SÍNTESIS CIUDADANA

EXPEDIENTE: INFOCDMX/RR.IP.6311/2022

Sujeto Obligado:

Secretaría de Administración y Finanzas

¿CUÁL FUE LA SOLICITUD?

Solicito las versiones públicas de los documentos de seguridad de los sistemas de datos personales de las Secretarias del Gobierno de la Ciudad de México, y que sean digitales ya que no tiene razón de ser que los pongan a consulta directa.

¿POR QUÉ SE INCONFORMÓ?

El Particular interpuso su recurso de debido a que el Sujeto obligado no otorgó las versiones públicas de lo peticionado.

¿QUÉ RESOLVIMOS?

REVOCAR la respuesta de la Secretaría de Administración y Finanzas y requerirle que entregue las versiones públicas de los documentos de seguridad con los que cuenta previa aprobación del Comité de Transparencia.
Todo lo anterior, debiéndose notificar a la persona recurrente, a través del medio de notificación que este haya señalado para oír y recibir notificaciones en el presente medio de impugnación.

CONSIDERACIONES IMPORTANTES:

En la atención a solicitudes de acceso a la información, los Sujetos Obligados deben cumplir a cabalidad con el procedimiento de atención de solicitudes.

Palabras clave: Versión pública, Documentos de seguridad, Sistemas de Datos personales, Revocar.

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	Secretaría de Administración y Finanzas
PNT	Plataforma Nacional de Transparencia

RECURSO DE REVISIÓN EN MATERIA DE ACCESO A LA INFORMACIÓN PÚBLICA

EXPEDIENTE:
INFOCDMX/RR.IP.6311/2022

SUJETO OBLIGADO:
Secretaría de Administración y Finanzas

COMISIONADA PONENTE:
Laura Lizette Enríquez Rodríguez[1]

Ciudad de México, a once de enero de dos mil veintitrés

VISTO el estado que guarda el expediente **INFOCDMX/RR.IP.6311/2022**, relativo al recurso de revisión interpuesto en contra de la Secretaría de Administración y Finanzas, este Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, en sesión pública resuelve **REVOCAR** en el medio de impugnación, conforme a lo siguiente:

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

1. Solicitud de Información. El cinco de noviembre de dos mil veintidós, recibida oficialmente el siete de noviembre de dos mil veintidós, recibido de manera oficial el siete de noviembre, mediante solicitud de acceso a la información pública, a la que se asignó el folio **090162822004066,** la ahora Parte Recurrente requirió a la Secretaría de Administración y Finanzas, lo siguiente:

[…]

[1] Colaboró Laura Ingrid Escalera Zúñiga.

> Solicito las versiones públicas de los documentos de seguridad de los sistemas de datos personales de las Secretarias del Gobierno de la Ciudad de México, y que sean digitales ya que no tiene razón de ser que los pongan a consulta directa.
> […][Sic]
>
> **Medio para recibir notificaciones**
> Sistema de solicitudes de la Plataforma Nacional de Transparencia
>
> **Formato para recibir la información solicitada**
> Copia simple

2. Respuesta. El dieciséis de noviembre de dos mil veintidós a través de la PNT, el Sujeto Obligado emitió respuesta mediante oficio sin número, de la misma fecha, signado por la Secretaría de Administración y Finanzas, donde se dio respuesta a la solicitud de información, en los siguientes términos:

> […]
> En lo referente a los "…documentos de seguridad de los sistemas de datos personales…", se le informa que cada uno de los sistemas debe de tener su propio documento de seguridad, el cual es un instrumento generado para **proteger y salvaguardar los sistemas de datos personales que este sujeto obligado detenta**. Dicho registro contiene las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales, pues se trata de un sistema de gestión, al cual tiene acceso el responsable, los usuarios y en su caso, los encargados de los sistemas de datos personales. Es decir, se trata de un documento interno para control, resguardo y verificación de cumplimiento por parte de cada responsable de cada sistema de datos personales.
>
> Para mayor referencia, se enuncian los significados de documento de seguridad y medidas de seguridad, establecidos en el artículo 3, fracciones XIV, XXII, XXIII, XXIV y XXV de la 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 almacenamiento de los recursos informáticos en el tratamiento de datos personales;"

Por lo que, al tratarse de un documento que contiene las medidas de seguridad que implementa este sujeto obligado a favor del resguardo, protección, salvaguarda y evitar la vulneración de datos personales en nuestra posesión, es importante informar a usted las obligaciones que la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México establece en su artículo 23, respecto a los deberes del Responsable, entendido este como "cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, Órganos Autónomos, Partidos Políticos, Fideicomisos y Fondos Públicos, que decida y determine finalidad, fines, medios, medidas de seguridad y demás cuestiones relacionadas con el tratamiento de datos personales" (Artículo 3, fracción XXVIII):

"Artículo 23. El responsable para cumplir con el tratamiento lícito, transparente y responsable de los datos personales, tendrá al menos los siguientes deberes:
Destinar recursos autorizados para la instrumentación de programas y políticas de protección de datos personales;

Elaborar políticas y programas de protección de datos personales, obligatorios y exigibles al interior del sujeto obligado;
Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales;
Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran;
Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales;
Garantizar a las personas, el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición
Diseñar, desarrollar e implementar políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la presente Ley y las demás que resulten aplicables en la materia;
Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan con la protección de datos personales y las obligaciones previstas en la presente Ley y las demás que resulten aplicables en la materia;
Cumplir con las políticas y lineamientos, así como las normas y principios aplicables para el tratamiento lícito y la protección de los datos personales;
Adoptar las medidas de seguridad necesarias para la protección de datos personales y los sistemas de datos personales, así como comunicarlas al Instituto para su registro, en los términos de la presente Ley;
Elaborar y presentar al Instituto un Informe correspondiente sobre las obligaciones previstas en la presente Ley, a más tardar en la segunda semana del mes de enero de cada año. La omisión de dicho informe será motivo de responsabilidad;
Informar al titular previo a recabar sus datos personales, la existencia y finalidad de los sistemas de datos personales;
Registrar ante el Instituto los Sistemas de Datos Personales, así como la modificación o supresión de los mismos;
Establecer los criterios específicos sobre el manejo, mantenimiento, seguridad y protección de los sistemas de datos personales; y
Coordinar y supervisar la adopción de medidas de seguridad a que se encuentren sometidos los sistemas de datos personales."

