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 veintiuno (21) de agosto de dos mil veinticuatro.

**VISTO el** expediente electrónico formado con motivo del recurso de revisión **05348/INFOEM/IP/RR/2023,** promovido por XXX XXX**,** en su calidad de **RECURRENTE**, en contra de la respuesta de la **Unidad de Asuntos Internos**,en lo sucesivo el **SUJETO OBLIGADO,** se procede a dictar la presente resolución, con base en los siguientes:

# **ANTECEDENTES**

1. El veinte (20) de julio de dos mil veintitrés, **EL RECURRENTE** presentó**,** ante el **SUJETO OBLIGADO** vía Plataforma Nacional de Transparencia **(PNT)** y Sistema de Acceso a la Información Mexiquense (**SAIMEX)**, la solicitud de información pública registrada con el número **00023/UAI/IP/2023**, la cual se tuvo por presentada el treinta y uno (31) de julio de dos mil veintitrés, por ser el siguiente día hábil,mediante la cual solicitó lo siguiente:

*“En cumplimiento al artículo 33 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados le solicito los documentos donde consten o en los cuales se pudiera obtener lo siguiente: A. La (s) política (s) gestión y tratamiento de los datos personales B. Las funciones y obligaciones del personal involucrado en el tratamiento de datos personales; C. El inventario de datos personales y de los sistemas de tratamiento; D. El procedimiento de análisis de riesgos E. Los resultados de los análisis de riesgo de los datos personales, en el cual debieron de haber considerado 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; F. Los resultados de los análisis de brecha (comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable) G. El plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales; H. El procedimiento o mecanismos de monitoreo periódico de las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, I. El programa de capacitación de acuerdo al nivel, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales J. Procedimiento de Auditoría al sistema de gestión de protección de datos personales y se indique quien realiza ese procedimiento K. Los resultados de las auditorías al sistema de gestión de protección de datos personales desde su implementación a la fecha Por favor NO ENTREGAR SU DOCUMENTO ORIENTADOR, solo la DOCUMENTACIÓN SOLICITADA y que HA GENERADO esa dependencia, la temporalidad de la información solicitada: de enero del año 2018 al 20 de julio de 2023 a excepción del numeral K). Por ultimo me permito solicitar el documento de seguridad de esta Institución de manera íntegra, de no ser así, favor de remitirlo en versión pública.”*

1. Señaló como modalidad de entrega de la información a través del **SAIMEX.**
2. El veintiuno (21) de agosto de dos mil veintitrés dio respuesta a la solicitud, en los siguientes términos:

*“Se adjunta respuesta a su Solicitud de Acceso a la Información Pública con número de folio 00023/UAI/IP/2023 a fin de dar cumplimiento a su requerimiento.*

*ATENTAMENTE*

*LIC. MIRIAM ROCÍO SANTANA RAMÍREZ” (sic)*

1. El Sujeto Obligado adjuntó a la respuesta los siguientes documentos electrónicos:

* **OFICIO DE RESPUESTA A LA SOLICITUD DE INFORMACIÓN 00023-UAI-IP-2023.pdf:** Oficio UT\*UAI/0114/2023 signado por el Titular de la Unidad de Transparencia en el que refiere que la información requerida por el particular actualiza causal de clasificación como información confidencial, por lo que se remite el acta correspondiente del Comité de Transparencia.
* **ACTA DE LA SEXTA SESIÓN EXTRAORDINARIA 2023.pdf:** Contiene el Acta de la Sexta Sesión Extraordinaria de 2023 de Comité de Transparencia del Sujeto Obligado mediante el cual se aprobó por unanimidad de votos la clasificación de la información requerida.

1. El tres (3) de septiembre de dos mil veinticuatro, **EL RECURRENTE** interpuso el recurso de revisión, en contra de la respuesta; sin embargo, al corresponder a día inhábil, se tuvo por presentado el cuatro (4) de septiembre de dos mil veintitrés y señaló como:

**Acto impugnado:** *“la clasificación de la información” (sic)*

**Motivos o razones de inconformidad: “***…” (sic)*

1. El Recurrente adjuntó el documento electrónico denominado Archivo1693795111844null, del cual no se puede visualizar su contenido.
2. Se registró el recurso revisión bajo el número de expediente al rubro indicado, asimismo con fundamento en lo dispuesto por el artículo 185 fracción I de la **Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios** se turnó a la **Comisionada María del Rosario Mejía Ayala,** con el objeto de su análisis.
3. La Comisionada Ponente con fundamento en lo dispuesto por el artículo 185 fracción II de la ley de la materia, a través del acuerdo de admisión de fecha once (11) de septiembre de dos mil veintitrés, puso a disposición de las partes el expediente electrónico vía **SAIMEX** a efecto de que en un plazo máximo de siete días manifestaran lo que a derecho convinieran, ofrecieran pruebas y alegatos según corresponda al caso concreto, de esta forma para que el **SUJETO OBLIGADO** presentara el informe justificado procedente.
4. El **SUJETO OBLIGADO** el diecinueve (19) de septiembre de dos mil veintitrés, rindió informe justificado a través del documento electrónico denominado **INFORME JUSTIFICADO 05348-INFOEM-IP-RR-2023.pdf**, el cual se puso a la vista del Recurrente el dieciséis (16) de julio de dos mil veinticuatro; sin embargo, se describe su contenido medular, siendo el siguiente:

* ***INFORME JUSTIFICADO 05348-INFOEM-IP-RR-2023.pdf:*** Documento remitido por el Titular de la Unidad de Transparencia mediante el cual ratifica su respuesta inicial, argumentando que no puede proporcionar la información por actualizar causal de clasificación como confidencial.

1. El dieciséis (16) de julio de dos mil veinticuatro, la Comisionada Ponente notificó el acuerdo de ampliación para emitir resolución.
2. El cinco (5) de agosto de dos mil veinticuatro se notificó el acuerdo mediante el cual se decretó el cierre de instrucción.
3. Este organismo garante no pasa por alto explicar que la dilación en la resolución del presente asunto encuentra su justificación en que, el alto número de recursos de revisión recibidos ha incrementado el número de medios de impugnación que deben resolverse por este instituto, circunstancia atípica que ha rebasado las capacidades técnicas y humanas del personal encargado de la elaboración de resoluciones a dichos medios de impugnación.
4. Por ello, es menester precisar que, si bien se ha excedido el plazo para resolver el presente medio de impugnación, de conformidad con la ley de la materia, el plazo para emitir resolución se encuentra justificado en los elementos para medir su razonabilidad de asuntos conforme a los parámetros establecidos por diversos órganos jurisdiccionales federales, aplicables también en procedimientos análogos, como el que nos ocupa.
5. Así, en términos de lo que establecen los artículos 8.1 y 25 de la Convención Americana sobre Derechos Humanos, los recursos deben ser sencillos y resolverse en el menor tiempo posible, tomando en consideración la dilación total del procedimiento; esto es, en un plazo razonable.
6. En ese sentido, el legislador fijó los términos procesales en las leyes, de manera general, sin que pudiera prever la variada gama de casos que son resueltos por los órganos jurisdiccionales o cuasi jurisdiccionales, tanto por la complejidad de los hechos, como por el número de casos que conocen.
7. Por ello, excepcionalmente, si un asunto es resuelto con posterioridad a los plazos señalados por la norma debe analizarse la razonabilidad del tiempo necesario para su resolución, atentos a los siguientes criterios:

a) Complejidad del asunto: La complejidad de la prueba, la pluralidad de sujetos procesales, el tiempo transcurrido, las características y contexto del recurso.

b) Actividad Procesal del interesado: Acciones u omisiones del interesado.

c) Conducta de la Autoridad: Las Acciones u omisiones realizadas en el procedimiento. Así como si la autoridad actuó con la debida diligencia.

d) La afectación generada en la situación jurídica de la persona involucrada en el proceso: Violación a sus derechos humanos.

