

SÍNTESIS CIUDADANA

EXPEDIENTE: INFOCDMX/RR.IP.1486/2021

Sujeto Obligado:

Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México



¿CUÁL FUE LA SOLICITUD?

Acceso al análisis de riesgo y brecha del Documento de Seguridad del Sistema de Datos Personales de Recursos Humanos del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal”



¿POR QUÉ SE INCONFORMÓ?

Porque el Sujeto Obligado no atendió su petición.



¿QUÉ RESOLVIMOS?

El recurso de revisión quedó sin materia, es decir, concluyó de forma anticipada, pues durante la tramitación del mismo, la inconformidad de la persona solicitante quedó sin efectos.



CONSIDERACIONES IMPORTANTES:

En la atención a solicitudes de acceso a la información, los Sujetos Obligados deben realizar una interpretación amplia de su contenido, a fin de favorecer el derecho de acceso a la información de las personas.

LAURA L. ENRÍQUEZ RODRÍGUEZ

GLOSARIO

Constitución Local	Constitución Política de la Ciudad de México
Constitución Federal	Constitución Política de los Estados Unidos Mexicanos
Instituto de Transparencia u Órgano Garante	Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México
Ley de Transparencia	Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México
Recurso de Revisión	Recurso de Revisión en Materia de Acceso a la Información Pública
Sujeto Obligado	Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México
PNT	
INFOMEX	Plataforma Nacional de Transparencia
	Sistema de Solicitudes de Información de la Ciudad de México



RECURSO DE REVISIÓN EN MATERIA DE ACCESO A LA INFORMACIÓN PÚBLICA

EXPEDIENTE:

INFOCDMX/RR.IP.1486/2021

SUJETO OBLIGADO:

Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México

COMISIONADA PONENTE:

LAURA LIZETTE ENRÍQUEZ
RODRÍGUEZ¹

Ciudad de México, a uno de diciembre de dos mil veintiuno

VISTO el estado que guarda el expediente **INFOCDMX/RR.IP.1486/2021**, relativo al recurso de revisión interpuesto en contra del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, por lo que, en sesión pública, este Órgano Garante resuelve **SOBRESEER** en el medio de impugnación, conforme a lo siguiente:

I. ANTECEDENTES

1. Solicitud de Información. El veintiuno de agosto de dos mil veintiuno, mediante solicitud de acceso a la información pública, a la que se asignó el folio 3100000142521, la ahora Parte Recurrente requirió al Instituto de Transparencia,

¹ Colaboró Pedro de los Santos Otero.

Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, lo siguiente:

SOLICITO EL ANALISIS DE BRECHA Y ANALISIS DE RIESGO DE SU SISTEMA DE DATOS PERSONALES DE RECURSOS HUMANOS [Sic]

Asimismo, la entonces persona solicitante señaló “medio electrónico” como modalidad de entrega de la información, a través del sistema de solicitudes de acceso a la información de la PNT y como medio de notificación de la respuesta el sistema INFOMEX.

2. Respuesta. El tres de septiembre de dos mil veintiuno, el Sujeto Obligado notificó la parte entonces solicitante, el oficio MX09.INFODF/6/SE-UT/11.4/1584/SDP/2021, suscrito por el Responsable de la Unidad de Transparencia, mediante el cual respondió la solicitud de información en los siguientes términos:

[...]

A efecto de garantizar el Derecho de Acceso a la Información Pública y en atención a la Solicitud de, registrada a través del “Sistema Electrónico Infomex” con el siguiente número de folio, **310000142521**, en la que se requiere lo siguiente:

[...]

En atención a la Solicitud de Acceso a la Información Pública, dirigida al Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México y con la finalidad de dar cumplimiento a lo solicitado, y con los artículos 1, 2, 3, 7 último párrafo, 8 párrafo uno, 13, 212 y 213 de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México.

Resulta conveniente recordar que las atribuciones de este Instituto son: garantizar a toda persona el derecho humano del ejercicio de Acceso a la Información Pública, así como el Derecho a la Protección de sus Datos Personales (Acceso, Rectificación, Cancelación y Oposición) que detentan los Sujetos Obligados de la Ciudad de México, resolver los medios de impugnación derivados de incumplimiento a las Leyes que rigen la materia, asesorar a los Sujetos Obligados respecto de la creación, modificación y supresión de los Sistemas de Datos Personales, así como coordinar los programas y proyectos de capacitación, para promover la cultura de la transparencia.

Por lo antes expuesto, la Unidad de Transparencia de este Instituto, turno la solicitud de información pública a la, **Dirección Administración y Finanzas**, esto conforme al Artículo 211 de la LTAIPRC y del Reglamento Interior del Instituto, donde se establecen las atribuciones:

Con relación a su cuestionamiento donde “Solicito el Análisis de Brecha y Análisis de Riesgo de su Sistema de Datos Personales de Recursos Humanos”, se informa que de conformidad a artículo 26 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, señala ocho acciones para la seguridad de los datos personales, para los efectos de la presente solicitud son aplicable la cuarta referente a análisis de brecha y la quinta consiste en el análisis de riegos, los mismo son componentes de diseño del Documento de Seguridad.

En ese sentido, todas las acciones relacionadas con las medidas de seguridad se encuentran contenidas en el Documento de Seguridad del Sistema de Datos Personales, como lo es el tratamiento que efectúa esta Unidad Administrativa, garantizando la confidencialidad, calidad, finalidad y consentimiento, lo que en suma permite que los documentos, archivos o expedientes que se contienen en dicho sistema se encuentren debidamente resguardados.

Asimismo, se debe tener en cuenta, como se integra el documento de seguridad, toda vez que lo que se requiere en la presente solicitud, forma parte de los elementos

que permiten garantizar el debido tratamiento de los datos personales de este sistema.

En ese sentido, Ley en la Materia, establece los elementos que debe contener el documento de seguridad siendo los siguiente algunos:

- Análisis de Brecha, lo plantearemos como la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de datos personales, es decir, es la concentración de elementos específicos que pueden existir entre lo deseable y lo actual.
- Análisis de Riesgos, será la identificación de peligros y estimar los riesgos, considerando las amenazas y vulnerabilidad existentes para los datos personales y los recursos involucrados en su tratamiento como puede ser, de manera enunciativa más no limitativa: hardware, software, personal servidoras publicas responsable, entre otros.

Por lo antes citado, y con el propósito de atender su solicitud de información, Solicito el Análisis de Brecha y Análisis de Riesgo de su Sistema de Datos Personales de Recursos Humanos ,se encuentra descritos el Documento de Seguridad con el que se dispone en la Unidad Administrativa, como son: Normatividad aplicable; Finalidad; Unidad Administrativa responsable; Encargados; Usuarios; Origen; Proceso de Obtención de Datos; Destino; Interrelación; Tiempo de Conservación; Cesión de Datos; Nivel de Seguridad; Mecanismos de identificación y autenticación, procesos de notificación, gestión y respuestas ante incidencias y Funciones de Personas Servidoras Publicas que intervenga en el tratamiento de los Sistemas de Datos Personales.

En este contexto, se informa que después de haber realizado una búsqueda exhaustiva en los archivos de la Unidad Administrativa, y con el propósito no condicionar el principio de certeza y si garantizar su derecho de acceso a la información pública y máxima publicidad, adjunto a la presente en **ANEXO 1**, el

Documento de Seguridad del Sistema de Datos Personales, como obra en los archivos de esta Unidad Administrativa de conformidad al artículo 219 de la Ley en la Materia, que a la letra indica:

Artículo 219. *Los sujetos obligados entregarán documentos que se encuentren en sus archivos. La obligación de proporcionar información no comprende el procesamiento de la misma, ni el presentarla conforme al interés particular del solicitante. Sin perjuicio de lo anterior, los sujetos obligados procurarán sistematizar la información.*

Dicho lo anterior, el documento se entrega en “versión pública”, debido a que contiene información de acceso restringido que contienen las medidas de seguridad técnica y organizativa, bajo las disposiciones del artículo 180 de Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México y los artículos 1, 3 fracción XIV, XXXIV, XXII, XXIII, XXIV, XXV, 9, 10, 17 y 24 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

“LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DE LA CIUDAD DE MÉXICO

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

...

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

XXII. Medidas de seguridad: *Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales y los sistemas de datos personales*

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

XXIV. Medidas de seguridad físicas: *Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su*

tratamiento. De manera enunciativa más no limitativa, se consideran las siguientes actividades:

- a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
- b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
- c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad;

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

- a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
- b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
- c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y d) Gestionar las comunicaciones, operaciones y medios de almacena

XXXIV. Tratamiento: *Cualquier operación o conjunto de operaciones efectuadas sobre datos personales o conjunto de datos personales, mediante procedimientos manuales o automatizados relacionadas con la obtención, uso, registro, organización, estructuración, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión o cualquier otra forma de habilitación de acceso, cotejo, interconexión, manejo, aprovechamiento, divulgación, transferencia, supresión, destrucción o disposición de datos personales;*

Artículo 9. *El responsable del tratamiento de Datos Personales deberá observar los principios de:*

1. **Calidad:** *Los datos personales deben ser ciertos, adecuados, pertinentes y proporcionales, no excesivos, en relación con el ámbito y la finalidad para la que fueron recabados.*
2. **Confidencialidad:** *El Responsable garantizará que exclusivamente el titular pueda acceder a sus datos, o en su caso, el mismo Responsable y el usuario a fin de cumplir con las finalidades del tratamiento. En cualquier caso, se deberá garantizar la secrecía y la no difusión de los mismos. Sólo el titular podrá autorizar la difusión de sus datos personales.*
3. **Consentimiento:** *Toda manifestación previa, de voluntad libre, específica, informada e inequívoca por la que el titular acepta, mediante declaración o acción afirmativa, el tratamiento de sus datos personales.*
4. **Finalidad:** *Los datos personales recabados y tratados tendrán fines determinados, explícitos y legítimos y no podrán ser tratados ulteriormente con fines distintos para los que fueron recabados. Los datos personales con fines de archivo de interés público, investigación científica e histórica, o estadísticos no se considerarán incompatibles con la finalidad inicial.*

5. La Finalidad incluirá el ciclo de vida del dato personal, de tal manera, que concluida ésta, los datos puedan ser suprimidos, cancelados o destruidos.
6. **Información:** El Responsable deberá informar al titular de los datos sobre las características principales del tratamiento, la finalidad y cualquier cambio del estado relacionados con sus datos personales.
7. **Lealtad:** El tratamiento de datos personales se realizará sin que medie dolo, engaño o medios fraudulentos, tengan un origen lícito, y no vulneren la confianza del titular.
8. **Licitud.** El tratamiento de datos personales será lícito cuando el titular los entregue, previo consentimiento, o sea en cumplimiento de una atribución u obligación legal aplicable al sujeto obligado; en este caso, los datos personales recabados u obtenidos se tratarán por los medios previstos en el presente ordenamiento, y no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.
9. **Proporcionalidad:** El Responsable tratará sólo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con la finalidad o finalidades, para lo cual se obtuvieron.
10. **Transparencia:** La información relacionada con el tratamiento de datos será accesible y fácil de entender, y siempre a disposición del titular.
11. **Temporalidad:** Los datos personales tendrán un ciclo de vida o una temporalidad vinculada a la finalidad para la cual fueron recabados y tratados. Una vez concluida su finalidad o hayan dejado de ser necesarios, pertinentes o lícitos, pueden ser destruidos, cancelados o suprimidos.