Por lo anterior, y en apego estricto a la normatividad en materia de protección de datos personales, debemos proteger las medidas de seguridad implementadas al interior del sujeto obligado, para salvaguardar los datos personales a los que tenemos acceso, en el ejercicio de nuestras funciones, con fundamento en el artículo 24 de la ley en la materia, que a la letra señala:

"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.

Es importante comunicarle que las medidas de seguridad deben considerar los posibles riesgos, el nivel de seguridad, 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, entre otras. Es decir, el documento de seguridad de los sistemas de datos personales contempla las medidas que cada responsable debe establecer, adoptar y vigilar en el acceso a los datos personales recabados. Para mayor referencia, se expresa lo descrito en el artículo 25 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México:

"Artículo 25. Las medidas de seguridad adoptadas por el responsable deberán considerar:
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; y
El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.
Estas medidas tendrán al menos los siguientes niveles de seguridad:
Básico: relativas a las medidas generales de seguridad cuya aplicación será obligatoria para el tratamiento y protección de todos los sistemas de datos personales en posesión de los sujetos obligados.
Medio: se refiere a las medidas de seguridad requeridas para aquellos sistemas de datos relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, datos patrimoniales, así como los sistemas que contengan datos con los que se permita obtener evaluación de personalidad o perfiles de cualquier tipo en el presente pasado o futuro.
Alto: corresponde a las medidas de seguridad aplicables a sistemas de datos concernientes a ideología, religión,
creencias, afiliación política, origen racial o étnico, salud, biométricos, genéticos o vida sexual, así como los que contengan datos recabados para fines policiales, de seguridad, prevención, investigación y persecución de delitos.
Las medidas de seguridad que adopten los sujetos obligados para mayores garantías en la protección y resguardo de los sistemas de datos personales, únicamente se comunicarán al Instituto, para su registro, el nivel de seguridad aplicable."

Debido a lo anterior, las medidas de seguridad de los sistemas de datos personales de esta dependencia, únicamente podrán comunicarse al Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (INFO), por lo que no constituye un documento de

acceso a información pública, al tratarse de un instrumento para proteger e impedir la vulneración de datos personales en posesión de este sujeto obligado.

Robustece lo anterior, lo establecido en la normatividad aplicable en materia de protección de datos personales, la cual constituye las acciones a realizar por parte del sujeto obligado, con el propósito de proteger, resguardar e imposibilitar la vulneración o mal uso de los datos personales bajo resguardo de cada unidad administrativa que tiene sistemas de datos personales bajo su responsabilidad. A continuación, se informa de dichas acciones asentadas en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México y en los Lineamientos Generales 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 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:
Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;
Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;
Elaborar un inventario de datos personales contenidos en los sistemas de datos;
Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;
Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;
Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales; y
Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

Artículo 27. Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión denominado documento de seguridad.

Artículo 28. El responsable deberá elaborar el documento de seguridad que contendrá, al menos, lo siguiente:

El inventario de datos personales en los sistemas de datos;
Las funciones y obligaciones de las personas que intervengan en el tratamiento datos personales, usuarios y
encargados, en el caso de que los hubiera;
Registro de incidencias;
Identificación y autentificación;
Control de acceso; gestión de soportes y copias de respaldo y recuperación;
El análisis de riesgos;
El análisis de brecha;
Responsable de seguridad;
Registro de acceso y telecomunicaciones;
Los mecanismos de monitoreo y revisión de las medidas de seguridad;
El plan de trabajo; y
El programa general de capacitación.

Lineamientos Generales de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México:

"Artículo 41. El Responsable deberá establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales en su posesión de conformidad con lo previsto en los artículos 24, 25, 26 y 27 de la Ley, con el objetivo de impedir, que cualquier tratamiento de los datos personales contravenga las disposiciones de dicho ordenamiento y los presentes Lineamientos.

Las medidas de seguridad a las que se refiere el párrafo anterior constituyen los mínimos exigibles, por lo que el Responsable podrá adoptar las medidas adicionales que estime necesarias para brindar mayores garantías en la protección de los datos personales en su posesión.
Lo anterior, sin perjuicio de lo establecido por aquellas disposiciones vigentes en materia de seguridad de la información emitidas por otras autoridades, cuando estas contemplen una mayor protección para el titular o complementen lo dispuesto en la Ley y en los presentes Lineamientos.
Artículo 52. El Responsable elaborará, difundirá e implementará las normas internas de seguridad de la información mediante el documento de seguridad que será de observancia obligatoria para todos los servidores públicos del sujeto obligado, así como para toda aquella persona que en su carácter de encargado, conforme al
artículo 3, fracción XV de la Ley, tenga acceso a los sistemas de datos personales y/o al sitio donde se ubican los mismos, para ello, el Responsable deberá tomar en cuenta lo dispuesto en la Ley y en los presentes Lineamientos.
El documento de seguridad deberá contener, como mínimo, lo siguiente:
El inventario de datos personales en los sistemas de datos;
Las funciones y obligaciones de las personas que intervengan en el tratamiento de datos personales, usuarios y encargados, en el caso de que los hubiera;
Registro de incidencias;
Identificación y autentificación;
Control de acceso; gestión de soportes y copias de respaldo y recuperación;
El análisis de riesgos;

El análisis de brecha;
Responsable de seguridad;
Registro de acceso y telecomunicaciones;
Los mecanismos de monitoreo y revisión de las medidas de seguridad;
El plan de trabajo, y
El programa general de capacitación.
El Responsable deberá actualizar el documento de seguridad anualmente, o cuando se produzcan modificaciones relevantes en el tratamiento de los datos que impliquen un cambio en el nivel de riesgo; ante acciones de mejora continua derivadas del monitoreo del sistema de seguridad; ante una vulneración ocurrida; ante la implementación de acciones preventivas y correctivas derivadas de una vulneración de seguridad, o bien por recomendación del Instituto."
[…]
En consecuencia, los documentos de seguridad de los sistemas de datos personales de este sujeto obligado, contemplan las acciones, políticas, detección de riesgos y las medidas de seguridad que implementa cada responsable con el objetivo de proteger e impedir cualquier tipo de acceso no autorizado o vulneración de los datos personales bajo posesión de esta dependencia. Dichos documentos constituyen los instrumentos necesarios para salvaguardar y proteger los datos personales que se recaban al interior de este ente, por lo que nos vemos obligados a cumplir con lo dispuesto en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, e informar sobre dicho documento **únicamente al Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México,** cuando el órgano garante así lo solicite o determine, de conformidad con el artículo 25 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, el cual fue citado en párrafos anteriores.