1. De modo que, cuando se trate de un asunto excepcional, por alguna o todas las características mencionadas o bien, cuando el ingreso de asuntos al órgano jurisdiccional o cuasi jurisdiccional respectivo supere notoriamente al que podría considerarse normal, debe concluirse que es una excluyente de responsabilidad en relación con la actuación del funcionario, como ha acontecido en el caso que nos ocupa.
2. Argumento que encuentra sustento en la jurisprudencia P./J. 32/92 emitida por el Pleno de la Suprema Corte de Justicia de la Nación de rubro “TÉRMINOS PROCESALES. PARA DETERMINAR SI UN FUNCIONARIO JUDICIAL ACTUÓ INDEBIDAMENTE POR NO RESPETARLOS SE DEBE ATENDER AL PRESUPUESTO QUE CONSIDERÓ EL LEGISLADOR AL FIJARLOS Y LAS CARACTERÍSTICAS DEL CASO.”, visible en la Gaceta del Seminario Judicial de la Federación con el registro digital 205635.
3. Razones por las cuales cabe concluir que, la resolución al recurso de revisión se solventa hasta esta fecha, debido a que existe una excesiva carga de trabajo en desproporción a la capacidad de los recursos materiales y humanos con que cuenta este Instituto para atender la enorme demanda de usuarios que acuden para que se les garantice su Derecho de acceso a la información Pública y Protección de Datos Personales, aunado a la complejidad de los hechos a los que se refieren, así como al volumen del expediente, la extensión de los escritos y pruebas aportadas y desahogadas por las partes; lo que impide la tramitación de los recursos dentro de los términos legales previamente establecidos por la Ley, por tratarse de causas de fuerza mayor.
4. Al respecto, también son de considerar los criterios sostenidos por el Cuarto Tribunal Colegiado en Materia Administrativa del Primer Circuito, cuyos rubros y datos de identificación son los siguientes:

“PLAZO RAZONABLE PARA RESOLVER. DIMENSIÓN Y EFECTOS DE ESTE CONCEPTO CUANDO SE ADUCE EXCESIVA CARGA DE TRABAJO.” consultable en el Seminario Judicial de la Federación y su gaceta, con el registro digital 2002351.

“PLAZO RAZONABLE PARA RESOLVER. CONCEPTO Y ELEMENTOS QUE LO INTEGRAN A LA LUZ DEL DERECHO INTERNACIONAL DE LOS DERECHOS HUMANOS.”, visible en el Seminario Judicial de la Federación y su gaceta, con el registro digital 2002350.

1. Por ello, este organismo garante comprometido con la tutela de los derechos humanos confiados, señala que este exceso del plazo legal para resolver el presente asunto, resulta de carácter excepcional.

# **CONSIDERANDO**

## **PRIMERO. De la competencia**

1. Este 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 del presente recurso de conformidad con el artículo: 6, apartado A, fracción IV de la **Constitución Política de los Estados Unidos Mexicanos**; 5, párrafos trigésimo segundo, trigésimo tercero y trigésimo cuarto fracciones IV y V de la **Constitución Política del Estado Libre y Soberano de México**; artículos 1, 2 fracción II, 13, 29, 36 fracciones I y II, 176, 178, 179, 181 párrafo tercero y 185 de la **Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios**; y 7, 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. De la oportunidad y procedencia.**

1. El medio de impugnación fue presentado a través del SAIMEX en el formato previamente aprobado para tal efecto y dentro del plazo legal de quince días hábiles otorgados; siendo así que el **SUJETO OBLIGADO** entregó respuesta el veintiuno (21) de agosto de dos mil veintitrés, de tal forma que el plazo para interponer el recurso de revisión transcurrió del veintidós (22) de agosto al once (11) de septiembre de dos mil veintitrés, el recurso de revisión fue interpuesto el cuatro (4) de septiembre de dos mil veintitrés, éste se encuentra dentro de los márgenes temporales previstos en el artículo 178 de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipiosvigente.
2. Consecuencia de lo anterior, este Órgano Garante advierte que el escrito contiene las formalidades previstas por el artículo 180 último párrafo de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, por lo que es procedente que este Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios, conozca y resuelva el presente recurso.

# **TERCERO. Planteamiento de la Litis**

1. El recurrente solicitó la siguiente información de enero del año 2018 al 20 de julio de 2023:

* *A. La (s) política (s) gestión y tratamiento de los datos personales*
* *B. Las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;*
* *C. El inventario de datos personales y de los sistemas de tratamiento;*
* *D. El procedimiento de análisis de riesgos*
* *E. Los resultados de los análisis de riesgo de los datos personales, en el cual debieron de haber considerado 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;*
* *F. Los resultados de los análisis de brecha (comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable)*
* *G. El plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;*
* *H. El procedimiento o mecanismos de monitoreo periódico de las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales,*
* *I. El programa de capacitación de acuerdo al nivel, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales*
* *J. Procedimiento de Auditoría al sistema de gestión de protección de datos personales y se indique quien realiza ese procedimiento*
* *K. Los resultados de las auditorías al sistema de gestión de protección de datos personales desde su implementación a la fecha*
* *L. Documento de seguridad de esta Institución de manera íntegra, de no ser así, favor de remitirlo en versión pública.*

1. El Sujeto Obligado clasificó la información como confidencial.
2. El Recurrente se inconformó por la clasificación de la información.
3. Por lo tanto, el presente recurso de revisión se circunscribe en determinar si se actualiza las causales de procedenciacontenidas en el artículo 179 fracciones II, relativo a la entrega de información incompleta, de la **Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios**.