Artículo 10. Todo tratamiento de datos personales que efectúe el responsable deberá sujetarse a los principios, facultades o atribuciones, además de estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera. El responsable podrá tratar datos personales para finalidades distintas a aquéllas que dieron origen al tratamiento, siempre y cuando cuente con atribuciones conferidas en la ley y medie el consentimiento expreso y previo del titular, salvo en aquellos casos donde la persona sea reportada como desaparecida, en los términos previstos en la presente Ley y demás disposiciones que resulten aplicables.

Artículo 17. El responsable deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la calidad de éstos. Los datos personales deberán ser suprimidos, previo bloqueo de ser necesario el caso, una vez que concluya el ciclo de vida de los mismos. El ciclo de vida de los datos personales concluye, cuando los datos han dejado de ser necesarios para el cumplimiento de la finalidad o finalidades previstas y el tratamiento que de ésta se deriva.

La conservación de los datos personales o sistemas de datos personales no deberá exceder el cumplimiento de las finalidades que justificaron su tratamiento, y deberán atender a las disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales, para tratamientos ulteriores, que pueden ser disociación, minimización o supresión, entre otros.

...

Artículo 24. Con independencia del tipo de sistema de datos personales en el que se encuentren los datos o el tipo de tratamiento que se efectúe, el responsable deberá

establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.”

Lo anterior garantiza la confidencialidad e integridad de los contenidos en el Documento de Seguridad del Sistema de Datos Personales de los Recursos Humanos, preservando el pleno ejercicio de los derechos tutelados frente a terceros, previniendo la alteración, pérdida, transmisión y acceso no autorizado, (Derecho ARCO) de conformidad al artículo 3 fracción XI, XXXIV, XXII, XXIII, XXIV, XXV de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, en particular las medidas de seguridad aplicables se detallan a continuación:

a) Medidas de seguridad administrativas y físicas:

- “Mapa de ubicación topográfica de los archivos del Sistema de Datos Personales”; es información con bienes inmuebles geolocalizables, esto lo hace identificable, con la ubicación espacial y física del sistema de archivos, además de formar parte de los aspectos que conforman las medidas de seguridad, en el nivel básico, en términos de los establecido en los artículos 25 fracción I y 28 fracción IV de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México y 52 de los Lineamientos Generales sobre Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.
- “Funciones y Obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales” es información organizacional y funcional, que vulnera las medidas de protección, que permiten la identificación y autenticación de las personas o usuarios autorizados para el tratamiento de los datos personales, además de formar parte de los aspectos que conforman las medidas de seguridad, en el nivel medio,

en términos de lo establecido en los artículos 25 fracción II y 28 fracción II de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México y 52 de los Lineamientos Generales sobre Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

- “Medidas normas procedimientos y criterios enfocados a garantizar el nivel de seguridad alto” es información de esquemas organizacionales concerniente al tratamiento y la tutela del Sistema de Datos Personales, además de formar parte de los aspectos que conforman las medidas de seguridad, en el nivel alto, en términos de lo establecido en los artículos
- 25 fracción III y 28 fracciones V y X de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México y 52
- de los Lineamientos Generales sobre Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.
- “Procedimientos de notificación gestión y respuesta ante incidencias” representa” es información operativa y funcional, que vulnera las medidas de protección, que permiten la identificación y autenticación de las personas o usuarios autorizados para el tratamiento de los datos personales, además de formar parte de los aspectos que conforman las medidas de seguridad, en el nivel básico, en términos de lo establecido en los artículos 25 fracción I y 28 fracciones III y V de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México y 52 de los Lineamientos Generales sobre Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.
- “Procedimientos para la realización de auditorías, en su caso” es información operativa y funcional, que vulnera las medidas de seguridad y protección, que permiten la identificación y autenticación de las personas o usuarios autorizados para el tratamiento de los datos personales, además de formar parte de los aspectos que conforman las medidas de seguridad, en el nivel medio, en términos de lo establecido en

los artículos 25 fracción II y 28 Fracción X de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México y 52 de los Lineamientos Generales sobre Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

- “Número de inventario de los archiveros donde se resguarda” forma parte de información física y espacial, que identifica o hace identificable, la ubicación del resguardo físico, además de formar parte de los aspectos que conforman las medidas de seguridad, en el nivel medio, en términos de lo establecido en los artículos 25 fracción II y 28 fracciones I y X de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México y 52 de los Lineamientos Generales sobre Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.
- b) Medidas de seguridad técnicas:
 - “Procedimiento para la realización de copias de respaldo y recuperación de los datos para los sistemas de datos personales automatizados” representa información concerniente al cifrado, consistente en una de las medidas de seguridad, que implementa algoritmos, claves, contraseñas, así como dispositivos concretos de protección, que garantizan la integridad y confidencialidad de la información, además de formar parte de los aspectos que conforman las medidas de seguridad, en el nivel medio, en términos de lo establecido en los artículos 25 fracción II y 28 fracción IX de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México y 52 de los Lineamientos Generales sobre Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.
 - “Número de inventario de los equipos de cómputo donde se resguarda” constituyen información de bienes muebles físicos, que identifica o hace identificable, la ubicación del equipo de cómputo, además de vulnerar las restricciones preventivas y de riesgos, para acceder a los dominios o los programas autorizados, lo cual vulnera las medidas de seguridad

establecidas en el Sistema de Datos Personales, además de formar parte de los aspectos que conforman las medidas de seguridad, en el nivel medio, en términos de lo establecido en los artículos 25 fracción II y 28 fracciones I y IX de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México y 52 de los Lineamientos Generales sobre Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

Con los elementos contenidos en el listado anterior que constituyen información de identificación y autenticación dentro del documento de seguridad del Sistema de Datos Personales de la Unidad Administrativa, la entrega la versión pública, no vulneraría la seguridad de los datos personales existentes en los registros resguardados en la Unidad Administrativa, salvaguardando la secrecía de los documentos; expedientes; archivos, registros físicos, electrónicos y biométricos.

Asociado a lo anterior, le informo para mayor proveer, que esta información fue previamente clasificada por el Comité de Transparencia, de conformidad con el artículo 171 y 183 fracciones I y IX, de Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México, en la segunda sesión ordinaria, mediante acuerdo ACUERDO 010/SE/CT-16-08-2019 lo cual le da mayor sustento, para mayor precisión se pone a su disposición:

ACUERDO 010/SE/CT-16-08-2019 SE MODIFICA LA CLASIFICACIÓN DE LA INFORMACIÓN RELATIVA A LA SOLICITUD DE INFORMACIÓN CON FOLIO **310000182119**, PROPUESTA POR LA DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS, CONCEDIÉNDOSE EL ACCESO A UNA VERSIÓN PÚBLICA DEL DOCUMENTO DE SEGURIDAD DEL SISTEMA DE DATOS PERSONALES DE LOS RECURSOS HUMANOS DEL INSTITUTO DE ACCESO A LA INFORMACIÓN PÚBLICA DEL DISTRITO FEDERAL.

LA INFORMACIÓN PÚBLICA A LA QUE SE DARÁ ACCESO SERÁ LA SIGUIENTE:

1. NOMBRE DEL SISTEMA
2. NOMBRE DE LAS PERSONAS SERVIDORAS Y EX SERVIDORAS PÚBLICAS
3. FECHA DE ELABORACIÓN
4. FECHA DE ÚLTIMA ACTUALIZACIÓN
5. ELABORÓ
6. APROBÓ
7. GUÍA DE CONTENIDO
8. INTRODUCCIÓN
9. NOMBRE DEL SISTEMA
10. RESPONSABLE DEL SISTEMA
11. ÁMBITO DE APLICACIÓN
12. ÁMBITO ESPACIAL
13. ÁMBITO DE CONTENIDOS
14. NORMATIVIDAD APLICABLE
15. ESTRUCTURA Y DESCRIPCIÓN DEL SISTEMA DE DATOS PERSONALES
16. PROCEDIMIENTO DE LA OBTENCIÓN DE LOS DATOS
17. CESIÓN DE DATOS
18. NIVEL DE SEGURIDAD
19. ESPECIFICACIÓN DETALLADA DE LA CATEGORÍA DE DATOS PERSONALES

AHORA BIEN, SE RESGUARDA LA INFORMACIÓN DE ACCESO RESTRINGIDO EN SU MODALIDAD DE CONFIDENCIAL CONSISTENTE EN:

1. MAPA DE UBICACIÓN TOPOGRÁFICA DE LOS ARCHIVOS DEL SISTEMA DE DATOS PERSONALES DE RECURSOS HUMANOS Y LOS ARCHIVOS DEL SISTEMA DE DATOS PERSONALES

2. FUNCIONES Y OBLIGACIONES DEL PERSONAL QUE INTERVENGA EN EL TRATAMIENTO DE LOS SISTEMAS DE DATOS PERSONALES
3. MEDIDAS NORMAS PROCEDIMIENTOS Y CRITERIOS ENFOCADOS A GARANTIZAR EL NIVEL DE SEGURIDAD ALTO
4. PROCEDIMIENTO PARA LA REALIZACIÓN DE COPIAS DE RESPALDO Y RECUPERACIÓN DE LOS DATOS PARA LOS SISTEMAS DE DATOS PERSONALES AUTOMATIZADOS
5. PROCEDIMIENTOS DE NOTIFICACIÓN GESTIÓN Y RESPUESTA ANTE INCIDENCIAS
6. PROCEDIMIENTOS PARA LA REALIZACIÓN DE AUDITORÍAS, EN SU CASO
7. NÚMERO DE INVENTARIO DE LOS ARCHIVEROS DONDE SE RESGUARDA
8. NÚMERO DE LOCAL
9. NÚMERO DE INVENTARIO DE LOS EQUIPOS DE CÓMPUTO DONDE SE RESGUARDA

De conformidad con el Acuerdo antes transcrito, es que en la presente respuesta se citan la resolución del Comité de Transparencia de este Instituto, en las cuales ya fueron clasificados los datos personales previamente enlistados, con el fin de que los mismos se tengan por clasificados:

Finalmente, que una vez más la Unidad Administrativa se ciñe al “Criterio que deberán de aplicar los Entes Obligados, respecto a la clasificación de información en la modalidad de confidencial.” Acuerdo 1072/SO/03-08/2016 aprobado por el Pleno y publicado en la Gaceta Oficial de la Ciudad de México el 15 de agosto del 2016, con base en el principio de celeridad los datos antes referidos no deben ser clasificados nuevamente por el Comité de Transparencia de este Instituto. Para mayor comprensión se cita a la letra el criterio mencionado:

- *Cuando la información que se brindará en respuesta a una solicitud de acceso a la información pública contenga datos personales, deberá*

procederse conforme a lo establecido en los artículos 89, párrafo quinto; 90, fracciones II, VIII y XII; así como el artículo 173 primer párrafo, de la LTAIPRC, para que, en su caso, el Comité de Transparencia emita el acuerdo mediante el cual se restringirá el acceso a los datos personales existentes por revestir el carácter de confidencial.