Por último, por lo que hace a "…de las Secretarias del Gobierno de la Ciudad de México…", se le informa que la presente respuesta corresponde solo a la Secretaría de Administración y Finanzas, por lo que corresponde a las atribuciones de esta dependencia. Sin embargo, en aras de garantizar el derecho al acceso a la información, de ser de su interés obtener información de algún otro Sujeto Obligado, se proporciona el vínculo electrónico por el cual se puede descargar el Padrón de Sujetos Obligados a fin de que pueda ponerse en contacto e ingresar su solicitud:

http://www.infocdmx.org.mx/evaluacioncdmx/padron.php

Si así lo prefiere, puede consultar el Directorio de los Sujetos Obligados de la Ciudad de México, en el sitio:

http://www.infodf.org.mx/directorio/consulta.php

En esta página podrá visualizar los datos de contacto de todos los Sujetos Obligados de la Ciudad de México.
[…][Sic]

3. Recurso. El diecisiete de noviembre de dos mil veintidós, 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:

> […]
> No se me dio la información que solicité, me dicen que es un documento que no pueden dar, cuando lo cierto es que se puede hacer una versión pública.
> […] [Sic]

4. Admisión. El veintidós de noviembre de dos mil veintidós, con fundamento en lo establecido en los artículos, 51 fracciones I y II, 52, 53, fracción II, 233, 234 fracción I, 236, 237 y 243, fracción I de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México, **se admitió a trámite** el presente recurso de revisión.

Asimismo, con fundamento en los artículos 230 y 243, fracciones II y III de la Ley de Transparencia, se pone a disposición de las partes el expediente en que se actúa, para que, dentro del plazo de siete días hábiles contados a partir del día siguiente a aquel en que se practique la notificación del presente acuerdo, realicen manifestaciones, ofrezcan pruebas y formulen alegatos.

Con la finalidad de evitar dilaciones innecesarias en la substanciación y resolución de este medio de impugnación, con fundamento en lo dispuesto en el artículo 250 de la Ley de Transparencia se requiere a las partes para que dentro del plazo otorgado manifiesten su voluntad para llevar a cabo una Audiencia de Conciliación.

5. Alegatos y manifestaciones. El veinte de diciembre de dos mil veintidós, a través de la PNT, el Sujeto Obligado envió el oficio **SAF/DGAJ/DUT/463/2022**, de fecha diecinueve de diciembre, signado por la Directora de la Unidad de Transparencia de la Secretaría de Administración y Finanzas de la Ciudad de México, donde rindió manifestaciones y alegatos, al tenor de lo siguiente:

> […]
>
> **MANIFESTACIONES**
>
> **PRIMERO.** El agravio manifestado por la parte recurrente se estima **INFUNDADO**, toda vez que, como se le hizo saber en la respuesta primigenia, esta dependencia está obligada a entregar la información que es de interés público, asimismo, tiene la responsabilidad de salvaguardar y proteger los datos personales que esta institución recaba, mediante la creación de los sistemas de datos personales, los cuales se encuentran protegidos por cada unidad administrativa que funge como responsable de dichos sistemas.
>
> De esta forma, en la respuesta del folio recurrido, este sujeto obligado exhibió la fundamentación que imposibilita compartir los documentos de seguridad que las diversas áreas responsables de los datos personales a los que brindan tratamiento elaboran y, por ende, las razones por las que no se pueden hacer públicas las medidas de seguridad que cada una de ellas implementa en sus actividades diarias.
>
> Cabe mencionar que en apego a la normatividad local en materia de transparencia, esta Unidad de Transparencia procedió a explicar de forma fundada y motivada, las razones por las cuales los documentos de seguridad no forman parte de la información pública que este sujeto obligado genere en el ejercicio de sus atribuciones, sino por el contrario, son documentos con la descripción de las medidas que cada área implementa en la salvaguarda, protección, resguardo y seguridad en el tratamiento de los datos personales que conforman los sistemas, con la finalidad de evitar vulneraciones o accidentes en la custodia de la información confidencial.
>
> Como se puede constatar, en la respuesta ofrecida al ahora recurrente, se le informó que cada uno de los sistemas debe de tener su propio documento de seguridad, el cual es un instrumento generado para **proteger y salvaguardar los sistemas de datos personales que este sujeto obligado detenta**. Dicho registro contiene las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales, pues se trata de un sistema de gestión, al cual tiene acceso el responsable, los usuarios y en su caso, los encargados de los sistemas de datos personales. Es decir, se trata de un documento interno para control, resguardo y verificación de cumplimiento por parte de cada responsable de cada sistema de datos personales.

Asimismo, se enunciaron las disposiciones normativas con el sustento de dicha información:

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 almacenamiento de los recursos informáticos en el tratamiento de datos personales;

De la misma forma, esta dependencia comunicó que al tratarse de un documento que contiene las medidas de seguridad que implementa este sujeto obligado a favor del resguardo, protección, salvaguarda y evitar la vulneración de datos personales en nuestra posesión, es importante retomar el artículo 23 de la ley local en la materia de protección de datos, respecto a los deberes del Responsable, entendido este como "cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, Órganos Autónomos, Partidos Políticos, Fideicomisos y Fondos Públicos, que decida y determine finalidad, fines, medios, medidas de seguridad y demás cuestiones relacionadas con el tratamiento de datos personales" (Artículo 3, fracción XXVIII):