## **CUARTO. Estudio y Resolución del asunto.**

**I. De la atención a la solicitud de información.**

## **De la fuente obligacional**

1. El Derecho de Acceso a la Información Pública, es un derecho humano reconocido en el Pacto de Derechos Civiles y Políticos en su artículo 19.2; en la Convención Americana sobre Derechos Humanos en su artículo 13.1; en el artículo sexto de la Constitución Política de los Estados Unidos Mexicanos y en el artículo quinto de la Particular del Estado de México, por lo que al respecto el **SUJETO OBLIGADO** debe ser cuidadoso del debido cumplimiento de las obligaciones constitucionales que se le imponen, en consecuencia, a todas las autoridades, en el ámbito de su competencia, según lo dispone el tercer párrafo del artículo primero de la **Constitución Política de los Estados Unidos Mexicanos** al señalar la obligación de “promover, **respetar**, proteger y **garantizar** los derechos humanos”, entre los cuales se encuentra dicho derecho.
2. Definiendo el Derecho de Acceso a la Información Pública como: *La igualdad de oportunidades para recibir, buscar e impartir información[[1]](#footnote-1)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,[[2]](#footnote-2)*que se constituye como una herramienta fundamental para ejercer *el control democrático de las gestiones estatales, de forma tal que puedan cuestionar, indagar y considerar si se está dando un adecuado cumplimiento a las funciones públicas,[[3]](#footnote-3)*fomentando *la transparencia de las actividades estatales y* promoviendo *la responsabilidad de los funcionarios sobre su gestión pública,[[4]](#footnote-4)*que permite *saber qué están haciendo los gobiernos por sus pueblos, sin lo cual la verdad languidecería y la participación en el gobierno permanecería fragmentada.*
3. Se deduce que el derecho de acceso a la información pública es un derecho humano constitucionalmente reconocido, en consecuencia, todas las autoridades en el ámbito de sus competencias, funciones y atribuciones tienen la obligación de respetarlo, protegerlo y garantizarlo.

1. En tal sentido, el derecho de acceso a la información constituye una garantía primaria, tal y como lo señala el artículo 150 de la Ley de Transparencia y Acceso a la Información del Estado de México y Municipios, que además, establece que se regirá *por los principios de simplicidad, rapidez gratuidad del procedimiento, auxilio y orientación a los particulares*, contemplando el derecho de las personas con discapacidad y hablantes de lengua indígena.
2. Es así que la **Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios,** cuyo objeto es establecer principios, bases generales y procedimientos para tutelar y garantizar la transparencia y el derecho humano de acceso a la información pública en posesión de los sujetos obligados; en su artículo 176establece que ***el recurso de revisión es la garantía secundaria mediante la cual se pretende reparar cualquier posible afectación al derecho de acceso a la información pública*, s**iendo éste el medio a través del cual, este Órgano Garante después de realizar el análisis al procedimiento de acceso a la información, podrá determinar la posible afectación y de ser el caso ordenar la reparación a la violación del derecho en cuestión.
3. Establecido lo anterior, resulta evidente que las razones o motivos de inconformidad hechos valer en el recurso de revisión resultan **fundadas y procedentes**, debido a que el **SUJETO OBLIGADO** proporcionó información que no corresponde con lo solicitado.
4. Ahora bien, para entender los alcances de la información pública se considera importante citar el criterio de interpretación en el orden administrativo número 0002-11, emitido por Acuerdo del Pleno de este 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 dispone:

***“CRITERIO 0002-11***

***INFORMACIÓN PÚBLICA, CONCEPTO DE, EN MATERIA DE TRANSPARENCIA. INTERPRETACIÓN TEMÁTICA 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:*

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

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

*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.”*

1. El derecho de acceso a la información encuentra su materia elemental en los documentos, y la Ley de Transparencia local nos brinda el siguiente concepto, para darnos un mejor panorama:

***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;*

1. Es así que, todos los actos de autoridad que realicen los Sujetos Obligados deben estar documentados y, bajo el más alto estándar de transparencia deberán poner toda la información que se encuentre en su posesión, a disposición de los particulares que la soliciten.
2. Resulta necesario referir que, el artículo 6° apartado A fracción I, de la Constitución Política de los Estados Unidos Mexicanos, artículo 5 fracción I de la Constitución Política del Estado Libre y Soberano de México y el artículo 18 de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, guardan una estrecha relación, puesto que los ordenamientos citados concurren refiriendo que **los Sujetos Obligados deberán documentar todo acto que se derive del ejercicio de sus facultades, competencias o funciones,** considerando desde su origen la eventual publicidad y reutilización de la información que generen, posean o administren.
3. Además, debemos tomar en cuenta los artículos 4 y 12, de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, los cuales establecen lo siguiente:

***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 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.*

***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.***

1. Es así que, por un lado se tiene la obligación de documentar todos los actos que se lleven a cabo en el ejercicio de sus funciones, atribuciones y competencias, mientras que por otro, se ven impuestos por la obligación de hacer pública toda aquella información que se encuentre en su posesión en estricto apego a los principios de eficacia[[5]](#footnote-5) y máxima publicidad, sobre éste último se debe poner mayor énfasis, puesto que establece que toda la información en posesión de los Sujetos Obligados será pública, completa, oportuna y accesible, lo que permite que la ciudadanía tenga un amplio acceso sobre lo que es el actuar de las autoridades.
2. Robustece lo anterior la Tesis aislada identificada con la clave I.4º.A.40 A del Cuarto Tribunal colegiado en Materia Administrativa del Primer Circuito, publicada en el Seminario Judicial de la Federación y su Gaceta en el libro XVIII, Marzo 2013, Página 1899.

***ACCESO A LA INFORMACIÓN. IMPLICACIÓN DEL PRINCIPIO DE MÁXIMA PUBLICIDAD EN EL DERECHO FUNDAMENTAL RELATIVO.*** *Del artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos se advierte que el Estado Mexicano está constreñido a publicitar sus actos, pues se reconoce el derecho fundamental de los ciudadanos a acceder a la información que obra en poder de la autoridad, que como lo ha expuesto el Pleno de la Suprema Corte de Justicia de la Nación en la tesis P./J. 54/2008, publicada en el Semanario Judicial de la Federación y su Gaceta, Novena Época, Tomo XXVII, junio de 2008, página 743, de rubro: "ACCESO A LA INFORMACIÓN. SU NATURALEZA COMO GARANTÍAS INDIVIDUAL Y SOCIAL.", contiene una doble dimensión: individual y social. En su primer aspecto, cumple con la función de maximizar el campo de la autonomía personal, posibilitando el ejercicio de la libertad de expresión en un contexto de mayor diversidad de datos, voces y opiniones, mientras que en el segundo, brinda un derecho colectivo o social que tiende a revelar el empleo instrumental de la información no sólo como factor de autorrealización personal, sino como un mecanismo de control institucional, pues se trata de un derecho fundado en una de las características principales del gobierno republicano, que es la publicidad de los actos de gobierno y la transparencia en el actuar de la administración, conducente y necesaria para la rendición de cuentas. Por ello, el principio de máxima publicidad incorporado en el texto constitucional, implica para cualquier autoridad, realizar un manejo de la información bajo la premisa inicial que toda ella es pública y sólo por excepción, en los casos expresamente previstos en la legislación secundaria y justificados bajo determinadas circunstancias, se podrá clasificar como confidencial o reservada, esto es, considerarla con una calidad diversa.*