- *En caso de datos personales que ya fueron clasificados en los términos antes señalados, y estos mismos se encuentren en información que será entregada derivado de una nueva solicitud, el Área que la detente en coordinación con la Unidad de Transparencia atendiendo a naturaleza de la información, podrán restringir el acceso a dicha información refiriendo los acuerdos con los que el Comité de Transparencia los clasificó como información confidencial así como la fecha de los mismos, incluyendo además, la motivación y fundamentación correspondiente.*
- *En caso de que la información solicitada contenga datos confidenciales distintos a los que previamente el Comité de Transparencia haya clasificado como confidencial, la respuesta a dicha solicitud deberá someterse a consideración del dicho Comité.*

[...] [Sic]

El Sujeto Obligado adjuntó a su respuesta los siguientes documentos:

- a) Oficio MX09.INFODF/6DAF/11.4/0623/2021, suscrito por la Directora de Administración y Finanzas y dirigido al Responsable de la Unidad de Transparencia, cuyo contenido fue transcrito en el oficio MX09.INFODF/6/SE-UT/11.4/1584/SDP/2021 antes citado.
- b) Versión pública del “Documento de Seguridad del Sistema de Datos Personales de Recursos Humanos del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal”.

3. Recurso. El cuatro de octubre de dos mil veintiuno², la Parte Recurrente interpuso recurso de revisión en contra de la respuesta recaída a su solicitud, en el que, medularmente, se agravió de lo siguiente:

² Si bien el recurso de revisión se interpuso el 11 de septiembre de dos mil veintiuno, de conformidad con lo previsto en los Acuerdos 1531/SO/22-09/2021 y 1612/SO/29-09/2021,

[...]

1 La respuesta no atiende a lo requerido, por las siguientes razones:

a) Con respecto al análisis de brecha y de riesgo, menciona acciones que se realizarán y cómo lo harán, pero yo no pregunté eso, yo pedí el análisis de riesgo y de brecha, no sus definiciones, ni posibles acciones que podrían o no llevarse a cabo, sino el documento que contiene el análisis de brecha y de riesgo

b) Proporciona un documento de seguridad con última fecha de actualización de 2015, cuando todavía no era un deber contar con análisis de riesgo y de brecha, lo que quiere decir que el instituto está en total incumplimiento a los deberes que establece la Ley de Protección de Datos Personales, me agravia que me entreguen un documento que no tiene nada que ver con lo que solicité, porque de entrada aún no estaba establecido en la Ley local que se debiera contar con análisis de brecha y de riesgo y que la Dirección de Recursos Humanos, nos de trato como si los ciudadanos fuéramos ignorantes

Dejando, en evidencia con los propios argumentos que da la Dirección de Recursos Humanos el incumplimiento a lo establecido en la Ley en materia de protección de datos personales, por lo que SOLICITAMOS QUE NOS ENTREGUEN EL ANÁLISIS DE BRECHA Y DE RIESGO REQUERIDOS

[...] [Sic]

La Parte Recurrente adjuntó a su recurso de revisión el “Acuse de recibo de solicitud de acceso a la información pública”, expedido a su favor por la PNT y

aprobados por el Pleno del Instituto, así como el artículo 71 de la Ley de Procedimiento Administrativo de la Ciudad de México, de aplicación supletoria en la materia conforme a lo dispuesto por el artículo 10 de la Ley de Transparencia, el medio de impugnación se tuvo por presentado el cuatro de octubre de la misma anualidad.

correspondiente a la solicitud transcrita en el Antecedente 1 de la presente resolución.

4. Admisión. El siete de octubre de dos mil veintiuno³, la Comisionada Ponente admitió a trámite el presente medio de impugnación, con fundamento en el artículo 243, fracción I, de la Ley de Transparencia, otorgó a las partes el plazo de siete días hábiles para que realizaran manifestaciones, ofrezcan pruebas y formulen alegatos.

5. Alegatos. El veinte de octubre de dos mil veintiuno, se recibió el oficio MX09.INFODF/9/SE-UT/11.4/1822/SIP/2021, suscrito por el Responsable de la Unidad de Transparencia del Sujeto Obligado y dirigido a esta Ponencia, por medio del cual rindió los siguientes alegatos:

[...]

Mediante el Sistema Electrónico, recibido por esta Unidad de Transparencia el día 11 de octubre del 2021, me fue notificado el acuerdo mediante el que se admite a trámite el recurso de revisión en materia de Acceso a la Información Pública **INFOCDMX/RR.IP. 1486/2021** en el que se otorga a las partes siete días para hacer manifestaciones, ofrecer pruebas en su caso y formular alegatos, por lo que con fundamento en el artículo 243, fracción III, de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México (**LTAIPRC**) se formulan **manifestaciones y alegatos**, en los siguientes términos:

[...]

Precisados los antecedentes, me permito hacer las siguientes manifestaciones en relación a los argumentos formulados por la recurrente de la siguiente manera:

³ El acuerdo de admisión fue notificado el ocho de octubre a la Parte Recurrente y el once octubre al Sujeto Obligado.

AGRAVIOS

De la lectura integral del escrito recursal, se advierte que la persona inconforme se agravia “Proporciona un documento de seguridad con última fecha de actualización de 2015”.

En descargo de lo manifestado se formulan las siguientes manifestaciones:

PRIMERO. Mediante oficio **MX09.INFODF/6/SE-UT/11.4/1584/SDP/2021**. De fecha 03 de septiembre del año 2021, esta Unidad de Transparencia, notificó a la parte recurrente la respuesta original con la información proporcionada por la Dirección de Administración y Finanzas de este Instituto, poniendo a disposición de la persona recurrente la versión pública del documento solicitado, Fundando y motivando debidamente la razón de la expedición de la Versión pública correspondiente, tal como se desprende de la respuesta original.

SEGUNDO. Cabe destacar que con la respuesta original se puso a su disposición una versión pública con apego a lo establecido en el segundo párrafo del artículo 214 de la LTAIPRC motivo por el que hasta que se realice el pago correspondiente se hará la entrega, con lo que pierde sustento lo expresado en los agravios de la persona recurrente.

Para acreditar lo expuesto con antelación, adjunto a las presentes manifestaciones, las siguientes pruebas:

- **DOCUMENTAL.** Consistente en oficio **MX09.INFODF/6/SE-UT/11.4/1584/SDP/2021**, de fecha 03 de septiembre de 2021, que contiene la respuesta original sustentada en la información de la Dirección de Administración y Finanzas.

- **DOCUMENTAL.** Consistente en oficio **MX09.INFODF.6DAF/2.4/0781/2021**, de la Dirección de Administración y Finanzas en el que se envían los alegatos de la Dirección, con archivo adjunto en formato físico denominado Documento de Seguridad, como parte de las diligencias para mejor proveer.
- **INSTRUMENTAL DE ACTUACIONES** consistente en todas y cada una de las actuaciones que obran en el expediente en todo lo que favorezca a los intereses de este Sujeto Obligado.
- **PRESUNCIONAL EN SU DOBLE ASPECTO, LEGAL Y HUMANA** consistente en los razonamientos que ocupa el Pleno de este Instituto y en todo lo que favorezca los intereses de este Sujeto Obligado.

Por lo anteriormente expuesto y fundado, atentamente pido se sirva:

PRIMERO.- Tenerme por presentado en tiempo y forma en los términos de este recurso, formulando las manifestaciones requeridas mediante acuerdo de 07 de octubre de 2020.

SEGUNDO.- Admitir los medios de prueba ofrecidos y en su oportunidad, resolver lo que conforme a derecho proceda.

TERCERO. Tenerme por cumplido el requerimiento que como diligencias para mejor proveer se contiene en el acuerdo admisorio del recurso de interés.

TERCERO.- Tener por atendida la solicitud de información pública **3100000142521**, de manera íntegra y consecuentemente **CONFIRMAR** la misma en el presente recurso.

[...] [Sic]

A su oficio de alegatos, el Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, adjuntó los siguientes documentos:

- a) Oficio MX09.INFODF/6DAF/2.4/0781/2021, suscrito por la Directora de Administración y Finanzas y dirigido al Responsable de la Unidad de Transparencia, por medio del cual, dicha unidad administrativa rindió sus manifestaciones y alegatos al tenor de lo siguiente:

[...]

Sandra Ariadna Mancebo Padilla, en mi carácter de Directora de Administración y Finanzas del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, en atención y cumplimiento al contenido del proveído de fecha 12 de Octubre del 2021, dictado por usted dentro del recurso de revisión citado al rubro, el cual me fue notificado por medio de oficio: MX09.INFODF/6/SE-UT/11.4/1811/SDP/2021 el día 12 de Octubre del 2021; señalando como medio para recibir notificaciones e información de los acuerdos que se dicten en el presente recurso de revisión la cuenta de correo electrónico: sandra.mancebo@infocdmx.org.mx, con el debido respeto comparezco para rendir en tiempo y forma las siguientes **manifestaciones y alegatos**, con fundamento en el artículo 243, fracción II y III, de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México (LTAIPRC), así como en el numeral décimo séptimo fracción III, inciso a, 1 y 2, del Procedimiento para la Recepción, Sustanciación, Resolución y Seguimiento de los Recursos de Revisión interpuestos en materia de acceso a la información pública y protección de datos personales en la Ciudad de México.

[...]

A G R A V I O S

De la lectura integral al escrito inicial, se advierte que el particular al interponer el medio de impugnación que nos ocupa **describe los hechos en que funda su impugnación de la siguiente manera:**

“Con respecto al análisis de brecha y de riesgo, menciona acciones que se realizaran y como lo harán, pero yo no pregunte eso, yo pedí el análisis de riesgo y de brecha, no sus definiciones, ni posibles acciones que podrían o no llevarse a cabo, si no el documento que contiene el análisis de brecha y riesgo.”

Considerando los agravios señalados por el hoy recurrente, esta Unidad Administrativa, respondió en la solicitud de origen, lo siguiente:

[...]

De lo anterior, se desprende que esta Unidad Administrativa, respondió a cabalidad los requerimientos del hoy recurrente, como se podrá comprobar a continuación:

Primero, es necesario traer presente que antes del 22 de febrero del 2018, la Ley de Protección de Datos Personales del Distrito Federal, establecía diversas medidas de seguridad que constituían los mínimos exigibles para cada Sujeto Obligado con lo cual se cumplía el debido resguardo y la protección de los datos personales por este Sujeto Obligado.

Segundo, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, establece acciones relacionadas con las medidas de seguridad “**distintas**” a las que contenía la Ley de Protección de Datos Personales del Distrito Federal, las cuales no se contienen en el documento de seguridad del Sistema de Datos Personales de Recursos Humanos, como lo son:

1. **Análisis de riesgo** de los datos personales, considerando las amenazas y vulnerabilidades existentes
2. **Análisis de brecha**, en el cual se comparan las medidas de seguridad existentes, contra las faltantes.

*Siendo esto la razón del recurso de revisión que hoy nos ocupa: “con respecto al análisis de brecha y de riesgo menciona acciones que se realizaran y como lo harán pero yo no pregunte eso, **yo pedí el análisis de riesgo y de brecha**, no sus definiciones, ni posibles acciones que podrían o no llevarse a cabo, si no el documento que contiene el análisis de brecha y de riesgo”*

Del citado agravio, se desprende que el hoy recurrente, solicita información que no se encuentra en los documentos que se pusieron a su disposición, toda vez que la Ley de Protección de Datos Personales del Distrito Federal, con la que se creó en su momento el Documento de Seguridad del Sistema de Datos Personales de Recursos Humanos del Instituto, **no contemplaba la obligación de incluir esas dos acciones de seguridad como lo son análisis de riesgo y de brecha**, sin embargo en aras de privilegiar el derecho de acceso a la información, esta Unidad Administrativa, realizó una búsqueda exhaustiva en sus archivos, con la finalidad de localizar la información requerida por el hoy recurrente, de lo cual se entregó la información que obraba en nuestros archivos, de conformidad con el artículo 219 de la Ley natural, misma que indica que los sujetos obligados entregarán los documentos que se encuentren en sus archivos, sin la obligación de proporcionar información realizando el procesamiento de la misma, **ni el presentarla conforme al interés particular**, por ello, esta Unidad Administrativa actuó conforme a los principios de certeza, imparcialidad, legalidad, máxima publicidad, objetividad, profesionalismo y transparencia, entregando la totalidad de la información, atendiendo en todo momento lo establecido en la Ley de la materia.