"Artículo 23. El responsable para cumplir con el tratamiento lícito, transparente y responsable de los datos personales, tendrá al menos los siguientes deberes:
Destinar recursos autorizados para la instrumentación de programas y políticas de protección de datos personales;
Elaborar políticas y programas de protección de datos personales, obligatorios y exigibles al interior del sujeto obligado;
Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales;
Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran;
Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales;
Garantizar a las personas, el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición
Diseñar, desarrollar e implementar políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la presente Ley y las demás que resulten aplicables en la materia;
Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan con la protección de datos personales y las obligaciones previstas en la presente Ley y las demás que resulten aplicables en la materia;
Cumplir con las políticas y lineamientos, así como las normas y principios aplicables para el tratamiento lícito y la protección de los datos personales;
Adoptar las medidas de seguridad necesarias para la protección de datos personales y los sistemas de datos personales, así como comunicarlas al Instituto para su registro, en los términos de la presente Ley;
Elaborar y presentar al Instituto un Informe correspondiente sobre las obligaciones previstas en la presente Ley, a más tardar en la segunda semana del mes de enero de cada año. La omisión de dicho informe será motivo de responsabilidad;

Informar al titular previo a recabar sus datos personales, la existencia y finalidad de los sistemas de datos personales;
Registrar ante el Instituto los Sistemas de Datos Personales, así como la modificación o supresión de los mismos;
Establecer los criterios específicos sobre el manejo, mantenimiento, seguridad y protección de los sistemas de datos personales; y
Coordinar y supervisar la adopción de medidas de seguridad a que se encuentren sometidos los sistemas de datos personales."

Por lo anterior, le fue comunicado al solicitante que, en apego estricto a la normatividad en materia de protección de datos personales, se deben proteger las medidas de seguridad implementadas al interior del sujeto obligado, para salvaguardar los datos personales a los que tenemos acceso, en el ejercicio de nuestras funciones, con fundamento en el artículo 24 de la ley en la materia, que a la letra señala:

"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."

A su vez, se le señaló que las medidas de seguridad deben considerar los posibles riesgos, el nivel de seguridad, 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, entre otras. Es decir, el documento de seguridad de los sistemas de datos personales contempla las medidas que cada responsable debe establecer, adoptar y vigilar en el acceso a los datos personales recabados.

Por último, se le hizo de conocimiento a la persona solicitante que las medidas de seguridad de los sistemas de datos personales de esta dependencia, únicamente podrán comunicarse al Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (INFO), por lo que no constituye un documento de acceso a información pública, al tratarse de un instrumento para proteger e impedir la vulneración de datos personales en posesión de este sujeto obligado.

Como fundamento normativo, se entregaron las acciones asentadas en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México y en los Lineamientos Generales de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México para la salvaguarda de dichos documentos:

Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México:

"Artículo 25. Las medidas de seguridad adoptadas por el responsable deberán considerar:
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; y
El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.
Estas medidas tendrán al menos los siguientes niveles de seguridad:
Básico: relativas a las medidas generales de seguridad cuya aplicación será obligatoria para el tratamiento y protección de todos los sistemas de datos personales en posesión de los sujetos obligados.
Medio: se refiere a las medidas de seguridad requeridas para aquellos sistemas de datos relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, datos patrimoniales, así como los sistemas que contengan datos con los que se permita obtener evaluación de personalidad o perfiles de cualquier tipo en el presente pasado o futuro.
Alto: corresponde a las medidas de seguridad aplicables a sistemas de datos concernientes a ideología, religión, creencias, afiliación política, origen racial o étnico, salud, biométricos, genéticos o vida sexual, así como los que contengan datos recabados para fines policiales, de seguridad, prevención, investigación y persecución de delitos.
Las medidas de seguridad que adopten los sujetos obligados para mayores garantías en la protección y resguardo de los sistemas de datos personales, únicamente se comunicarán al Instituto, para su registro, el nivel de seguridad aplicable."

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:
Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto
en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;
Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;
Elaborar un inventario de datos personales contenidos en los sistemas de datos;

Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;
Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;
Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales; y
Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

Artículo 27. Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión denominado documento de seguridad.
Artículo 28. El responsable deberá elaborar el documento de seguridad que contendrá, al menos, lo siguiente:
El inventario de datos personales en los sistemas de datos;
Las funciones y obligaciones de las personas que intervengan en el tratamiento datos personales, usuarios y encargados, en el caso de que los hubiera;
Registro de incidencias;
Identificación y autentificación;
Control de acceso; gestión de soportes y copias de respaldo y recuperación;
El análisis de riesgos;
El análisis de brecha;
Responsable de seguridad;
Registro de acceso y telecomunicaciones;
Los mecanismos de monitoreo y revisión de las medidas de seguridad;
El plan de trabajo; y
El programa general de capacitación."

Lineamientos Generales de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México:

"Artículo 41. El Responsable deberá establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales en su posesión de conformidad con lo previsto en los artículos 24, 25, 26 y 27 de la Ley, con el objetivo de impedir, que cualquier tratamiento de los datos personales contravenga las disposiciones de dicho ordenamiento y los presentes Lineamientos.

Las medidas de seguridad a las que se refiere el párrafo anterior constituyen los mínimos exigibles, por lo que el Responsable podrá adoptar las medidas adicionales que estime necesarias para brindar mayores garantías en la protección de los datos personales en su posesión.
Lo anterior, sin perjuicio de lo establecido por aquellas disposiciones vigentes en materia de seguridad de la información emitidas por otras autoridades, cuando estas contemplen una mayor protección para el titular o complementen lo dispuesto en la Ley y en los presentes Lineamientos.
Artículo 52. El Responsable elaborará, difundirá e implementará las normas internas de seguridad de la información mediante el documento de seguridad que será de observancia obligatoria para todos los
servidores públicos del sujeto obligado, así como para toda aquella persona que en su carácter de encargado, conforme al artículo 3, fracción XV de la Ley, tenga acceso a los sistemas de datos personales y/o al sitio donde se ubican los mismos, para ello, el Responsable deberá tomar en cuenta lo dispuesto en la Ley y en los presentes Lineamientos.
El documento de seguridad deberá contener, como mínimo, lo siguiente:
El inventario de datos personales en los sistemas de datos;
Las funciones y obligaciones de las personas que intervengan en el tratamiento de datos personales, usuarios y encargados, en el caso de que los hubiera;
Registro de incidencias;
Identificación y autentificación;
Control de acceso; gestión de soportes y copias de respaldo y recuperación;
El análisis de riesgos;
El análisis de brecha;
Responsable de seguridad;
Registro de acceso y telecomunicaciones;
Los mecanismos de monitoreo y revisión de las medidas de seguridad;
El plan de trabajo, y
El programa general de capacitación.
El Responsable deberá actualizar el documento de seguridad anualmente, o cuando se produzcan modificaciones relevantes en el tratamiento de los datos que impliquen un cambio en el nivel de riesgo; ante acciones de mejora continua derivadas del monitoreo del sistema de seguridad; ante una vulneración ocurrida; ante la implementación de acciones preventivas y correctivas derivadas de una vulneración de seguridad, o bien por recomendación del Instituto."
[…]
Por lo expuesto en párrafos anteriores, queda comprobado que se le contestó al ahora recurrente, sobre la importancia del debido resguardo de los documentos de seguridad de los sistemas de datos personales de este sujeto obligado, ya que contemplan las acciones, políticas, detección de riesgos y las medidas de seguridad que implementa cada responsable con el objetivo de proteger e impedir cualquier tipo de acceso no autorizado o vulneración de los datos personales bajo posesión de esta dependencia. Se le hizo saber que dichos documentos constituyen los

