos previstos en la Ley de la materia.

Por lo tanto, la entrega de documentos en su versión pública debe acompañarse necesariamente del Acuerdo del Comité de Transparencia que la sustente el cual debe estar debidamente fundado y motivado, en el que se expongan los fundamentos y razonamientos que llevaron al **Sujeto Obligado** a testar, suprimir o eliminar datos de dicho soporte documental, ya que no hacerlo, se reitera que lo entregado no tendría un sustento jurídico ni resultaría ser una versión pública, sino más bien una documentación ilegible, incompleta o tachada; ya que el no justificar las causas o motivos por las que no se aprecian determinados datos -ya sea porque se testan o suprimen- deja al solicitante en estado de incertidumbre, al no conocer o comprender porque no aparecen en la documentación respectiva.

Así, con fundamento en lo prescrito en los artículos 5 párrafos trigésimo séptimo, trigésimo octavo y trigésimo noveno de la Constitución Política del Estado Libre y Soberano de México; 2, fracción II; 29, 36 fracciones I y II; 176, 178, 181, 185, fracción I, 186, fracción III, así como 188 de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, este Pleno:

**III. R E S U E L V E**

**Primero.** Resultan **fundados** los motivos de inconformidad hechos valer por la parte **Recurrente** en el recurso de revisión **01299/INFOEM/IP/RR/2025,** por lo que, en términos del Considerando **Cuarto** de la presente resolución, se **Revoca** la respuestadel **Sujeto Obligado.**

**Segundo.** Se **Ordena** al **Sujeto Obligado**, en términos de los Considerandos **Cuarto y Quinto** de esta resolución, **haga entrega vía Sistema de Acceso a la Información Mexiquense (SAIMEX), previa búsqueda exhaustiva y razonable**, los documentos donde conste lo siguiente:

1. Los avisos de privacidad integrales y simplificados, con los que se cuente al veinte de enero de dos mil veinticinco.
2. En versión pública, el o los documentos de seguridad de las bases o sistemas de datos personales vigentes al veinte de enero de dos mil veinticinco.
3. En versión pública, las cédulas de las bases o sistemas de datos personales vigentes al veinte de enero de dos mil veinticinco.

*Para la entrega en versión pública, se deberá emitir el Acuerdo del Comité de Transparencia de acuerdo con la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, en el que funde y motive las razones sobre los datos que se supriman o eliminen de los soportes documentales objeto de la versión públicas que se formule y se pongan a disposición de* ***la parte Recurrente****, mismo que igualmente hará de su conocimiento.*

**Tercero. Notifíquese,** vía **SAIMEX**, al Titular de la Unidad de Transparencia del **Sujeto Obligado,** la presente resolución para que conforme a los artículos 186, último párrafo y 189, párrafo segundo y 194 de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios; dé cumplimiento a lo ordenado dentro del plazo de diez días hábiles, e informe a este Instituto en un plazo de tres días hábiles siguientes sobre el cumplimiento dado a la presente, y, se le apercibe que en caso de negarse a cumplir la presente resolución o hacerlo de manera parcial, se le impondrá una medida de apremio de conformidad con lo previsto en los artículos 198, 200, fracción III; 214, 215 y 216 de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios.

**Cuarto.** **Notifíquese,** vía **SAIMEX**, al Titular de la Unidad de Transparencia del **Sujeto Obligado,** que de conformidad con el artículo 198 de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, de considerarlo procedente, de manera fundada y motivada, podrá solicitar una ampliación de plazo para el cumplimiento de la presente resolución.

**Quinto. Notifíquese vía SAIMEX,** la presente resolución a la parte **Recurrente**, y hágase del conocimiento que en caso de que considere que la presente resolución le causa algún perjuicio, podrá promover el Juicio de Amparo en los términos de las leyes aplicables, de acuerdo a lo estipulado por el artículo 196 de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios.

ASÍ LO RESUELVE, POR UNANIMIDAD DE VOTOS, EL PLENO DEL INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE MÉXICO Y MUNICIPIOS, CONFORMADO POR LOS COMISIONADOS JOSÉ MARTÍNEZ VILCHIS, MARÍA DEL ROSARIO MEJÍA AYALA, SHARON CRISTINA MORALES MARTÍNEZ, LUIS GUSTAVO PARRA NORIEGA Y GUADALUPE RAMÍREZ PEÑA; EN LA DÉCIMA SEGUNDA SESIÓN ORDINARIA CELEBRADA EL DOS DE ABRIL DE DOS MIL VEINTICINCO, ANTE EL SECRETARIO TÉCNICO DEL PLENO ALEXIS TAPIA RAMÍREZ.

1. Artículo 92. Los sujetos obligados deberán poner a disposición del público de manera permanente y actualizada de forma sencilla, precisa y entendible, en los respectivos medios electrónicos, de acuerdo con sus facultades, atribuciones, funciones u objeto social, según corresponda, la información, por lo menos, de los temas, documentos y políticas que a continuación se señalan: (…) [↑](#footnote-ref-1)
2. “Artículo 3. Para los efectos de la presente Ley se entenderá por: (…) XXII. Información de interés público: Se refiere a la información que resulta relevante o beneficiosa para la sociedad y no simplemente de interés individual, cuya divulgación resulta útil para que el público comprenda las actividades que llevan a cabo los sujetos obligados…” [↑](#footnote-ref-2)
3. “**Artículo 185.** El Instituto resolverá el recurso de revisión conforme a lo siguiente: (…)

II. Admitido el recurso de revisión, la o el Comisionado ponente deberá integrar un expediente y ponerlo a disposición de las partes, para que, en un plazo máximo de siete días hábiles, manifiesten lo que a su derecho convenga;” [↑](#footnote-ref-3)
4. Isabel Davara F. de Marcos (Coordinadora), “Diccionario de Protección de Datos Personales. Conceptos fundamentales”. INAI. México 2019. Páginas 828 y 829.

“…

Así, desde la perspectiva de la protección de datos personales, la situación de emergencia se presenta como un fundamento para el tratamiento de los datos personales para hacer frente a contingencias que podrían afectar el bienestar y seguridad de las personas a una gran escala (epidemias, desastres naturales, terrorismo y pandemias) o en un nivel individual (violencia familiar), pues en caso de que dicho tratamiento se sujete a mecanismos como el consentimiento y no se cuente con este último, las consecuencias de no facilitar la información personal necesaria en situaciones de emergencia pueden ser funestas, ya que en un contexto de esta naturaleza el acceso oportuno a la información es fundamental para atender las contingencias y proteger los derechos de los titulares y/o de terceras personas.” [↑](#footnote-ref-4)