Por lo que esta Unidad Administrativa fue exhaustiva, fundando y motivando su respuesta, dando certeza al particular, de conformidad con lo previsto en las fracciones VIII y X, del artículo 6, de la Ley de Procedimiento Administrativo del Distrito Federal, ordenamiento de aplicación supletoria a la Ley de la materia, mismo que indica lo siguiente:

LEY DE PROCEDIMIENTO ADMINISTRATIVO DE LA CIUDAD DE MÉXICO

Calle de La Morena No. 865, Local 1, “Plaza de la Transparencia”, Col. Narvarte Poniente,
Alcaldía Benito Juárez, Ciudad de México.

Teléfono: 56 36 21 20

TITULO SEGUNDO
DE LOS ACTOS ADMINISTRATIVOS
CAPITULO PRIMERO
DE LOS ELEMENTOS Y REQUISITOS DE VALIDEZ DEL ACTO
ADMINISTRATIVO

Artículo 6º.- Se considerarán válidos los actos administrativos que reúnan los siguientes elementos:

...

VIII. Estar fundado y motivado, es decir, citar con precisión el o los preceptos legales aplicables, así como las circunstancias especiales, razones particulares o causas inmediatas que se hayan tenido en consideración para la emisión del acto, debiendo existir una adecuación entre los motivos aducidos y las normas aplicadas al caso y constar en el propio acto administrativo;

...”

X. Expedirse de manera congruente con lo solicitado y resolver expresamente todos los puntos propuestos por los interesados o previstos por las normas.

...

De acuerdo con la fracción VIII del precepto legal aludido, para que un acto sea considerado válido, éste debe estar debidamente fundado y motivado, citando con precisión el o los artículos aplicables al caso en concreto, así como las circunstancias especiales, razones particulares o causas inmediatas que se hayan tenido en consideración para la emisión del acto, debiendo existir congruencia entre los motivos aducidos y las normas aplicadas; sirve de apoyo a lo anterior, la titulada Jurisprudencia emitida por el Poder Judicial de la Federación, FUNDAMENTACIÓN Y MOTIVACIÓN.

Asimismo, de conformidad con la fracción X, todo acto administrativo debe apegarse a los principios de **congruencia y exhaustividad**, entendiendo por lo primero la concordancia que debe existir entre el pedimento formulado y la

respuesta, y por lo segundo el que se pronuncie expresamente sobre cada uno de los puntos pedidos, lo que en materia de transparencia y acceso a la información pública se traduce en que las respuestas que emitan los Sujetos Obligados deben guardar una relación lógica con lo solicitado y atender de manera precisa, expresa y categórica cada uno de los contenidos de información requeridos por el particular, a fin de satisfacer la solicitud correspondiente, situación realizada en todo momento en la respuesta emitida por esta Unidad Administrativa.

En el mismo sentido, se ha pronunciado el Poder Judicial de la Federación en la Jurisprudencia 1a./J.33/2005, cuyo rubro es CONGRUENCIA Y EXHAUSTIVIDAD EN SENTENCIAS DICTADAS EN AMPARO CONTRA LEYES. ALCANCE DE ESTOS PRINCIPIOS

Por lo tanto, es claro que el agravio planteado por la parte recurrente **no es fundado**, toda vez que la respuesta se atiende de forma exhaustiva, ya que se entregó la información requerida; por lo anteriormente expuesto y fundado, es claramente improcedente la interposición de dicho recurso, puesto que la Dirección de

Administración y Finanzas respondió a cabalidad la totalidad del cuestionamiento con la información disponible y adicionalmente para garantizar el derecho de acceso a la información, formulo las acciones y definiciones concernientes al análisis de brecha y riesgo.

Conjuntamente, es necesario precisar una vez más, que la Dirección de Administración y Finanzas, remitió las documentales obrantes en su poder, por lo que dichas manifestaciones se encuentran investidas con el principio de **buena fe**, previsto en los artículos 5 y 32, párrafo segundo, de la Ley de Procedimiento Administrativo del Distrito Federal, ordenamiento de aplicación supletoria a la Ley de la materia.

Finalmente, reitero que esta Unidad Administrativa actuó en los términos establecidos en la Ley de Transparencia, entregando la información que por motivo de nuestras atribuciones detentamos, los cuales revisten de plena autenticidad, validez y certeza respecto de la información enviada, ya que se sobre entiende que es la información con la que contamos en nuestros archivos y nos encontramos obligados a entregar, cuidando en todo momento la realización de algún acto que pudiera transgredir el derecho de acceso a la información pública, consagrado en nuestra Carta Magna.

A efecto de acreditar lo expuesto con antelación, remito adjunto a las presentes manifestaciones, se ofrecen las siguientes pruebas:

- **LA INSTRUMENTAL DE ACTUACIONES** consistente en todas y cada una de las actuaciones que obran en el expediente en mención y en todo lo que favorezca a los intereses de este Sujeto Obligado.
- **LA PRESUNCIÓN EN SU DOBLE ASPECTO LEGAL Y HUMANA** consistente en los razonamientos que ocupa el Pleno de este Instituto y en todo lo que favorezca los intereses de este Ente Obligado.
- **COPIA SIMPLE DE:**
Respuesta a solicitud **3100000142521**

Por lo expuesto y fundado, atentamente pido se sirva:

PRIMERO. - Tenerme por presentada en tiempo y forma en los términos del presente curso, rindiendo el Informe de Ley requerido mediante oficio MX09.INFODF/6/SE-UT/11.4/1811/SDP/2021 dejando sin efectos el percibimiento dictado al suscrito dentro del mismo.

SEGUNDO. - Dar por atendida la solicitud de información **3100000142521**, para que de esta manera deje sin materia el presente recurso de revisión RR.IP. 1486/2021 y se dé sobreseimiento al mismo.

TERCERO. -Admitir los medios de prueba ofrecidos y en su oportunidad, resolver lo que conforme a derecho proceda, de conformidad a lo previsto por el artículo 249 fracción II de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México (LTAIPRC).
[...][Sic]

- b) Oficio MX09.INFODF/6/SE-UT/11.4/1584/SDP/2021, suscrito por el Responsable de la Unidad de Transparencia y transcrito en el Antecedente 2 de la presente resolución.

6. Alcance de Alegatos. El cuatro de noviembre de dos mil veintiuno, mediante oficio MX09.INFODF/6/SE-UT/11.4/1964/SIP/2021, la Unidad de Transparencia notificó a la Parte Recurrente notificó a la Parte Recurrente, en el medio señalado por éste para oír y recibir notificaciones, un alcance de alegatos, al tenor de lo siguiente:

[...]

A efecto de garantizar el Derecho de Acceso a la Información Pública y en atención a la Solicitud, registrada a través de la Plataforma Nacional de Transparencia con el siguiente número de folio 3100000142521, en la que se requiere lo siguiente:

“SOLICITO EL ANALISIS DE BRECHA Y ANALISIS DE RIESGO DE SU SISTEMA DE DATOS PERSONALES DE RECURSOS HUMANOS.” sic

Mediante la presente respuesta complementaria, adjunto al presente oficio, encontrará el ACTA DE LA CUARTA SESIÓN EXTRAORDINARIA DEL COMITÉ DE TRANSPARENCIA DEL INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA, PROTECCIÓN DE DATOS PERSONALES Y RENDICIÓN DE CUENTAS DE LA CIUDAD DE MÉXICO celebrada el día 16 de agosto de 2019.

[...] [Sic]

El Sujeto obligado adjuntó copia del Acta de la Cuarta Sesión Extraordinaria del Comité de Transparencia del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, celebrada el dieciséis de agosto de dos mil diecinueve, por medio de la cual se aprobó el Acuerdo 010/SE/CT-16-08-2019 a través del cual se confirmó la propuesta de clasificación como reservada, por un periodo de tres años, así como la elaboración de la versión pública del documento de seguridad, materia del presente medio de impugnación.

7. Alcance de Alegatos. El diecinueve de noviembre de dos mil veintiuno, el Sujeto Obligado remitió a la Parte Recurrente un alcance de alegatos, a través del cual le entregó los siguientes documentos:

- Oficio MX09.INFODF.6ADF/11.4/0846/2021, suscrito por la Directora de Administración y Finanzas y dirigido al Secretario Técnico del Sujeto Obligado y Presidente del Comité de Transparencia por medio del cual informó sobre la remisión de la propuesta de clasificación de la información solicitada.

- Oficio MX09.INFODF.6ADF/11.4/0845/2021, suscrito por la Directora de Administración y Finanzas y dirigido al Responsable de la Unidad de Transparencia del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, el cual contiene la propuesta de clasificación del Documento de Seguridad del Sistema de Datos Personales de Recursos Humanos, materia del presente medio de impugnación.
- Oficio MX09.INFODF.6ADF/11.4/0844/2021, suscrito por la Directora de Administración y Finanzas y dirigido al Comité de Transparencia, por medio del cual realizó la prueba de daño relativa a la clasificación de la información requerida.
- Acta de la Sexta Sesión Extraordinaria del Comité de Transparencia, celebrada el dieciséis de noviembre de dos mil veintiuno, por medio de la cual, se aprobó del Acuerdo 009/SE/CT-16-11-2021, se aprobó la clasificación, como reservada, de la información requerida, por un plazo de 1 año.

8. Cierre. El diecinueve de noviembre de dos mil veintiuno, con fundamento en el artículo 252, en correlación con el artículo 243, fracción V, ambos de la Ley de Transparencia, se decretó el cierre de instrucción y se tuvo por presentado al Sujeto Obligado formulando manifestaciones y alegatos.

Asimismo, no pasa desapercibido que la parte recurrente no presentó manifestaciones ni alegatos en el plazo antes mencionado, por lo que con fundamento en lo dispuesto por el artículo 133 del Código de Procedimientos

Civiles para el Distrito Federal de aplicación supletoria a la Ley de Transparencia, se declara precluido su derecho para tal efecto.

9. Hecho superveniente. El treinta de noviembre de dos mil veintiuno la Unidad de Transparencia del Sujeto Obligado notificó a la Parte Recurrente el oficio MX09,INFODF/6DAF/11.4/0915/2021, el cual contiene una respuesta complementaria a su solicitud de información, emitida por la Directora de Administración y Finanzas, por medio de la cual le puso a disposición la versión pública de los análisis de riesgo y brecha del Sistema de Datos Personales de Recursos Humanos, debido que dicha información fue clasificada como reservada, de conformidad con los artículos 169, 170, 171, 183, fracción I, y 216 de la Ley de Transparencia, a través del ACUERDO 010/SE/CT-29-11-2021.

A dicha comunicación electrónica, el Sujeto Obligado adjuntó la siguiente documentación:

- Versión pública de los análisis de riesgos y brecha requeridos por el entonces solicitada.
- Oficio MX09.INFODF/6ADF/11.4/0913-1/2021, suscrito por la Directora de Administración y Finanzas y dirigido al Comité de Transparencia, por medio del cual el Sujeto Obligado solicitó la aprobación de la clasificación del análisis de riesgo y brecha peticionado y emitió su prueba de daño.