instrumentos necesarios para salvaguardar y proteger los datos personales que se recaban al interior de este ente, por lo que en aras de cumplir con lo dispuesto en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, e **informar sobre dicho documento únicamente al Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México**, cuando el órgano garante así lo solicite o determine, no se le ofreció la información requerida al solicitante, de conformidad con el artículo 25 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, el cual fue citado en párrafos anteriores.

Con base a lo anterior, se puede advertir que el "agravio" carece de todo sustento y al limitarse a afirmar que no se le entregó lo requerido, deja de lado las razones y la fundamentación por la cual no se le puede hacer llegar el documento que cada área de este sujeto obligado elabora para la protección de los sistemas de datos personales bajo su responsabilidad.

Como se puede observar, los argumentos planteados por el recurrente son infundados ya que no se concreta una violación al supuesto al que hace referencia el mismo, toda vez que en su argumentación no fundamenta ni exhibe el supuesto que soporte su dicho siendo estas meras percepciones subjetivas del recurrente, al creer o pensar que esta dependencia no responde lo que corresponde a la información requerida, máxime que se le hizo saber que de conformidad con la normatividad expresada en la Ley para la Protección de Datos Personales en Posesión de los Sujetos Obligados de la Ciudad de México, existe la obligación de proteger y resguardar los datos en posesión de esta dependencia, así como implementar las medidas de seguridad que imposibiliten la vulneración de los mismos.

Soporta lo antes mencionado las siguientes tesis:

Registro digital: 355473
Instancia: Tercera Sala
Quinta Época
Materia(s): Común
Fuente: Semanario Judicial de la Federación.
Tomo LXIII, página 3558
Tipo: Aislada

AGRAVIOS INFUNDADOS.
Son infundados los agravios que no son consecuentes con el concepto de violación invocado en la demanda.

Amparo civil en revisión 6472/37. Puertos de Caselín Soledad, sucesión de. 16 de marzo de 1940.

Unanimidad de cinco votos. La publicación no menciona el nombre del ponente.

Registro digital: 355664
Instancia: Tercera Sala
Quinta Época
Materia(s): Común
Fuente: Semanario Judicial de la Federación.
Tomo LXI, página 3271
Tipo: Aislada

AGRAVIOS INFUNDADOS.
Los agravios que constituyen meras apreciaciones del quejoso, sin fundar éstas en algún motivo legal de que deba ocuparse el fallo respectivo, son improcedentes.
Amparo civil en revisión 7864/38. Terrazas viuda de Horcasitas Elena. 23 de agosto de 1939. Unanimidad de cuatro votos. El Ministro Luis Bazdresch no intervino en la resolución de este negocio, por las razones que constan en el acta del día. La publicación no menciona el nombre del ponente.

Sexta Época
Núm. de Registro: 269534
Instancia: Tercera Sala Tesis Aislada
Fuente: Semanario Judicial de la Federación
Volumen CXXII, Cuarta Parte Materia(s): Común
Tesis:
Página: 52

CONCEPTOS DE VIOLACION INFUNDADOS.
Los conceptos de violación no son fundados cuando en ellos no se concreta propiamente una violación, respecto de algún precepto de la ley, como sucede si el quejoso dice en su demanda que se infringen determinados artículos del Código de Procedimientos Civiles, porque no obstante que se probaron los elementos constitutivos de la acción intentada, la sentencia reclamada resolvió lo contrario, valorando ilegalmente las pruebas para favorecer al demandado, pero no dice por qué se violaron dichas disposiciones legales, ni cuáles fueron las pruebas mal estimadas; y si además, el concepto está formulado en una forma tan general, que no puede obligar a la Suprema Corte de Justicia a examinar todo el proceso, y a estudiar cada uno de los elementos de la acción deducida y de las excepciones opuestas, cuando el agraviado no precisa ni se refiere a ellas en particular, con la pretensión de que el Máximo Tribunal haga una revisión "res integra" del negocio, lo que no puede hacer, sin suplir la deficiencia de la queja, que terminantemente prohíbe el artículo 79 de la Ley de Amparo.
Bajo esa premisa, resulta evidente que el recurrente al expresar su queja no fundamenta ni motiva su manifestación para demostrar la inconsistencia de lo solicitado y lo enviado por este sujeto obligado, como respuesta a su requerimiento.

En ese sentido, el peticionario no genera elementos de convicción que permitan evidenciar la violación al Derecho de Acceso a la Información Pública o la transgresión a los numerales aplicables de ley de la materia. En caso contrario, este sujeto obligado demuestra que la respuesta a su cuestionamiento fue en apego a la normatividad aplicable, por lo que se le informó que la documentación solicitada no era información pública que este sujeto obligado genere en el ejercicio de sus atribuciones, sino por el contrario, se trata de la implementación de las medidas de seguridad que cada área debe cumplir en aras de garantizar la protección y salvaguarda de los datos personales en su posesión, por lo que no forma parte de la esfera pública, sino de la esfera relativa a la protección de la información confidencial a la que esta dependencia brinda tratamiento. De esta forma, los documentos de seguridad, solo podrán compartirse con el órgano garante local, en caso de ser requeridos.