*CUARTO TRIBUNAL COLEGIADO EN MATERIA ADMINISTRATIVA DEL PRIMER CIRCUITO.*

*Amparo en revisión 257/2012. Ruth Corona Muñoz. 6 de diciembre de 2012. Unanimidad de votos. Ponente: Jean Claude Tron Petit. Secretaria: Mayra Susana Martínez López.*

1. Como se ha señalado, los Sujetos Obligados deberán proporcionar toda la información que se encuentre en su posesión bajo los estándares más altos de transparencia y máxima publicidad.
2. Es pertinente enfatizar lo que respecto al derecho de acceso a la información pública, refiere el artículo 6° de la Constitución Política de los Estados Unidos Mexicanos, que en su parte conducente señala:

***“Artículo 6o.*** *La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, la vida privada o los derechos de terceros, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley.* ***El derecho a la información será garantizado por el Estado.***

*Toda persona tiene derecho al libre acceso a información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión.*

*Para efectos de lo dispuesto en el presente artículo se observará lo siguiente:*

*A. Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, 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.*

*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 los organismos autónomos especializados e imparciales que establece esta Constitución.*

***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.*

*VIII. Federación contará con un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados en los términos que establezca la ley.*

*…*

*La ley establecerá aquella información que se considere reservada o confidencial.”*

*(Énfasis añadido)*

1. Por su parte, la Constitución Política del Estado Libre y Soberano de México, en su artículo 5°, dispone en su parte conducente, lo siguiente:

***“Artículo 5. …***

***El derecho a la información será garantizado por el Estado****. La ley establecerá las previsiones que permitan asegurar la protección, el respeto y la difusión de este derecho.*

*Para garantizar el ejercicio del derecho de transparencia, acceso a la información pública y protección de datos personales, los poderes públicos y los organismos autónomos, transparentarán sus acciones, en términos de las disposiciones aplicables, la información será oportuna, clara, veraz y de fácil acceso.*

*Este derecho se regirá por los principios y bases siguientes:*

***I. Toda la información en posesión*** *de cualquier autoridad, entidad, órgano y organismos de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos estatales y municipales, así como* ***del gobierno y de la administración pública municipal y sus organismos descentralizados****, asimismo de cualquier persona física, jurídica colectiva o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito estatal y municipal,* ***es pública*** *y sólo podrá ser reservada temporalmente por razones previstas en la Constitución Política de los Estados Unidos Mexicanos de interés público y seguridad, 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 referente a la intimidad de la vida privada y la imagen de las personas será protegida a través de un marco jurídico rígido de tratamiento y manejo de datos personales, con las excepciones que establezca la ley reglamentaria.*

*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 el organismo autónomo especializado e imparcial que establece esta Constitución.*

*V. Los procedimientos de acceso a la información pública, de acceso, corrección y supresión de datos personales, así como los recursos de revisión derivados de los mismos, podrán tramitarse por medios electrónicos, a través de un sistema automatizado que para tal efecto establezca la ley reglamentaria y el organismo autónomo garante en el ámbito de su competencia. Las resoluciones que correspondan a estos procedimientos se sistematizarán para favorecer su consulta.*

***VI. 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 los resultados obtenidos.*

*VII. La ley reglamentaria, determinará la manera en que los sujetos obligados deberán hacer pública la información relativa a los recursos públicos que entreguen a personas físicas o jurídicas colectivas.”*

(Énfasis añadido)

1. Adicional, tenemos que la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, prevé en su artículo 23 fracción I, lo siguiente:

***“Artículo 23. Son sujetos obligados a transparentar y permitir el acceso a su información y proteger los datos personales que obren en su poder****:*

*…*

*I. El Poder Ejecutivo del Estado de México, las dependencias, organismos auxiliares, órganos, entidades, fideicomisos y fondos públicos, así como la Fiscalía General de Justicia del Estado de México;*

***…***

***Los sujetos obligados deberán hacer pública toda aquella información relativa a los montos y las personas a quienes entreguen, por cualquier motivo, recursos públicos****,* ***así como******los informes que dichas personas les entreguen sobre el uso y destino de dichos recursos.***

***Los servidores públicos deberán transparentar sus acciones así como garantizar y respetar el derecho de acceso a la información pública.”***

*(Énfasis añadido)*

1. Es así que, conforme a los preceptos legales citados, se desprende que el derecho de acceso a la información pública es un derecho individual que puede ser ejercido ante cualquier autoridad, entidad, órgano u organismo, tanto federales, como estatales, de la Ciudad de México, o Municipales, con el fin de que los particulares conozcan toda aquella información que es considerada como pública.
2. Por lo anterior, es de referir que, **la Unidad de Asuntos Internos**, al ser un Sujeto Obligado comprendido por la Legislación Local en materia de Transparencia, se encuentra obligado a hacer pública toda aquella información que genere, administre o posea.

**II. Del documento de seguridad.**

1. Derivado de la naturaleza de la información requerida, es necesario traer a contexto la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, pues el artículo 1°, dispone que es una ley de observancia general en toda la República, reglamentaria de los artículos 6o., Base A y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, en materia de protección de datos personales en posesión de sujetos obligados.
2. En los artículos 31 y 32 de este ordenamiento, se establece que el responsable del tratamiento de datos personales deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, con el objetivo de protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.
3. Dicha medidas deben considerar el riesgo inherente a los datos personales tratados; su sensibilidad; el desarrollo tecnológico; las posibles consecuencias de una vulneración para los titulares; las transferencias que se realicen; el número de titulares; las vulneraciones previas ocurridas en los sistemas de tratamiento, y el riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.
4. Para cumplir con lo anterior el artículo 33 de la Ley en cita refiere, los sujetos obligados deben:

* 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;
* Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;
* Elaborar un inventario de datos personales y de los sistemas de tratamiento;
* 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;
* Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;
* 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;
* Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, y
* 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.