10. Alcance al hecho superveniente. El treinta de noviembre de dos mil veintiuno, la Unidad de Transparencia del Sujeto Obligado notificó a la Parte Recurrente el Acta de la Séptima Sesión Extraordinaria de su Comité de

Transparencia, por medio de la cual se aprobó el Acuerdo 010/SE/CT-29-11-2021, a través del que se confirmó la clasificación del “Análisis de Brecha” y “Análisis de Riesgo” correspondiente al Sistema de Datos Personales de Recursos Humano, materia de la solicitud de mérito, en su carácter de reservada, de conformidad con lo dispuesto en el artículo 183, fracción I, de la Ley de Transparencia.

A dicha comunicación electrónica, el Sujeto Obligado, de nueva cuenta, remitió a la Parte Recurrente las documentales precisadas en el Antecedente inmediato anterior.

Finalmente, es menester señalar que las documentales contenidas en el expediente del medio de impugnación que ahora se resuelve, se tienen por desahogadas en virtud de su propia y especial naturaleza, y se les otorga valor probatorio pleno con fundamento en lo dispuesto en los artículos 374, 402 y 403 del Código de Procedimientos Civiles para el Distrito Federal, de aplicación supletoria a la Ley de la materia.

En virtud de que ha sido debidamente substanciado el presente expediente, y

II. CONSIDERANDO

PRIMERO. Competencia. El Instituto es competente para investigar, conocer y resolver el presente recurso de revisión con fundamento en lo establecido en los artículos 6, párrafos primero, segundo y apartado A de la Constitución Federal; 1, 2, 37, 51, 52, 53 fracciones XXI, XXII, 214 párrafo tercero, 220, 233, 236, 237,

238, 242, 243, 244, 245, 246, 247, 252 y 253 de la Ley de Transparencia; así como los artículos 2, 3, 4 fracciones I y XVIII, 12 fracciones I y IV, 13 fracciones IX y X, y 14 fracciones III, IV, V y VII de su Reglamento Interior.

Asimismo, este Instituto también es competente para conocer el presente medio de impugnación, a pesar de la Contingencia ocasionada por COVID-19, en términos de los puntos PRIMERO y SEGUNDO, de conformidad con el **“ACUERDO POR EL QUE SE APRUEBA EL CALENDARIO DE REGRESO ESCALONADO, RESPECTO DE LOS PLAZOS Y TÉRMINOS DE LAS SOLICITUDES DE ACCESO A LA INFORMACIÓN PÚBLICA Y DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN DE DATOS PERSONALES, DERIVADO DEL CAMBIO DE COLOR DEL SEMÁFORO EPIDEMIOLÓGICO EN LA CAPITAL DEL PAÍS A VERDE POR LA CONTINGENCIA SANITARIA ORIGINADA POR EL COVID-19**, identificado con la clave alfanumérica 0827/SO/09-06/2021, los cuales dan cuenta de la aprobación del calendario de reanudación gradual de plazos y términos para dar atención a las solicitudes de acceso a la información pública, acceso, rectificación, cancelación y oposición de datos personales presentadas ante los Sujetos Obligados, mismas que se reanudarán a partir del veintiocho de junio del dos mil veintiuno.

De igual manera resulta aplicable el **ACUERDO POR EL QUE SE SUSPENDEN PLAZOS Y TÉRMINOS PARA LOS EFECTOS DE LOS ACTOS Y PROCEDIMIENTOS QUE SE INDICAN DEL INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA, PROTECCIÓN DE DATOS PERSONALES Y RENDICIÓN DE CUENTAS DE LA CIUDAD DE MÉXICO, DERIVADO DEL SISMO DEL SIETE DE SEPTIEMBRE DE DOS MIL**

VEINTIUNO, identificado con la clave alfa numérica ACUERDO 1409/SO/08-09/2021, se determinó suspender plazos y términos el ocho de septiembre de dos mil veintiuno.

A su vez, también se considera lo previsto por el **ACUERDO MEDIANTE EL CUAL EL INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA, PROTECCIÓN DE DATOS PERSONALES Y RENDICIÓN DE CUENTAS DE LA CIUDAD DE MÉXICO SUSPENDE PLAZOS Y TÉRMINOS PARA LOS DÍAS, EFECTOS Y PROCEDIMIENTOS QUE SE INDICAN**, identificado con la clave alfa numérica ACUERDO 1531/SO/22-09/2021, por medio del cual se aprobó suspender plazos y términos los días trece, catorce, quince, diecisiete, veinte, veintiuno, veintidós, veintitrés y veinticuatro de septiembre de dos mil veintiuno, respecto de las solicitudes de acceso a la información pública y de datos personales, presentadas ante los Sujetos Obligados de la Ciudad de México, así como los recursos de revisión, en dichas materias, que son competencia de este Órgano Garante.

Finalmente, se contempla lo estipulado en el **SEGUNDO ACUERDO MEDIANTE EL CUAL EL INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA, PROTECCIÓN DE DATOS PERSONALES Y RENDICIÓN DE CUENTAS DE LA CIUDAD DE MÉXICO SUSPENDE PLAZOS Y TÉRMINOS PARA LOS DÍAS, EFECTOS Y PROCEDIMIENTOS QUE SE INDICAN**, identificado con la clave alfa numérica ACUERDO 1612/SO/29-09/2021, en virtud del cual se determinó la suspensión de plazos y términos durante los días veintisiete, veintiocho, veintinueve y treinta de septiembre, así como el primero de octubre, ambos de dos mil veintiuno, únicamente en relación

con los recursos de revisión en las materias de acceso a la información pública y de datos personales que estén pendientes de registrar y turnar a las Comisionadas y Comisionados Ciudadanos que son competencia de este Instituto de Transparencia.

SEGUNDO. Procedencia. El medio de impugnación interpuesto resultó admisible porque cumplió con los requisitos previstos en los artículos 234, 236 y 237 de la Ley de Transparencia, como se expone a continuación:

a) Forma. De las constancias que integran el expediente en que se actúa, se advierte que la Parte Recurrente hizo constar: su nombre; Sujeto Obligado ante quien presentó la solicitud materia del presente recurso; medio para recibir notificaciones; los hechos en que se fundó la impugnación y los agravios que le causó el acto; mientras que tanto en el sistema INFOMEX como en la PNT, se advirtieron tanto la respuesta impugnada como las constancias relativas a su tramitación.

b) Oportunidad. La presentación del recurso de revisión es oportuna, pues de las constancias del expediente se advierte que **la respuesta recurrida fue notificada al particular el tres de septiembre, mientras que** por virtud de previsto en los Acuerdos 1531/SO/22-09/2021 y 1612/SO/29-09/2021, aprobados por el Pleno del Instituto, se tuvo por interpuesto **el recurso de revisión de la Parte Recurrente, el cuatro de octubre, ambas fechas de dos mil veintiuno.**

En ese sentido, **el plazo de quince días hábiles de la Parte Recurrente para interponer su recurso de revisión comenzó a computarse a partir del seis**

de setiembre y feneció el quince de octubre, ambos de octubre de dos mil veintiuno⁴; por lo que resulta evidente que el medio de impugnación se interpuso en tiempo.

TERCERO. Causales de Improcedencia. Previo al estudio de fondo de los agravios formulados por la Parte Recurrente, este Instituto realizará el análisis oficioso de las causales de improcedencia del recurso de revisión, por tratarse de una cuestión de orden público y estudio preferente, atento a lo establecido en la jurisprudencia VI.2o. J/323, publicada en la página 87, de la Octava Época del Semanario Judicial de la Federación y su Gaceta, con registro digital 210784, de rubro y texto siguientes:

***IMPROCEDENCIA.** Sea que las partes la aleguen o no, debe examinarse previamente la procedencia del juicio de amparo, por ser una cuestión de orden público en el juicio de garantías.*

En tal virtud, del análisis de las constancias que integran el expediente, este Órgano Garante advierte que **el recurso de revisión ha quedado sin materia**, por lo que es procedente sobreseer el recurso de revisión, con fundamento en lo dispuesto por el artículo 249, fracción II de la Ley de Transparencia, que a la letra dice:

Artículo 249. El recurso será sobreseído cuando se actualicen alguno de los siguientes supuestos:

⁴ Al plazo referido fueron descontados por inhábiles los días comprendidos entre el once y el treinta de setiembre así como el uno, dos y tres de octubre, todos dos mil veintiuno, de conformidad con lo establecido por el artículo 71 de la Ley de Procedimiento Administrativo de la Ciudad de México, de aplicación supletoria en la materia, conforme a lo dispuesto por el artículo 10 de la Ley de Transparencia, así como lo previsto por los Acuerdos 1531/SO/22-09/2021 y 1612/SO/29-09/2021, aprobados por el Pleno del Instituto.

[...]

II. Cuando por cualquier motivo quede sin materia el recurso.

[...]

Señalado lo anterior, previo a exponer los motivos por los que el medio de impugnación ha quedado sin materia, es importante traer a colación las partes medulares de la solicitud, respuesta, recurso de revisión, alegatos y respuesta complementaria.

a) Cuestión previa

En primer lugar, por lo que respecta a la solicitud de información de la ahora Parte Recurrente y la respuesta del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, es menester destacar:

Solicitud	Respuesta
Acceso al análisis de brecha y riesgo del sistema de datos personales de recursos humanos.	La Dirección de Administración y Finanzas señaló que de conformidad con la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, entre las acciones para garantizar la seguridad de los datos personales se encuentran los análisis de brecha y riegos, mismos que son componentes

	de diseño del “Documento de Seguridad”.
	Todas las acciones relacionadas con las medidas de seguridad se encuentran contenidas en el “Documento de Seguridad”.
	Indicó los elementos que deben contener los “Documento de Seguridad”, enfatizando en el análisis de riesgo y brecha y sus características.
	Después de haber realizado una búsqueda exhaustiva en los archivos de la Dirección de Administración y Finanzas, a fin de no condicionar el principio de certeza y si garantizar su derecho de acceso a la información pública y máxima publicidad, puso a disposición de la Parte Recurrente el “Documento de Seguridad del Sistema de Datos Personales de Recursos Humanos del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal”.
	La citada documental se entrega como obra en los archivos de esta Unidad

	<p>Administrativa de conformidad al artículo 219 de la Ley de Transparencia.</p>
	<p>El documento en comento se entrega en “versión pública”, debido a que contiene información de acceso restringido que contienen las medidas de seguridad técnica y organizativa del referido sistema de datos personales, lo que garantiza la confidencialidad e integridad de sus contenidos; en particular las medidas de seguridad aplicables.</p>
	<p>La entrega la versión publica, no vulneraría la seguridad de los datos personales existentes en los registros resguardados en la Unidad Administrativa, salvaguardando la secrecía de los documentos; expedientes; archivos, registros físicos, electrónicos y biométricos.</p>
	<p>La información puesta a disposición, fue previamente clasificada por el Comité de Transparencia, de conformidad con el artículo 171 y 183 fracciones I y IX, de Ley de</p>

	Transparencia, mediante Acuerdo 010/SE/CT-16-08-2019.
--	---

Con base en lo anterior, la Parte Recurrente interpuso antes este Órgano Garante recurso de revisión y una vez admitido a trámite, el Sujeto Obligado rindió alegatos, de cuyos actos procedimentales es menester destacar lo siguiente:

Recurso de Revisión	Alegatos
La respuesta no atiende lo requerido ya que con respecto al análisis de brecha y de riesgo, el Sujeto Obligado únicamente menciona acciones relacionadas con su implementación.	La Dirección de Administración y Finanzas manifestó que, en su momento, la Ley de Protección de Datos Personales del Distrito Federal, establecía diversas medidas de seguridad a fin de cumplir con el debido resguardo y la protección de los datos personales por dicho Sujeto Obligado, algunas distintas a Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.
El Sujeto Obligado le proporcionó un documento de seguridad con fecha última fecha de actualización de dos mil quince, en el que no constituía un deber, contar con análisis de riesgo y de brecha.	Si bien la otrora Ley de Protección de Datos Personales del Distrito Federal, con la que se creó en su momento el “Documento de Seguridad del Sistema de Datos Personales de Recursos Humanos del Sujeto Obligado”, no

	<p>contemplaba la obligación de incluir el análisis de riesgo y de brecha, en aras de privilegiar el derecho de acceso a la información, se entregó la información que obraba en nuestros archivos, de conformidad con el artículo 219 de la Ley de Transparencia, es decir, sin la obligación de proporcionar información realizando el procesamiento de la misma, ni el presentarla conforme al interés de la parte solicitante.</p>
	<p>Dicha Unidad Administrativa fue exhaustiva, fundando y motivando su respuesta, así como dando certeza al particular, de conformidad con lo previsto en las fracciones VIII y X, del artículo 6, de la Ley de Procedimiento Administrativo de la Ciudad de México, de aplicación supletoria a la Ley de la materia y apegándose a los principios de congruencia y exhaustividad.</p>
	<p>La Unidad Administrativa competente, remitió las documentales que obran en</p>

	<p>su poder, por lo que dichas manifestaciones se encuentran investidas con el principio de buena fe, previsto en los artículos 5 y 32, párrafo segundo, de la Ley de Procedimiento Administrativo de la Ciudad de México, ordenamiento de aplicación supletoria a la Ley de la materia.</p>
--	--

A su vez, el Sujeto Obligado emitió dos alcances de alegatos, de los cuales se desprende medularmente lo siguiente:

Primer Alcance de Alegatos	Segundo Alcance de Alegatos
<p>El Sujeto Obligado notificó y remitió a la Parte Recurrente –en la cuenta de correo electrónico señalada para oír y recibir notificaciones en el presente medio de impugnación– el Acta de la Cuarta Sesión Extraordinaria de su Comité de Transparencia, celebrada el dieciséis de agosto de dos mil diecinueve, por medio de la cual se aprobó el Acuerdo 010/SE/CT-16-08-2019, a través del cual se confirmó la propuesta de clasificación como reservada, por un periodo de tres</p>	<p>El Sujeto Obligado notificó y remitió a la Parte Recurrente –en la cuenta de correo electrónico señalada para oír y recibir notificaciones en el presente medio de impugnación– el Acta de la Sexta Sesión Extraordinaria del Comité de Transparencia, celebrada el dieciséis de noviembre de dos mil veintiuno, por medio de la cual, a través del a través del Acuerdo 009/SE/CT-16-11-2021, se aprobó la clasificación, como reservada, del</p>

<p>años, así como la elaboración de la versión pública del documento de seguridad, materia del presente medio de impugnación.</p>	<p>documento de seguridad requerido, por un plazo de 1 año.</p>
	<p>Adicionalmente, en aras de garantizar la máxima transparencia, el Sujeto Obligado notificó y remitió a la Parte Recurrente –en la cuenta de correo electrónico señalada para oír y recibir notificaciones en el presente medio de impugnación–, entre otros, los siguientes documentos:</p> <ul style="list-style-type: none"> • Propuesta de clasificación del Documento de Seguridad del Sistema de Datos Personales de Recursos Humanos, materia del presente medio de impugnación. • Prueba de daño relativa a la clasificación de la información requerida.

Finalmente, es importante señalar que durante la tramitación del presente medio de impugnación, el Sujeto Obligado emitió una serie de actos, orientados a atender la solicitud de información de la persona solicitante, al tenor de lo siguiente:

Hecho superveniente	Hecho superveniente
<p>La Directora de Administración y Finanzas puso a disposición la versión pública de los análisis de riesgo y brecha del Sistema de Datos Personales de Recursos Humanos, debido que dicha información fue clasificada como reservada, de conformidad con los artículos 169, 170, 171, 183, fracción I, y 216 de la Ley de Transparencia.</p>	<p>El Sujeto Obligado remitió, en alcance, Acta de la Séptima Sesión Extraordinaria de su Comité de Transparencia, por medio de la cual se aprobó el Acuerdo 010/SE/CT-29-11-2021, a través del que se confirmó la clasificación del “Análisis de Brecha” y “Análisis de Riesgo” correspondiente al Sistema de Datos Personales de Recursos Humano, materia de la solicitud de mérito, en su carácter de reservada, de conformidad con lo dispuesto en el artículo 183, fracción I, de la Ley de Transparencia.</p>
<p>La clasificación de la información mencionada se aprobó mediante ACUERDO 010/SE/CT-29-11-2021.</p>	

Precisado lo anterior, este Órgano Garante considera que los últimos actos y gestiones efectuadas por el Sujeto Obligado, a saber la puesta a disposición de versión pública de los análisis de riesgo y brecha del Sistema de Datos Personales de Recursos Humanos, así como la entrega del Acta del Comité por

la cual se clasificó la información requerida, en su carácter de reservada, serán valorados en la presente resolución, en su carácter de hechos supervenientes.

Sirve de sustento a lo anterior, la tesis XXII.9 K, publicada en la página 449, de la Novena Época del Semanario Judicial de la Federación y su Gaceta, con registro digital 202746, de rubro y texto siguientes:

PRUEBAS EN LA REVISION, LA RECEPCION Y SU VALORACION NO CONTRAVIENE EL ARTICULO 78 DE LA LEY DE AMPARO, CUANDO TIENDE A DEMOSTRAR UN HECHO SUPERVENIENTE.

La prohibición contenida en el artículo 78 de la Ley de Amparo, en cuanto a que en las sentencias que se dicten en los juicios de amparo, el acto reclamado se apreciará tal como aparezca probado ante la autoridad responsable, y que no se admitirán ni se tomarán en consideración las pruebas que no se hubiesen rendido ante dicha autoridad para comprobar los hechos que motivaron o fueron objeto de la resolución reclamada, **no tiene el alcance de impedir la recepción y en su caso la valoración de una documental, que es la base de los agravios aducidos**, mediante la cual se demuestra que la autoridad responsable rindió oportunamente su informe justificado, habida cuenta de que tal probanza, por su misma naturaleza, está encaminada a demostrar lo erróneo de los motivos que sustentan la presunción de existencia del acto reclamado, mas no a sostener la legalidad del mismo, que es la prohibición a que se refiere el invocado precepto legal.

Adicionalmente, es necesario traer a colación lo señalado en la tesis 1a. CCVII/2018 (10a.), publicada en el Libro 61, Tomo I, página 378, de la Décima Época del Semanario Judicial de la Federación y su Gaceta, con registro digital 2018781, de rubro y texto siguientes:

PRINCIPIO PRO PERSONA. SÓLO PUEDE UTILIZARSE EN SU VERTIENTE DE CRITERIO DE SELECCIÓN DE INTERPRETACIONES CUANDO ÉSTAS RESULTAN PLAUSIBLES.

De acuerdo con lo previsto en el artículo 1o., segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, las normas de derechos humanos se interpretarán y aplicarán "favoreciendo en todo tiempo a las personas la protección más amplia", ello implica que el principio pro persona opera como un criterio que rige la selección entre: (i) dos o más normas de derechos humanos que, siendo aplicables, tengan contenidos que sea imposible armonizar y que, por tanto, exijan una elección; o (ii) dos o más posibles interpretaciones admisibles de una norma, de modo que se acoja aquella que adopte el contenido más amplio o la limitación menos restrictiva del derecho. Así, es importante que tanto las normas entre las que se elige como las interpretaciones que se pretendan comparar sean aplicables en el primer caso y plausibles en el segundo, por ser el resultado de técnicas válidas de interpretación normativa. Ahora bien, la Primera Sala de la Suprema Corte de Justicia de la Nación en las jurisprudencias 1a./J. 104/2013 (10a.) y 1a./J. 10/2014 (10a.), sostuvo que el principio pro persona no puede entenderse como una exigencia para que se resuelva de conformidad con las pretensiones de la parte que lo invoque, ni como un permiso para soslayar el cumplimiento a los requisitos de admisibilidad o procedencia de recursos y medios de impugnación, aunque sí exige que su interpretación se realice en los términos más favorables a las personas. Lo anterior, refleja que **el principio pro persona debe beneficiar a quienes participen dentro de un procedimiento jurisdiccional, ya que opera como criterio para determinar el fundamento, alcances, regulación y límites de los derechos humanos de cada una**, según se encuentren en juego en un asunto, mientras que su falta de utilización puede ser reclamada en juicio por el efecto potencialmente perjudicial que podría tener para la tutela de un derecho humano.

De la lectura armónica de los criterios jurisprudenciales referidos, es posible colegir que no es impedimento para los órganos resolutores, la recepción y en su

caso la valoración de documentales que constituyen la base de los agravios aducidos, cuando éstas son tendientes a desvirtuar los motivos que sustentan la presunción de existencia del acto reclamado a través de un hecho superveniente.

Aunado a lo anterior, no es óbice mencionar que **este Órgano Garante está constreñido a cumplir con el principio “pro persona”**, privilegiando la interpretación más amplia de las normas relativas a los derechos humanos y favoreciendo en todo tiempo a las personas la protección más amplia, también está conminado a beneficiar a las personas que participen dentro de los procedimientos materia de este Instituto de Transparencia, **pues dicho principio opera como criterio para determinar el fundamento, alcances, regulación y límites de los derechos humanos de cada una de las Partes.**

Por otra parte, no pasa inadvertido para este Instituto de Transparencia que, entre sus agravios, la Parte Recurrente señaló que el Sujeto Obligado ***le proporcionó un documento de seguridad con fecha última fecha de actualización de dos mil quince, en el que no constituía un deber, contar con análisis de riesgo y de brecha.***

Al respecto es menester mencionar que dicho pronunciamiento no guarda relación con la petición primigenia del entonces solicitante, por lo que este Instituto de Transparencia considera que, respecto de dicho agravio, la Parte Recurrente realizó una ampliación a su solicitud de información, por lo que, en el presente caso, se actualiza la causal de improcedencia prevista en la fracción VI del artículo 248 de la Ley de Transparencia que dispone:

Artículo 248. El recurso será desechado por improcedente cuando:

[...]

VI. El recurrente amplíe su solicitud en el recurso de revisión, únicamente respecto de los nuevos contenidos.

En tal virtud, dado que a través del citado agravio, la Parte Recurrente amplió su solicitud de información mediante la incorporación de elementos novedosos, no será procedente entrar a su estudio de fondo.

Acotado lo anterior, se tiene que el único agravio subsistente de la Parte Recurrente es el relativo a que **la respuesta del Sujeto Obligado no atendió su petición, respecto al análisis de brecha y de riesgo** del “Documento de Seguridad del Sistema de Datos Personales de Recursos Humanos del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal”, **pues el Sujeto Obligado únicamente mencionó acciones relacionadas con su implementación.**

a) Estudio de la respuesta complementaria

Previo a verter los argumentos por los cuales se considera que la respuesta complementaria, y su respectivo alcance, ha dejado sin materia el presente recurso de revisión, es necesario realizar algunas precisiones sobre la atención brindada por el Sujeto Obligado a la solicitud de información que nos ocupa.