Sin perjuicio de lo anterior, esta Unidad de Transparencia procede a defender la congruencia y legalidad de la respuesta emitida, por lo que se manifiesta, que esta Autoridad actuó en estricto apego al procedimiento establecido para la atención a las solicitudes en materia de información pública y garantizar en todo momento el Derecho de Acceso a la Información del ahora recurrente conforme a los principios de certeza y buena fe.

SEGUNDO. Una vez expuestas las consideraciones de este sujeto obligado, es procedente que este Instituto proceda a **CONFIRMAR** la respuesta emitida con fundamento en lo dispuesto por el artículo 244, fracción III, de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México, en atención a la solicitud de información que el particular ha realizado en esta Secretaría de Administración y Finanzas, máxime que la misma atiende en todo el derecho humano de acceso a la información Pública en términos de la normatividad aplicable.

Como sustento de lo aquí expuesto, se señalan a continuación las documentales públicas que deberán considerarse al momento de emitir la resolución que en derecho proceda.

PRUEBAS

1.- LA DOCUMENTAL PÚBLICA, consistente en la solicitud de información pública con número de folio 090162822004066.

2.- LA DOCUMENTAL PÚBLICA, consistente en el oficio de respuesta, emitido por la Unidad de Transparencia de esta Secretaría.

3.- LA DOCUMENTAL PÚBLICA, consistente en el Acuse de información entrega vía Plataforma Nacional de Transparencia, generado por el SISAI.

Por lo anteriormente expuesto, atentamente solicito:

PRIMERO. Tener por presentadas en tiempo y forma las manifestaciones de ley y por ofrecidas las pruebas mencionadas en el presente escrito.

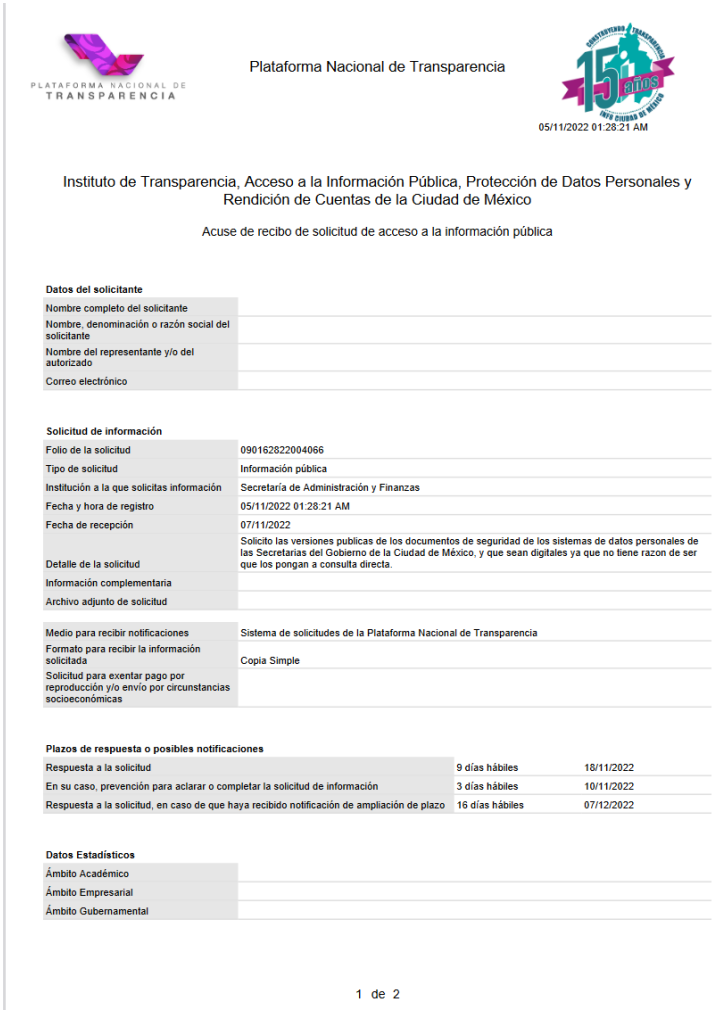
SEGUNDO. CONFIRMAR la respuesta emitida por esta Dependencia, en términos de lo establecido por el artículo 244 fracción III, de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México.

TERCERO. Registrar como medio para recibir información, toda clase de documentos y notificaciones sobre los acuerdos que se dicten en el presente recurso los correos electrónicos, ut@finanzas.cdmx.gob.mx y saf.recursosrevision@gmail.com.

CUARTO. Tener por autorizados para oír y recibir cualquier tipo de notificación, así como para imponerse de los autos, a los ciudadanos señalados en el presente escrito.
[…][sic]

Asimismo, el sujeto obligado anexó lo siguiente:

- Oficio sin número, de fecha dieciséis de noviembre, signado por la Secretaría de Administración y Finanzas, transcrito con anterioridad.
- Acuse de recibo de solicitud de acceso a la información pública del folio de la solicitud **090162822004066**



Plataforma Nacional de Transparencia

05/11/2022 01:28:21 AM

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

Acuse de recibo de solicitud de acceso a la información pública

Datos del solicitante

Nombre completo del solicitante	
Nombre, denominación o razón social del solicitante	
Nombre del representante y/o del autorizado	
Correo electrónico	

Solicitud de información

Folio de la solicitud	090162822004066
Tipo de solicitud	Información pública
Institución a la que solicitas información	Secretaría de Administración y Finanzas
Fecha y hora de registro	05/11/2022 01:28:21 AM
Fecha de recepción	07/11/2022
Detalle de la solicitud	Solicito las versiones publicas de los documentos de seguridad de los sistemas de datos personales de las Secretarias del Gobierno de la Ciudad de México, y que sean digitales ya que no tiene razon de ser que los pongan a consulta directa.
Información complementaria	
Archivo adjunto de solicitud	

Medio para recibir notificaciones	Sistema de solicitudes de la Plataforma Nacional de Transparencia
Formato para recibir la información solicitada	Copia Simple
Solicitud para exentar pago por reproducción y/o envío por circunstancias socioeconómicas	

Plazos de respuesta o posibles notificaciones

Respuesta a la solicitud	9 días hábiles	18/11/2022
En su caso, prevención para aclarar o completar la solicitud de información	3 días hábiles	10/11/2022
Respuesta a la solicitud, en caso de que haya recibido notificación de ampliación de plazo	16 días hábiles	07/12/2022

Datos Estadísticos

Ámbito Académico	
Ámbito Empresarial	
Ámbito Gubernamental	

1 de 2

- Acuse de información entrega vía Plataforma Nacional de Transparencia de fecha dieciséis de noviembre, donde rindió su respuesta primigenia.