1. Ahora bien, la Ley General dispone en el artículo 35 la obligación de generar un **documento de seguridad** que entre otros aspectos contenga el análisis de riesgos, el análisis de brecha; el plan de trabajo; los mecanismos de monitoreo y revisión de las medidas de seguridad, y el programa general de capacitación; información que son de interés del ahora Recurrente.
2. Ahora bien, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, sobre nuestro tema de interés refiere lo siguiente:

*Del objeto de la Ley*

*Artículo 1. La presente Ley es de orden público, interés social y observancia obligatoria en el Estado de México y sus Municipios. Es reglamentaria de las disposiciones en materia de protección de datos personales previstas en la Constitución Política del Estado Libre y Soberano de México. Tiene por objeto establecer las bases, principios y procedimientos para tutelar y garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de los sujetos obligados.*

*De las finalidades de la Ley*

*Artículo 2. Son finalidades de la presente Ley:*

*I. a III. …*

*IV. Proteger los datos personales en posesión de los sujetos obligados del Estado de México y municipios a los que se refiere esta Ley, con la finalidad de regular su debido tratamiento.*

*V. Promover la adopción de medidas de seguridad que garanticen, la integridad, disponibilidad y confidencialidad de los datos personales en posesión de los sujetos obligados, estableciendo los mecanismos para asegurar su cumplimiento.*

*VI. a X.…*

*Glosario*

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

*I. a XVII. …*

*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. XIX. a XXX. …*

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

*XXXII. Medidas de seguridad físicas: a las acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se considerarán las actividades siguientes:*

*a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información.*

*b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información.*

*c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización.*

*d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz que asegure su disponibilidad e integridad.*

*XXXIII. Medidas de seguridad técnicas: a las acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se considerarán las actividades siguientes:*

*a) Prevenir que el acceso a los sistemas y bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados.*

*b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones.*

*c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.*

*d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.*

*XXXIII. a LI. …*

*LII. Violación de la seguridad de los datos personales: a la violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transferidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, o cualquier otra que afecte la confidencialidad, integridad y disponibilidad de los datos personales. Se encuentran comprendidas dentro de este concepto las vulneraciones a las que hace referencia la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.*

*CAPÍTULO SEGUNDO*

*DE LAS MEDIDAS DE SEGURIDAD*

*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.*

*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***

*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.***

*CAPÍTULO TERCERO DE LAS VIOLACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES*

*Plan de Contingencia y Plan de Trabajo*

*Artículo 51. En caso de que ocurra una violación a la seguridad de los datos personales, el responsable implementará las acciones definidas en su plan de contingencia. De manera posterior y durante la ocurrencia de los efectos de la violación a la seguridad de los datos personales, el responsable analizará las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso, a efecto de evitar que la violación se repita.*

1. El o los documentos de seguridad generados por los Responsables del Tratamiento, buscan la protección de los datos personales que se resguardan a través de sistemas y/o bases de datos personales, es importante resaltar que, para dar cumplimiento a la ley de la materia específicamente aplicable a nuestra Entidad, pero plenamente correspondiente con la Ley General, toda las instituciones públicas tienen la obligación de proteger los sistemas de datos personas que administran y para ello, debe cumplir con estándares mínimos que garanticen que los datos no serán alterados, sustraídos, incompletos, inexactos, destruidos, etc., para ello las instituciones públicas deben:

* Proteger los datos personales y promover la adopción de medidas de seguridad en sus sistemas de datos.
* Las medidas de seguridad deben garantizar que los datos personales se mantengan exactos, completos, correctos y actualizados, en atención al principio de calidad.
* **Poner en práctica un programa de capacitación y actualización de su personal, para que conozcan las obligaciones que implica el tratamiento de datos personales.**
* **Implementar políticas y programas de seguridad de los datos personales**, los cuales requieren una revisión continua para realizar las mejoras que se requieran.
* Las medidas de seguridad que se pueden implementar son técnicas, administrativas y físicas y para determinar las que se deben aplicar es necesario tomar en consideración el riesgo inherente, así como el riesgo por el valor potencial de los datos, la sensibilidad de los datos, el desarrollo tecnológico, las posibles consecuencias de vulneración, si se realizan transferencias de los datos, el número de personas de quienes se tratan los datos, así como en su caso, si existieron anteriormente vulneraciones.
* Para establecer las medidas de seguridad es necesario realizar **análisis de riesgo de los datos personales, así como análisis de brecha.**  No se deja de lado que la Ley no establece una temporalidad en la que se deben realizar estar actividades.
* También se requiere **elaborar un plan de trabajo para la implementación de medidas de seguridad,** este se entiende que es trabajo complementario, pues derivado de los análisis la mejora de la protección debe basarse en dicho plan.
* El **documento de seguridad,** debe componerse de diversos apartados entre los que destacan el de **medidas de seguridad,** que a su vez debe integrarse por bitácoras de acceso, operación cotidiana y violaciones a la seguridad de los datos.

1. Para ello, la base de las acciones que se establezcan deben estar en el documento de seguridad, el cual se compone entre otros aspectos con la identificación de los sistemas de datos personales; las medidas de seguridad que se aplican, entre las que se encuentran la **descripción de bitácoras, análisis de riesgos y análisis de brechas.**
2. En este contexto debemos señalar que las medidas de seguridad, son confidenciales de conformidad a lo que contempla el artículo 43 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios que contempla:

*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.*

•Análisis de la información clasificada consistente en medidas de seguridad de los datos personales.

1. El Sujeto Obligado en su versión pública, eliminó por cada sistemas de datos, los rubros siguientes: **análisis de riesgos; análisis de brecha y plan de trabajo**; **mecanismos de monitoreo y seguridad;** supresión y borrado seguro; auditorías; plan de contingencia; procedimiento y respaldo de recuperación de datos; identificación y autentificación; acceso a las instalaciones; gestión de incidentes; bitácoras; resguardo de soportes físicos, estos directamente guardan relación con los mecanismos implementados por el Ayuntamiento para evitar el robo, alteración o supresión no autorizada de los datos personales y poder garantizar que se encuentran completos y sin alteraciones.
2. Como es de explorado derecho, desde hace algunos años, el valor de los datos personales ha incrementado cuando estos están sistematizados, debido al vertiginoso avance de las tecnologías, motivo por el cual incluso, se les ha denominado como “el nuevo oro negro”, en tal sentido el objeto de la Ley de Protección de Datos, busca que en todo momento las instituciones públicas lleven a cabo acciones que impidan un acceso o tratamiento fuera del marco de la ley, pues dado el valor que han cobrado, existen muchos individuos que buscan acceder a los sistemas de datos con fines ilícitos, lo que ocasiona también una vulneración a los derechos humanos de las personas.
3. En tal sentido, el artículo 39, fracción IV, de la Ley en comento señala que se deberán observar deberes para garantizar un nivel de seguridad adecuado al riesgo de los datos personales, pues no es lo mismo tener un sistema de datos personales en donde se contenga el directorio de servidores públicos, con nombre, cargo y extensión telefónica de, centro de trabajo, que uno que contenga el nombre y sueldo sumado al nombre del banco y número de cuenta al que se deposita, incluso no es lo mismo esta información bancaria que los expedientes clínicos que constituyen datos sensibles y que el riesgo que representan es mucho mayor; para ello, parte de esos deberes es realizar un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.
4. Refuerza lo anterior, lo establecido en el artículo 45, fracciones I y VIII, de la Ley en cita, ya que refiere que dentro de los elementos que se deben considerar está el riesgo inherente a los datos personales tratados, así como 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.
5. De acuerdo con lo expuesto, el artículo 49, fracción II, de la Ley multi referida, determina que entre los contenidos que el Documento de seguridad debe contener respecto de los sistemas de datos personales es justamente todos estos contenidos, con el objetivo de que las medidas de seguridad de los datos personales sean continuas y atiendan a cada momento las necesidades del sistema y evidentemente el avance de las tecnologías.
6. Particularmente los análisis de brecha, análisis de riesgo contemplan la áreas de vulnerabilidad de deben ser atendidas por los responsables, los mecanismos de monitoreo y seguridad, supresión y borrado seguro procedimiento y respaldo de recuperación de datos; identificación y autentificación; acceso a las instalaciones, contienen las acciones específicas por tipo de sistema para mantener la seguridad de los datos.
7. Acceso a las instalaciones y auditorías contienen el primero las previsiones de cuidado que se requieren a cada servidor público y las auditorías pueden están programadas para identificar áreas de oportunidad o para identificar actuaciones indebidas, de tal suerte que esta información también corresponde a las medidas de seguridad vigentes de los sistemas de datos personales, por lo que procede su clasificación.
8. Por lo que hace al Plan de Contingencia y el Plan de Trabajo, de acuerdo con los artículos 51 y 52 de la Ley en comento, este se realiza para los casos en que ocurra una violación a la seguridad de los datos personales, con acciones definidas, esto quiere decir que los análisis de riesgo y brecha son antes de que ocurra alguna vulneración, en el caso de que esta llegara a suceder, con el objetivo de que la violación no se repita; lo que debe considerarse como violación a los sistemas de datos son:

• La pérdida, robo, extravío.

• La copia o destrucción no autorizada.

• El uso o tratamiento no autorizado.

• El daño, la alteración o modificación no autorizada.

1. Como se advierte el contenido de estos apartados del Documento de seguridad justamente debe contener en sus apartados estos rubros como parte de las acciones de protección de los sistemas de datos personales que de manera sistemática deben realizar los sujetos obligados; en este sentido, como se trata de medidas de seguridad implementadas y los detalles de las áreas de oportunidad en la protección de los sistemas que van detectando los expertos en protección de sistemas de datos, tanto físicos como electrónicos, constituye información que en manos expertas puede ser utilizada para vulnerar los sistemas de datos personales, por lo que aplica lo dispuesto en el artículo 43 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, ya que si bien, no son formalmente las medidas de seguridad implementadas, se trata del análisis de estas y su eficacia, así como sus áreas de oportunidad sobre lo que se debe hacer o mejorar, por lo que procede su clasificación como información confidencial.

• Programa general de capacitación

1. Sobre el Programa General de Capacitación, el artículo 49, fracción II, inciso o), de la Ley de la materia, dispone también es un elemento que forma parte del documento de seguridad, en relación con las medidas de seguridad. Esto evidentemente y por el avance de las tecnologías implica que los servidores públicos deben ser capacitados sobre las mejores opciones para garantizar la protección de los sistemas de datos personales.
2. Al respecto la Ley en cita, no establece periodos ni detalles sobre cómo y cada cuándo deben realizarse las capacitaciones y lo deja al arbitrio de cada sujeto obligado, en razón evidentemente de sus necesidades, el tipo de sistemas de datos personales con los que cuente y el tipo de los datos. Así, no existe disposición tampoco que indique que esta información deba ser clasificada, por el contrario, hacer público un programa de capacitación permite que las personas conozcan que las instituciones públicas dan la importancia debida a la protección de datos personales y cumplen con sus obligaciones legales, de tal suerte que la información es de naturaleza pública, susceptible de entrega.
3. No obstante lo anterior, se clasificó, por lo que, se revoca la clasificación de este rubro en cada uno de los sistemas de seguridad que testó el Ayuntamiento, pues la entrega de esa información no pone en riesgo los sistemas de datos personales, por el contrario, conocer que los servidores públicos son capacitados para afrontar los retos que implica el avance de las tecnologías, implica brindar confianza a las personas de las que hacen uso y tratamiento de sus datos y en general a toda la población implica un acto de transparencia y rendición de cuentas, por lo que, no actualiza el supuesto de confidencialidad y procede ordenar la entrega de la información.

* **Inventario de datos personales o sistemas de Bases de Datos Personales**

1. Sobre este punto, es conveniente referir que los inventarios de datos personales o sistemas de gestión, forman parte de las actividades interrelacionadas para establecer y mantener las medidas de seguridad, conforme lo que dispone el artículo 46, de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de México y Municipios antes citado, dicho inventario se constituye con la información de cada tratamiento de datos que realice el responsable, que contenga un catálogo de medios físicos y electrónicos, finalidades, tipo de datos tratados, formatos de almacenamiento, lista de los servidores públicos que tienen acceso al tratamiento, en su caso, nombre o razón social del encargado, así como de los destinarios de las transferencias.
2. Realizar el inventario de datos personales implica llevar a cabo un diagnóstico de los datos personales y sistemas de tratamiento que se encuentran bajo resguardo del sujeto obligado, identificando los siguientes elementos relevantes:

1. Cada uno de los procesos en los que la unidad administrativa trata datos personales.

2. La unidad administrativa que está a cargo del proceso en donde se tratan los datos personales, según las atribuciones o facultades normativas.

3. De acuerdo con el ciclo de vida de los datos personales, se debe identificar:

I. ¿Cómo se obtienen los datos personales?

II. ¿Qué tipo de datos personales se tratan? ¿Son sensibles?

III. ¿Dónde se almacenan los datos personales?

IV. ¿Para qué finalidades se utilizan los datos personales?

V. ¿Quién tiene acceso a la base de datos o archivos y a quién se comunican los datos personales al interior de la organización?

VI. ¿Intervienen encargados en el tratamiento de los datos personales?

VII. ¿Qué transferencias se realizan o se podrían realizar de los datos personales y con qué finalidad?

VIII. ¿Se difunden los datos personales?

X. ¿Cuál es el plazo de conservación de los datos personales?

1. En consecuencia, los inventarios de datos personales o los sistemas de bases de datos, son documentos susceptibles de proporcionarse, de ser el caso en versión pública, para tal efecto, deberá estar a lo dispuesto en el Considerando QUINTO de la presente resolución.
2. Por lo que corresponde a las auditorías, como se ha dicho son parte integral del documento de seguridad, como lo establece el citado artículo 49 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de México y Municipios; en ese sentido, es necesario traer a contexto los artículos 18 fracción IV; 44, apartado B, fracción II, inciso b); y 153 del mismo cuerpo normativo, los cuales establecen lo siguiente:

***Mecanismos para demostrar el cumplimiento del principio de responsabilidad***

***Artículo 28.*** *Entre los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en la presente Ley están, al menos, los siguientes:*

*…*

*V. Establecer un sistema de supervisión y vigilancia interna y/o externas, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales*

*…*

***Tipos y Niveles de Seguridad***

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

*…*

***B. Niveles de seguridad:***

*…*

***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.*

***Práctica de Auditorías Voluntarias***

***Artículo 153.*** *Los responsables podrán voluntariamente someterse a la realización de auditorías por parte del Instituto, que tengan por objeto verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la presente Ley y demás normativa que resulte aplicable.*