En primer lugar este Órgano Garante estima que **en el caso concreto se actualizó la hipótesis prevista en el Criterio 16/17 Expresión documental,**

sostenido por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, que a la letra dice:

Expresión documental. Cuando los particulares presenten solicitudes de acceso a la información sin identificar de forma precisa la documentación que pudiera contener la información de su interés, o bien, la solicitud constituya una consulta, pero la respuesta pudiera obrar en algún documento en poder de los sujetos obligados, éstos deben dar a dichas solicitudes una interpretación que les otorgue una expresión documental.

De Criterio del Órgano Garante Nacional se desprende que cuando **las personas solicitantes no identifiquen, en forma precisa, la documentación que pudiera contener la información de su interés, deberán otorgar una expresión documental.**

En tal virtud, de las constancias que integran la respuesta primigenia, se advierte que el Sujeto Obligado realizó diversas precisiones, entre las cuales destacan:

- a) Que entre las acciones para garantizar la seguridad de los datos personales se encuentran los análisis de brecha y riegos, mismos que son componentes de diseño del denominado “Documento de Seguridad”.
- b) Que todas las acciones relacionadas con las medidas de seguridad se encuentran contenidas en el “Documento de Seguridad”.
- c) Que indicó los elementos que deben contener los “Documento de Seguridad”, enfatizando en el análisis de riesgo y brecha y sus características.

Por tanto, de las precisiones formuladas por el Sujeto Obligado y relativas al documento de seguridad, sus elementos y las características de los análisis de riesgo y brecha, así como del agravio de la Parte Recurrente, por el cual señaló que la autoridad recurrida esgrimió las acciones relacionadas con la implementación de los análisis de brecha y de riesgo, este Órgano Garante colige que **la Dirección de Administración y Finanzas del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México emitió una expresión documental concerniente a lo peticionado.**

Adicionalmente, si bien es cierto que la Parte Recurrente no identificó en forma precisa el documento que pudiera contener la información de su interés, en aras de privilegiar una interpretación amplia de su solicitud de información, la citada Dirección de Administración y Finanzas le indicó que la información relativa a los análisis de riesgo y brecha, de acuerdo a la normatividad aplicable, se encuentran contenidos en los denominados “documentos de seguridad”.

Lo anterior, en virtud de que **las personas solicitantes no tienen la obligación de ser peritos en la materia, por lo que las autoridades requeridas, al atender una solicitud de información, deben hacer una interpretación amplia respecto de su contenido y no limitarse a la literalidad de las expresiones que se emplean en la misma.**

En esa tesitura, en aras de garantizar el derecho de acceso a la información de la ahora Parte Recurrente y en cumplimiento a lo dispuesto en el artículo 219 de la Ley de Transparencia que conmina a los Sujetos Obligados a los Sujetos

Obligados a entregar los documentos que se encuentren en sus archivos, la Dirección de Administración y Finanzas del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, puso a disposición de la Parte Recurrente, el “Documento de Seguridad del Sistema de Datos Personales de Recursos Humanos del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal”, en la modalidad elegida, tal como obra en sus archivos y a través de la versión pública aprobada por su Comité de Transparencia.

Acotado lo anterior, por lo que concierne al primer alcance de alegatos emitido por el Sujeto Obligado y descrito en el Antecedente 6 de la presente resolución, se advirtió que el Sujeto Obligado puso a disposición de la Parte Recurrente, en la dirección de correo electrónico señalada como medio de para oír y recibir notificaciones, el Acta de la Cuarta Sesión Extraordinaria del Comité de Transparencia del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, celebrada el dieciséis de agosto de dos mil diecinueve, por medio de la cual se aprobó el Acuerdo 010/SE/CT-16-08-2019, informado a la persona solicitante en su respuesta primigenia.

Al respecto, es menester precisar que este Órgano Garante procedió a revisar el contenido del citado Acuerdo 010/SE/CT-16-08-2019 y fue posible advertir que el Comité de Transparencia:

- a) Se emitieron las pruebas de daño correspondientes.

- b) Confirmó la clasificación como reservada, del “Documento de Seguridad del Sistema de Datos Personales de Recursos Humanos del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal”.
- c) Aprobó la versión pública del citado documento.
- d) El documento referido se clasificó en su carácter de reservado, por un periodo de tres años, a partir de la fecha de emisión del citado acuerdo, por lo que a la fecha de la presente resolución, la clasificación de referencia aún se encuentra vigente.

Posteriormente, en su segundo alcance de alegatos, tal como se indicó en el Antecedente 7 de la presente resolución, el Sujeto Obligado puso a disposición de la Parte Recurrente, en la dirección de correo electrónico señalada como medio de para oír y recibir notificaciones, el Acta de la Sexta Sesión Extraordinaria del Comité de Transparencia, celebrada el dieciséis de noviembre de dos mil veintiuno, a través de la cual se aprobó del Acuerdo 009/SE/CT-16-11-2021, del que se desprende lo siguiente:

- Emitió la respectiva prueba de daño.
- Confirmó la clasificación como reservada, del multicitado documento de seguridad.
- Avaló la versión pública que se generó del citado documento.
- Aprobó la clasificación, como reservada, de la información requerida, por un plazo de 1 año.

Acotado lo anterior, es menester señalar que de las constancias que obran en el expediente de mérito, se advirtió que el Sujeto Obligado realizó dos gestiones finales, por medio de las cuales, en aras del principio de máxima publicidad informó a la Parte Recurrente, informó y puso a su disposición –en el medio señalado para tal efecto– la versión pública de los análisis de riesgo y brecha del Sistema de Datos Personales de Recursos Humanos, así como el Acta de la Séptima Sesión Extraordinaria de su Comité de Transparencia, por medio de la cual se aprobó el Acuerdo 010/SE/CT-29-11-2021, a través del que se confirmó la clasificación de la información referida, en su carácter de reservada, de conformidad con el artículo 183, fracción I de la Ley de Transparencia, celebrada el veintinueve de noviembre de dos mil veintiuno.

En ese sentido, con la finalidad de verificar la idoneidad de la clasificación de la información en comento, este Instituto de Transparencia procedió a revisar el Acta de la Séptima Sesión Extraordinaria de su Comité de Transparencia, antes referida, a través de la cual se advirtió que el Sujeto Obligado:

- Emitió la respectiva prueba de daño.
- Confirmó la clasificación como reservada, de los análisis de riesgo y brecha requeridos.
- Aprobó la clasificación, como reservada, de la información en comento, por un plazo de año.

Por otra parte, este Órgano Garante también procedió a verificar las razones emitidas, a manera de justificación, por las que el Sujeto Obligado, en su

respectiva prueba de daño, sustentó la clasificación de la información, en las que destacan:

- Las medidas de seguridad son el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten proteger los datos personales y los sistemas de datos personales.
- Las medidas de seguridad permiten proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico donde se encuentren los datos personales, pudiendo adoptarse también, medidas para un mantenimiento eficaz que asegure la confidencialidad, disponibilidad e integridad de la información, entre la que se encuentran datos personales.
- El objeto de las medidas necesarias para prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados, pues el responsable está obligado a garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.
- Entre otras cuestiones, las medidas de seguridad referidas pueden guardar relación con:
 - El registro de incidencias; la identificación y autenticación; el control de acceso; la gestión de soportes y copias de respaldo y recuperación, así como el registro de acceso y telecomunicaciones; información que se considera debe ser protegida.
 - Las funciones y obligaciones de las personas que intervengan en el tratamiento datos personales; responsable de seguridad; los mecanismos de monitoreo y revisión de las medidas de seguridad.

Acotado lo anterior, es menester traer a colación lo señalado por el artículo 26, fracciones IV y V de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, que a la letra dicen:

Artículo 26. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:

[...]

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;

[...]

Por su parte, los artículos 46 y 47 Lineamientos Generales de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, disponen:

[...]

Análisis de riesgos

Artículo 46. Para dar cumplimiento al artículo 26, fracción IV de la Ley, el Responsable deberá realizar un análisis de riesgos de los datos personales tratados considerando lo siguiente:

I. Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;

II. El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida;

- III. El valor y exposición de los activos involucrados en el tratamiento de los datos personales;
- IV. Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida , y
- V. Los factores previstos en el artículo 25 de la Ley.

Análisis de la brecha

Artículo 47. Para el debido cumplimiento de la obligación establecida en el artículo 26, fracción V de la Ley, en la realización del análisis de brecha el Responsable deberá considerar lo siguiente:

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

[...]

De los preceptos legales, en primer lugar, se destaca que, lo siguiente:

- Con la finalidad de establecer y mantener la seguridad de los datos personales en su posesión, los Sujetos Obligado deben implementar diversas medidas de seguridad.
- Entre las medidas de seguridad que deben implementar los Sujetos Obligado, se encuentran los análisis de riesgo y brecha constituyen medidas de seguridad.

Como corolario, es menester señalar que al implementar un **análisis de riesgos** –respecto de los datos personales objeto de tratamiento–, los Sujetos Obligados deberán considerar lo siguiente:

- ✓ Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico.
- ✓ El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida.
- ✓ El valor y exposición de los activos involucrados en el tratamiento de los datos personales.
- ✓ Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida.
- ✓ Diversos factores tales como:
 - El riesgo inherente a los datos personales tratados.
 - La sensibilidad de los datos personales tratados.
 - El desarrollo tecnológico.
 - Las posibles consecuencias de una vulneración para los titulares.
 - Las transferencias de datos personales que se realicen.
 - El número de titulares.
 - Las vulneraciones previas ocurridas en los sistemas de datos.
 - 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.

Por su parte, para la implementación del **análisis de brecha** los Sujetos Obligados deberán considerar lo siguiente:

- ✓ Las medidas de seguridad existentes y efectivas;
- ✓ Las medidas de seguridad faltantes, y

- ✓ La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.

Precisado lo anterior, a fin de contar con mayores elementos para resolver en el presente medio de impugnación, este Órgano Garante procedió a revisar la el documento denominado “Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales”⁵, elaborado por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Entre otras cuestiones, la citada guía establece que un **“activo”** es **“cualquier valor que requiera ser protegido”** y entre éstos, se encuentra aquéllos que están relacionados con el ciclo de vida de los datos personales.

Asimismo, el documento referido señala que los activos deben identificarse y ponderar con suficiente nivel de detalle para proveer información que permita hacer la valoración de riesgos. Se pueden identificar dos tipos de activos:

1. Activos de información, corresponden a la esencia de la organización:
 - Información relativa a los datos personales o Información de procesos del negocio en los que interviene el flujo de datos personales y actividades involucradas en el tratamiento de los mismos.
2. Activos de apoyo, en los cuales residen los activos de información, como son:

⁵ Disponible para su consulta en: [http://inicio.inai.org.mx/DocumentosdeInteres/Guía_Implementación_SGSDP\(Junio2015\).pdf](http://inicio.inai.org.mx/DocumentosdeInteres/Guía_Implementación_SGSDP(Junio2015).pdf)

- Hardware o Software o Redes y Telecomunicaciones o Personal o Estructura organizacional o Infraestructura adicional.

Una vez identificados y descritos los activos de información y de apoyo, se podrán encontrar sus vulnerabilidades y posibles amenazas.

Por otra parte, de la citada guía se desprende que una “**amenaza**” tiene el potencial de dañar un activo y causar una vulneración a la seguridad organizacional de los Sujetos Obligado; asimismo, las amenazas pueden ser:

- De origen natural o humano.
- Accidentales o deliberadas.
- Provenir del interior o del exterior de la organización del Sujeto Obligado.
- Las amenazas deben ser identificadas considerando que algunas pueden afectar a más de un activo al mismo tiempo.