Plataforma Nacional de Transparencia

16/11/2022 13:54:03 PM

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

Acuse de información entrega vía Plataforma Nacional de Transparencia

Solicitud presentada

Folio de la solicitud	090162822004066
Sujeto Obligado al que se dirige	Secretaría de Administración y Finanzas
Fecha y hora de recepción	05/11/2022 01:28:21 AM
Fecha de caducidad de plazo	18/11/2022
Información solicitada	Solicito las versiones publicas de los documentos de seguridad de los sistemas de datos personales de las Secretarias del Gobierno de la Ciudad de México, y que sean digitales ya que no tiene razon de ser que los pongan a consulta directa.
Datos adicionales	
Archivo adjunto	

Respuesta a la solicitud

Se hace entrega de la información solicitada a través del medio electrónico gratuito del sistema Plataforma Nacional de Transparencia.

Fecha y hora de entrega de información	16/11/2022 13:54:03 PM
	Estimado Usuario del Sistema P r e s e n t e Se adjunta respuesta, de folio en comento. Asimismo, se le informa que para garantizar tanto el ejercicio del derecho fundamental a la información, como el principio democrático de publicidad de los actos de gobierno, estamos a sus órdenes para cualquier duda o comentario sobre el particular, en el correo electrónico ut@finanzas.cdmx.gob.mx de lunes a viernes en un horario de 9:00 a 15:00 horas. De la misma manera, le comunicamos que tiene el derecho a interponer el recurso de revisión correspondiente, a través de los medios electrónicos o de manera directa presentando escrito en formato libre o el proporcionado por el Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, dentro de un plazo de 15 días hábiles contados a partir de la fecha en que surte efectos la notificación de la respuesta emitida por este Sujeto Obligado. Finalmente, esta respuesta se encuentra ajustada a derecho, toda vez que se atiende en términos de los artículos en los artículos 6 de la Constitución Política de los Estados Unidos Mexicanos; 1, 121 de la Ley General de Transparencia y Acceso a la Información Pública; 2, 3, 4, 6, fracciones I, XIII, XIV y XLII, 8, 11, 13, 14, 19, 92, 93, 192, 193, 200, 208, 212, 233, 234, 236 y demás relativos de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México, artículo 27 y numerales Décimo Séptimo y Décimo Octavo transitorios de la Ley Orgánica del Poder Ejecutivo y de la Administración Pública de la Ciudad de México. A t e n t a m e n t e Unidad de Transparencia De la Secretaría de Administración y Finanzas De la Ciudad de México.
Respuesta Información Solicitada	
Archivo(s) adjunto(s)	respuesta de la solicitud 4066.pdf

1 de 2

6. Cierre de Instrucción. El veintidós de diciembre de dos mil veintidós, 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 tuvieron por presentadas las 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.

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

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

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.

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, en la PNT, se advirtió la respuesta impugnada como las constancias relativas a su tramitación.

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.*

Cabe señalar que, si bien el Sujeto Obligado emitió una respuesta, no es posible desprender del estudio de las constancias que obran en el expediente que la respuesta que otorgó el Sujeto Obligado sea suficiente para dejar sin materia el recurso de revisión, tal como se analizará posteriormente. Por este motivo, este Organismo Autónomo considera que debe entrarse al estudio de fondo del presente asunto.

CUARTO. Estudio de fondo. Una vez realizado el estudio de las constancias que integran el expediente en que se actúa, se desprende que la presente resolución consiste en determinar la legalidad de la respuesta emitida por el sujeto obligado, en atención a la solicitud de acceso al rubro citada, de conformidad con lo dispuesto por la Ley de Transparencia.

En el presente caso, la ***litis*** consiste en determinar si la respuesta emitida por el sujeto obligado se ajustó a los principios que rigen la materia, de conformidad con las disposiciones normativas aplicables.

- **Tesis de la decisión**

El agravio plantado por la parte recurrente resulta fundado y suficiente para **revocar** la respuesta brindada por la Secretaría de Administración y Finanzas.

- **Razones de la decisión**

Con el objeto de ilustrar la controversia planteada y lograr claridad en el tratamiento del tema en estudio, resulta conveniente precisar la solicitud de información, la respuesta del sujeto obligado y el agravio de la parte recurrente.

En primer lugar, por lo que concierne a la solicitud de información y la respuesta otorgada por el Sujeto Obligado, en sus partes medulares, señalan lo siguiente:

Solicitud	Respuesta
El Particular solicitó saber: • Las versiones públicas de los documentos de seguridad de los sistemas de datos personales de las Secretaría.	El Sujeto obligado a través de la **Unidad de Transparencia,** informó que los documentos de seguridad de los sistemas de datos personales de ese sujeto obligado, contemplan las acciones, políticas, detección de riesgos y las medidas de seguridad que implementa cada responsable con el objetivo de proteger e impedir cualquier tipo de acceso no autorizado o vulneración de los datos personales bajo posesión de esta dependencia, por lo que no proporcionó la información peticionada.

Por lo anterior, la Parte recurrente interpuso su recurso de revisión en el tenor de lo siguiente:

Recurso de revisión	Alegatos y manifestaciones del Sujeto obligado
El Particular interpuso su recurso de debido a que el Sujeto obligado no otorgó las versiones públicas de lo peticionado.	El Sujeto obligado reiteró su respuesta primigenia.

Expuestas las posturas de las partes, este órgano colegiado procede al análisis de la legalidad de la respuesta emitida a la solicitud motivo del presente recurso de revisión, a fin de determinar si el sujeto obligado garantizó el derecho de acceso a la información pública de la persona solicitante, en razón al agravio formulado.