*El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles implementados por el responsable, identificar sus deficiencias, así como proponer acciones correctivas complementarias, o bien, recomendaciones que en su caso correspondan.*

1. Es así que, de la interpretación al cuerpo normativo, se aprecia que los Sujetos Obligados o Responsables del tratamiento de datos personales, deben implementar sistemas o mecanismos de supervisión y vigilancia respecto a la protección de datos personales, entre los que se encuentra la práctica de auditorías voluntarias, estableciéndose estas como una medida de seguridad a las bases de datos o sistemas de datos de nivel medio.
2. Dichas Auditorias son realizadas por el Instituto y tienen por objeto verificar la adaptación, adecuación y eficacia de los controles de medidas y mecanismos implementados para el cumplimiento de las disposiciones contenidas en la Ley de Datos referida.
3. Por su parte, el Instituto debe emitir un dictamen sobre la adecuación de las medidas y controles implementados por el responsable, identificando sus deficiencias, así como proporciones acciones correctivas y recomendaciones correspondientes.
4. Entonces, al ser parte del Documento de Seguridad, se debe proporcionar el documento donde conste el procedimiento de auditoría al sistema de gestión de datos, así como el responsable de realizar la o las auditorías.
5. En consecuencia, y conforme al artículo 49, fracción II y 149 de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, se deberá hacer entrega del Acuerdo del Comité de Transparencia por el cual se informen de manera fundada y motivada, las causas y/o razones por las cuales dicha información actualiza una causal de clasificación como información confidencial de lo siguiente:

* **Procedimiento de análisis de riesgos;**
* **Resultados de los análisis de riesgo;**
* **Resultados de los análisis de brecha;**
* **Plan de trabajo para la implementación de las medidas de seguridad;**
* **Procedimiento o mecanismos de monitoreo periódico de las medidas de seguridad implementadas, las amenazas y vulneraciones a las que están sujetos los datos personales.**
* **Resultados de las auditorias del sistema de gestión de protección de datos personales desde que se implementaron al veintitrés (23) de agosto de dos mil veintiuno**
* **Las políticas de gestión y tratamiento de los datos personales**

1. Por lo que el Sujeto Obligado deberá emitir, a través del Comité de Transparencia, el acuerdo mediante el cual se clasifique como confidencial la información antes referida.
2. Ahora bien, no es procedente la clasificación de la información en su totalidad de la información como lo hizo valer el Sujeto Obligado, siendo pública aquella información relacionada con los siguientes puntos, razón por la que se ordena su entrega:

* **El inventario de datos personales y los sistemas de tratamiento**
* **Programa o plan de capacitación respecto del tratamiento de los datos personales**;
* **Procedimientos de auditoría al sistema de gestión de protección de datos personales así como quien realiza dicho procedimiento**;
* **Funciones y obligaciones del personal involucrado en el tratamiento de datos personales;**

1. Para la elaboración de las versiones públicas y la clasificación de la información, es necesario que el Sujeto Obligado esté a lo dispuesto en el Considerando QUINTO de la presente resolución.
2. Es así que, como resultado del estudio y análisis de la información que se solicitó, es que se determina que la respuesta del Sujeto Obligado atiende parcialmente la solicitud, pues contrario a lo que manifestó no es procedente la clasificación total del documento de seguridad, es decir, este puede proporcionarse a través de una versión pública, en los términos antes señalados.

# **QUINTO. De la versión pública.**

# **Nociones generales.**

1. Debe destacarse que, debido a la naturaleza de la información solicitada**,** eventualmente pudiera obrar datos personales susceptibles de protegerse, así como información susceptible de clasificarse como reservada, el **Sujeto Obligado** deberá de hacer la adecuada versión pública, protegiendo los datos que no son susceptibles de ser proporcionados.
2. No pasa desapercibido para este Órgano Garante que los **Sujetos Obligados** serán responsables de los datos personales en su posesión y que, en caso de localizarse datos concernientes a terceros, éstos no podrán difundir, distribuir o comercializar los datos personales. Cabe destacar que, para la realización de la clasificación de la información, se deben seguir una serie de pasos y procedimientos, por lo que es menester reiterar los mismos:

|  |  |
| --- | --- |
| a) Requisitos previos. | Los artículos 100 y 122 de la Ley Estatal y de la Ley General, respectivamente, señalan que si los Sujetos Obligados determinan que la información actualiza alguno de los supuestos de clasificación, es deber de los titulares de las áreas proponer su clasificación y no del Comité de Transparencia.  Al hacerlo tienen que precisar de qué información se trata, señalando el supuesto de clasificación (confidencialidad o reserva).  Además, se debe señalar el procedimiento, de los tres que establecen los artículos 132 y 106 de la Ley Estatal y General, respectivamente.  El último de estos requisitos previos consiste en que no se pueden emitir acuerdos de carácter general ni particular, esto es, no se puede hacer un acuerdo para clasificar de manera general todos los documentos de un expediente o área, sin individualizar su análisis y tampoco se puede hacer un acuerdo por cada dato que se vaya a clasificar dentro de un documento con diez datos, por ejemplo, susceptibles de ser clasificados. |
| b) Supuestos de clasificación. | Las disposiciones constitucionales y legales en la materia establecen los dos supuestos generales para clasificar la información: por reserva y por confidencialidad.  Los artículos 116 y 143 de la Ley Estatal y de la Ley General, respectivamente, señalan los supuestos para que la información pueda ser clasificada como confidencial. Mientras que los artículos 105 y 130 de la Ley Estatal y de la Ley General, respectivamente, señalan que la aplicación de estos supuestos debe realizarse de manera restrictiva y limitada, por lo que debe acreditarse que se cumple con esta condición y no se pueden ampliar las excepciones o supuestos de clasificación aduciendo analogía o mayoría de razón.  El **Sujeto Obligado** debe identificar claramente el tipo de información y hacer un juicio de subsunción o encaje para acreditar que el supuesto de hecho corresponde estrictamente con la hipótesis jurídica. Esto también lo debe de realizar el servidor público habilitado y el titular del área que administra la información. |
| c) Formalidades para emitir el acuerdo de clasificación. | El Comité de Transparencia, según lo dispuesto en los artículos cuenta con las facultades para aprobar, modificar o revocar la clasificación de la información que haya propuesto.  Es necesario que **el acto reúna con los requisitos elementales**, entre ellos, que la autoridad que va a emitir el acto de autoridad sea la legalmente facultada para ello.  La decisión de aprobar, modificar o revocar la clasificación deberá de asentarse en un documento que registre la determinación a la que se llegue después de un análisis minucioso a partir de lo propuesto por el Titular del I. área que administra la información, cuyo análisis debe integrarse en la agenda de los asuntos a tratar en las sesiones, se insiste, a partir de las decisiones adoptadas previamente por los titulares de áreas y que son sujetas a control, en primera instancia, por el Comité de Transparencia. |
| d) Requisitos de fondo del acuerdo de clasificación. | Como se ha señalado antes, al hacer el juicio de subsunción o encaje entre el supuesto de hecho y la hipótesis jurídica, se debe acreditar la estricta correspondencia entre un elemento y otro. Ahora, en esta parte del procedimiento, que se desahoga en sede del Comité de Transparencia, la ley señala que la carga de la prueba, para justificar las restricciones, corresponde a los **Sujetos Obligados**, por lo que deberán fundar y motivar debidamente la clasificación.  De lo anterior, se desprende que para una correcta **clasificación total o parcial**, esto es determinar los datos que se suprimen en las versiones públicas, es necesario fundar y motivar, de manera correcta, la clasificación; considerando que todo acto que la autoridad pronuncie en el ejercicio de sus atribuciones, debe expresar los fundamentos legales que le dieron origen y las razones por las que se deben aplicar al caso concreto.  Así, en un acto de autoridad se cumple con la debida fundamentación cuando se cita el precepto legal aplicable al caso concreto y la debida motivación cuando se expresan las razones, motivos o circunstancias que tomó en cuenta la autoridad para adecuar el hecho a los fundamentos de derecho. De este modo, la persona que se sienta afectada pueda impugnar la decisión, permitiéndole una real y auténtica defensa.  En ese mismo sentido, el numeral trigésimo tercero fracción V de los Lineamientos Generales, precisa que para motivar la clasificación se deben acreditar las circunstancias de tiempo, modo y lugar.  Ahora bien, **para cada caso además de fundar y motivar**, se debe identificar con claridad que datos contenidos en las documentales que son susceptibles de suprimirse, por ejemplo; Clave Única de Registro de Población (CURP), Registro Federal de Contribuyentes (R.F.C.), claves de seguros, préstamos o descuentos personales, secretos bancario, fiduciario, industrial, comercial, fiscal, bursátil y postal, cuya titularidad corresponda a particulares, entre otros. |
| e) Condiciones especiales de la clasificación de la información como confidencial. | Los artículos 148 y 120 de la Ley Estatal y de la Ley General, respectivamente, establecen que aun tratándose de datos personales, se podrán proporcionar, incluso sin solicitar el consentimiento de su titular.  En el caso de lo señalado en la fracción IV, será el Instituto quien deba aplicar la prueba de interés público, considerando también que como recientemente ha discutido la Suprema Corte de Justicia de la Nación, los servidores públicos nos encontramos sujetos a un régimen menor de protección.  Pero si la información que se pretende clasificar como confidencial no se encuentra en los supuestos de los artículos señalados y es posible, se deberá consultar al titular de los datos si permite o no el acceso. De no ser posible, la realización de la consulta, procede, fundando y motivando, la clasificación. |

1. Si el servidor público incumple con estas formalidades y entrega la información sin proteger los datos personales incumple con lo que estipula las disposiciones legales establecidas, asimismo que si entrega un documento testado sin el debido acuerdo de clasificación.
2. Por lo anteriormente expuesto y fundado, este **ÓRGANO GARANTE** emite los siguientes:

# **R E S O L U T I V O S**

**PRIMERO.** Resultan parcialmente fundadas lasrazones o motivos de inconformidad hechos valer en el recurso de revisión **05348/INFOEM/IP/RR/2023** en términos de los **Considerandos** **CUARTO y QUINTO** de la presente resolución.

**SEGUNDO.** Se **MODIFICA** la respuesta y se **ORDENA** a la **Unidad de Asuntos Internos** entregar, vía Sistema de Acceso a la Información Mexiquense (SAIMEX), de ser el caso en versión pública, del **primero (01) de enero de dos mil dieciocho al veinte (20) de julio de dos mil veintitrés del o los Documentos de Seguridad,** la siguiente información:

1. **Programa de capacitación;**
2. **Procedimientos de auditoría al sistema de gestión de protección de datos personales así como quien realiza dicho procedimiento**
3. **Funciones y obligaciones del personal involucrado en el tratamiento de datos personales;**

* **Acuerdo del Comité de Transparencia mediante el cual se clasifique como confidencial la información relativa a las medidas de seguridad, análisis de riesgo, análisis de brecha, plan de trabajo y procedimiento o mecanismos de monitoreo periódico de las medidas de seguridad implementadas, las amenazas y vulneraciones a las que están sujetos los datos personales; resultados de las auditorias del sistema de gestión de protección de datos personales desde que se implementaron al veintitrés (23) de agosto de dos mil veintiuno, las políticas de gestión y tratamiento de los datos personales**.

Para efectos de lo anterior se deberá emitir el Acuerdo del Comité de Transparencia en términos de los artículos 49 fracción VIII y 132 fracción II de 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 dentro del soporte documental respectivo objeto de las versiones públicas que se formulen y se ponga a disposición de la parte recurrente.

**TERCERO. NOTIFÍQUESE** la presente resolución al Titular de la Unidad de Transparencia del Sujeto Obligado vía SAIMEX, para que conforme al artículo 186 último párrafo, 189 segundo párrafo 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** al **RECURRENTE** la presente resolución a través del Sistema de Acceso a la Información Mexiquense (SAIMEX).

**QUINTO.** 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, el Sujeto Obligado de manera fundada y motivada, podrá solicitar una ampliación de plazo para el cumplimiento de la presente resolución.

**SEXTO.** Se hace del conocimiento del **RECURRENTE** que, de conformidad con lo establecido en el artículo 196 de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, y en lo dispuesto en los artículos 159 y 160 de la Ley General de Transparencia y Acceso a la Información Pública, en caso de que considere que la resolución le cause algún perjuicio podrá impugnarla vía recurso de inconformidad ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos, o bien, vía juicio de amparo en los términos de las leyes aplicables.

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 VIGÉSIMA NOVENA SESIÓN ORDINARIA CELEBRADA EL VEINTIUNO (21) DE AGOSTO DE DOS MIL VEINTICUATRO, ANTE EL SECRETARIO TÉCNICO DEL PLENO ALEXIS TAPIA RAMÍREZ.

1. Convención Americana sobre Derechos Humanos. Artículo 13. [↑](#footnote-ref-1)
2. Constitución Política de los Estados Unidos Mexicanos. Artículo sexto, sección A, fracción I. [↑](#footnote-ref-2)
3. Corte Interamericana de Derechos Humanos. Caso Claude Reyes y otros vs. Chile. Sentencia de 19 de septiembre de 2006. Serie C. No. 151. Párr. 86. [↑](#footnote-ref-3)
4. Ibídem. Parr. 87. [↑](#footnote-ref-4)
5. Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios. Artículo 9. …

   II. Eficacia: Obligación del Instituto para tutelar, de manera efectiva, el derecho de acceso a la información;

   … [↑](#footnote-ref-5)