A su vez, el documento en comento define las “**vulnerabilidades**” como “**debilidades en la seguridad de los activos**”, las cuales pueden ser identificadas en los siguientes ámbitos:

- Organizacionales.
- De procesos y procedimientos.
- De personal.
- Del ambiente físico.
- De la configuración de sistemas de información.

- Del hardware, software o equipo de comunicación.
- De la relación con prestadores de servicios.
- De la relación con terceros.

Al respecto, es menester señalar que **la presencia de vulnerabilidades no causa daño por sí misma, sino que se requiere de una amenaza que la explote** y no obstante que dicha vulnerabilidad no se encuentre expuesta a una amenaza identificada, ésta debe ser reconocida y monitoreada constantemente, o bien, cuando surja algún cambio.

En ese tenor, a manera general es posible señalar que los análisis de riesgo permitirán a los Sujetos Obligados, obtener valores del riesgo para cada uno de los activos identificados con respecto a cada una de las vulneraciones mencionadas con antelación, así como identificar los escenarios que podrían llevar a cada uno de los activos de su organización, incluidos los datos personales, a sufrir una posible vulneración; lo que, a su vez, permitirá, mediante los análisis de brecha, a identificar los controles y medidas, necesarios o faltantes, que permitan mitigar o minimizar los citados riesgos, en ambos casos, privilegiando la realización de una ponderación de escenarios en los que **el riesgo es la combinación de los factores: amenaza, vulnerabilidad e impacto.**

Una vez esgrimidos los argumentos por los cuales se pudo conocer la naturaleza, importancia, objeto y alcance de la implementación de medidas de seguridad, específicamente lo concerniente a los análisis de riesgo y brecha, es necesario recordar que el Sujeto Obligado, respecto los análisis de riesgo y brecha del

sistema de datos personales de recursos humanos, requeridos por la ahora Parte Recurrente, el Sujeto Obligado procedió a su clasificación, en su carácter de reservados, de conformidad con lo dispuesto en el artículo 183, fracción I, de la Ley de Transparencia que a la letra dice:

Artículo 183. Como información reservada podrá clasificarse aquella cuya publicación:

I. Pueda poner en riesgo la vida, seguridad o salud de una persona física;

[...]

Del precepto legal en cita se desprende que constituye información reservada aquella cuyo contenido pueda poner en riesgo la vida, seguridad o salud de una persona física.

Al respecto, es menester mencionar que, en el marco de la normatividad en materia de protección de datos personales, **el principal objeto de la implementación de las medidas de seguridad, incluidos los análisis de riesgo y brecha, es garantizar una adecuada protección de los datos personales contra daño, pérdida, alteración, destrucción, así como uso, acceso o tratamiento no autorizado, salvaguardando, en consecuencia, su confidencialidad, integridad y disponibilidad.**

Por lo tanto, dada la naturaleza del contenido de los análisis de riesgo y brecha del sistema de datos personales de recursos humanos requeridos, este Órgano Garante estima que la entrega de lo solicitado:

- Representa un riesgo real, demostrable e identificable, que podría causar daños y perjuicios significativo a los titulares de los datos personales que obran en el aludido sistema de datos personales.
- El riesgo de los daños y perjuicios que supondría la divulgación supera el interés público general.

En mérito de lo expuesto, la clasificación invocada por el Sujeto Obligado se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar la comisión de daños y/o perjuicios en contra de los titulares de los datos personales relacionados con el sistema de datos personales de recursos humanos.

No menos importante es que conceder el acceso los análisis de riesgo y brecha del sistema de datos personales de recursos humanos supondría permitir a una persona ajena a la organización del Sujeto Obligado, acceder no solo a los datos personales almacenados en el referido sistema, sino brindar información relacionada con activos de información tales como registros de incidencias de seguridad, datos de identificación y autenticación, controles de acceso, gestión de soportes, registros de acceso, telecomunicaciones, mecanismos de monitoreo y revisión de las medidas de seguridad, así como información inherente a las funciones y obligaciones de las personas que intervienen en el tratamiento datos personales como responsables de seguridad.

En ese tenor, derivado de la naturaleza y el grado de especificidad del tipo de información que contiene el **análisis de riesgo y brecha del documento de seguridad**, es que se colige que dar a conocer el mismo facilitaría que personas

expertas en informática perturben las medidas de seguridad de los datos personales que posee el Sujeto Obligado; por lo tanto, resulta procedente su reserva, de conformidad con el precepto jurídico en comento.

Finalmente, es importante señalar que el último párrafo del artículo 178 de la Ley de Transparencia establece que **la clasificación de información reservada se realizará conforme a un análisis caso por caso**, mediante la aplicación de la prueba de daño.

En ese sentido, no es óbice mencionar que la información requerida fue clasificada, en su carácter de reservada, a través del Comité de Transparencia del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, a través del Acuerdo 010/SE/CT-29-11-2021, aprobado mediante la Séptima Sesión Extraordinaria de su Comité de Transparencia de su Comité de Transparencia, cumpliendo así con el procedimiento de clasificación previsto en la Ley de Transparencia.

Con base en lo anterior, se estima que **el Sujeto Obligado dio cumplimiento al artículo 178 de la Ley de Transparencia, pues cumplió con el procedimiento de clasificación previsto en la ley de la materia y realizó un análisis, caso por caso**, de la clasificación de la información requerida, en su modalidad de reservada, emitiendo la prueba de daño correspondiente.

Una vez acotado lo anterior, este Instituto de Transparencia considera que resulta aplicable al caso concreto, el Criterio 07/21, que a la letra dice:

Requisitos para que sea válida una respuesta complementaria. Las manifestaciones y alegatos no son el medio idóneo para mejorar o complementar la respuesta que originalmente un sujeto obligado otorgó a una solicitud de información. **Para que los alegatos, manifestaciones o un escrito dirigido al particular puedan considerarse como una respuesta complementaria válida se requiere** de lo siguiente:

1. Que la ampliación de la respuesta sea notificada al solicitante **en la modalidad de entrega elegida.**
2. Que el Sujeto Obligado **remita la constancia de notificación** a este Órgano Garante para que obre en el expediente del recurso.
3. **La información proporcionada en el alcance** a la respuesta primigenia **colme todos los extremos de la solicitud.**

Lo anterior, ya que no basta con que el Sujeto Obligado haga del conocimiento del Órgano Garante que emitió una respuesta complementaria la cual satisfaga la integridad de la solicitud de información, sino que **debe acreditar que previamente la hizo del conocimiento del particular a través de los medios elegidos para recibir notificaciones.**

Si la respuesta complementaria no cumple con dicho requisito deberá ser desestimada. Previo análisis del contenido de la respuesta.

Por otro lado, **si la respuesta complementaria cumple con dicho requisito se pudiera sobreseer si del análisis al contenido de los documentos se advierte que atienden la totalidad de la solicitud.**

Del Criterio 07/21, se desprende medularmente que las respuestas complementarias pueden los recursos de revisión presentados ante este Órgano Garante, siempre y cuando los Sujetos Obligados colmen los siguientes extremos:

- a) Que la información remitida en respuesta complementaria se ponga a disposición de las personas recurrentes **en la modalidad de entrega elegida.**
- b) Que la información proporcionada en respuesta complementaria **colme todos los extremos de la solicitud de información.**
- c) Que se acredite que se hizo del conocimiento la Parte Recurrente, **a través del medio elegido para recibir notificaciones**, mediante la respectiva constancia de notificación.

En tal virtud, del análisis de las constancias que integran el expediente en que se actúa, fue posible advertir que, durante la tramitación del presente medio de impugnación concurrieron las siguientes circunstancias:

- a) **El Sujeto Obligado puso a disposición de la Parte Recurrente la versión pública de los análisis de riesgo y brecha del Sistema de Datos Personales de Recursos Humanos requerido, así como el Acta de la Séptima Sesión Extraordinaria de su Comité de Transparencia, por medio de la cual se aprobó el Acuerdo 010/SE/CT-29-11-2021, a través del que se confirmó la clasificación de la información referida, en su carácter de reservada; lo anterior por “medio electrónico”,**

siendo ésta la modalidad de entrega elegida por la entonces persona solicitante.

- b) La versión pública de los análisis de riesgo y brecha del Sistema de Datos Personales de Recursos Humanos requerido, el Acta de la Séptima Sesión Extraordinaria de su Comité de Transparencia y el Acuerdo 010/SE/CT-29-11-2021 –en correlación con la respuesta primigenia del Sujeto Obligado, en la que emitió una expresión documental de lo peticionado–, con lo cual es posible colmar los extremos de las pretensiones de la Parte Recurrente, así como cumplir con el procedimiento de atención de solicitudes información previsto en la Ley de Transparencia.
- c) El Sujeto Obligado acreditó haber notificado y puesto a disposición de la Parte Recurrente la información antes referida, a través de la dirección de correo electrónico señalada por la Parte Recurrente, como medio para oír y recibir notificaciones en su recurso de revisión.

Por lo antes expuesto, este Órgano Garante concluye que en el presente caso, se actualizó la hipótesis prevista en el artículo 249, fracción II, de la Ley de Transparencia, dejando insubsistente el agravio de la Parte Recurrente, **por lo que resulta procedente SOBRESEER el presente medio de impugnación**, de conformidad con lo estipulado por el artículo 244, fracción II, y 249, fracción II, de la Ley de Transparencia, **al haber quedado sin materia**.

En virtud de lo expuesto, el Pleno de este Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas



de la Ciudad de México,

RESUELVE

PRIMERO. En términos del Considerando Tercero de esta resolución, se **SOBRESEE** en el recurso de revisión, con fundamento en los artículos 244, fracción II y 249, fracción II de la Ley de Transparencia.

SEGUNDO. En cumplimiento a lo dispuesto por el artículo 254 de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México, se informa a la Parte Recurrente que, en caso de estar inconforme con la presente resolución, podrá impugnarla ante el Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales o ante el Poder Judicial de la Federación, sin poder agotar simultáneamente ambas vías.

NOTIFÍQUESE la presente resolución, a la Parte Recurrente, en el medio señalado para tal efecto, y por oficio al Sujeto Obligado.



Así lo resolvieron, los Comisionados Ciudadanos del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México: Julio César Bonilla Gutiérrez, Laura Lizette Enríquez Rodríguez, Arístides Rodrigo Guerrero García, María del Carmen Nava Polina y Marina Alicia San Martín Reboloso, ante Hugo Erik Zertuche Guerrero, Secretario Técnico, de conformidad con lo dispuesto en el artículo 15, fracción IX del Reglamento Interior de este Instituto, en Sesión Ordinaria celebrada el uno de diciembre de dos mil veintiuno, quienes firman para todos los efectos legales a que haya lugar.

MSD/PSO

**JULIO CÉSAR BONILLA GUTIÉRREZ
COMISIONADO CIUDADANO PRESIDENTE**

**LAURA LIZETTE ENRÍQUEZ RODRÍGUEZ
COMISIONADA CIUDADANA**

**ARÍSTIDES RODRIGO GUERRERO GARCÍA
COMISIONADO CIUDADANO**

**MARÍA DEL CARMEN NAVA POLINA
COMISIONADA CIUDADANA**

**MARINA ALICIA SAN MARTÍN REBOLLOSO
COMISIONADA CIUDADANA**

**HUGO ERIK ZERTUCHE GUERRERO
SECRETARIO TÉCNICO**