Estudio del agravio: clasificación de la información.

El Particular solicitó saber:

- **Las versiones públicas de los documentos de seguridad de los sistemas de datos personales de las Secretaría.**

El Sujeto obligado a través de la Unidad de Transparencia, informó que los documentos de seguridad de los sistemas de datos personales de ese sujeto obligado, contemplan las acciones, políticas, detección de riesgos y las medidas de seguridad que implementa cada responsable con el objetivo de proteger e impedir cualquier tipo de acceso no autorizado o vulneración de los datos personales bajo posesión de esta dependencia, por lo que no proporcionó la información peticionada.

El Particular interpuso su recurso de debido a que el Sujeto obligado omitió la entrega de versiones públicas de los documentos de seguridad.

Ahora bien, es conveniente hacer referencia a la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México, la cual establece lo siguiente:

> *"**Artículo 1**. La presente Ley es de orden público y de observancia general en el territorio de la Ciudad de México en materia de Transparencia, Acceso a la Información, Gobierno Abierto y Rendición de Cuentas.*
>
> *Tiene por **objeto** establecer los principios, bases generales y procedimientos para **garantizar a toda persona el Derecho de Acceso a la Información Pública** en posesión de cualquier autoridad, entidad, órgano y organismo del poder Ejecutivo, Legislativo y Judicial, Órganos Autónomos, Órganos Político Administrativos, Alcaldías y/o Demarcaciones Territoriales, Organismos Paraestatales, Universidades Públicas, Partidos Políticos, Sindicatos, Fideicomisos y Fondos Públicos, así como de cualquier persona física o moral que reciba y ejerza recursos públicos, realice actos de autoridad o de interés público en la Ciudad de México.*
> *…*
>
> ***Artículo 3**. El Derecho Humano de Acceso a la Información Pública comprende solicitar, investigar, difundir, buscar y recibir información.*
>
> ***Toda la información generada, obtenida, adquirida, transformada o en posesión de los sujetos obligados es pública y accesible a cualquier persona en los términos y condiciones que se establezcan en la presente Ley**, en los tratados internacionales de los que el Estado mexicano sea parte, en la Ley General y la normatividad aplicable en sus respectivas competencias; sólo podrá ser clasificada excepcionalmente como reservada temporalmente por razones de interés público, en los términos dispuestos por esta Ley.*
> *…*
>
> ***Artículo 6**. Para los efectos de esta Ley se entiende por:*
> *…*
> ***XIII**. **Derecho de Acceso a la Información Pública**: A la prerrogativa que tiene toda persona para acceder a la información **generada, administrada o en poder de los sujetos obligados**, en los términos de la presente Ley:*
> *…*
>
> ***XXXVIII**. **Rendición de Cuentas**: vista desde la perspectiva de la transparencia y el acceso a la información, **consiste en la potestad del individuo para exigir al poder público informe y ponga a disposición en medios adecuados, las acciones y decisiones emprendidas derivadas del desarrollo de su actividad, así como los indicadores que permitan el conocimiento y la forma en que las llevó a cabo, incluyendo los resultados obtenidos**; así como la obligación de dicho poder público de cumplir con las obligaciones que se le establecen en la legislación de la materia, y garantizar mediante la implementación de los medios que sean necesarios y dentro del marco de la Ley, el disfrute*

del Derecho de Acceso a la Información Pública consagrado en el artículo sexto de la Constitución General de la República;
…

***Artículo 7**. **Para ejercer el Derecho de Acceso a la Información Pública no es necesario acreditar derechos subjetivos, interés legítimo o razones que motiven el requerimiento**, ni podrá condicionarse el mismo por motivos de discapacidad, salvo en el caso del Derecho a la Protección de Datos Personales, donde deberá estarse a lo establecido en la ley de protección de datos personales vigente y demás disposiciones aplicables.*
…

***Artículo 8**. **Los sujetos obligados garantizarán de manera efectiva y oportuna, el cumplimiento de la presente Ley**. Quienes produzcan, administren, manejen, archiven o conserven información pública serán responsables de la misma en los términos de esta Ley.*

La pérdida, destrucción, alteración u ocultamiento de la información pública y de los documentos en que se contenga, serán sancionados en los términos de esta Ley.
…

***Artículo 28**. **Los sujetos obligados deberán preservar los documentos y expedientes en archivos organizados y actualizados** de conformidad con la Ley en la materia y demás disposiciones aplicables, asegurando su adecuado funcionamiento y protección, **con la finalidad de que la información se encuentre disponible, localizable, integra, sea expedita y se procure su conservación**.*
…

***Artículo 92**. Los sujetos obligados deberán de contar con una Unidad de Transparencia, en oficinas visibles y accesibles al público, que dependerá del titular del sujeto obligado y se integrará por un responsable y por el personal que para el efecto se designe. Los sujetos obligados harán del conocimiento del Instituto la integración de la Unidad de Transparencia.*

***Artículo 93**. Son atribuciones de la Unidad de Transparencia:*

***I**. Capturar, ordenar, analizar y procesar las solicitudes de información presentadas ante el sujeto obligado;*
…

***IV**. Recibir y tramitar las solicitudes de información así como darles seguimiento hasta la entrega de la misma, haciendo entre tanto el correspondiente resguardo;*
…

***Artículo 112**. Es obligación de los sujetos obligados:*
…

***V**. Poner a disposición las obligaciones de transparencia en formatos abiertos, útiles y reutilizables, para fomentar la transparencia, la colaboración y la participación ciudadana;*

***Artículo 113**. La información pública de oficio señalada en esta Ley, se considera como obligaciones de transparencia de los sujetos obligados.*

***Artículo 114**. Los sujetos obligados deberán poner a disposición, la información pública de oficio a que se refiere este Título, en formatos abiertos en sus respectivos sitios de Internet y a través de la plataforma electrónica establecidas para ello.*

…

***Artículo 200**. **Cuando la Unidad de Transparencia determine la notoria incompetencia por parte del sujeto obligado dentro del ámbito de su aplicación**, para atender la solicitud de acceso a la información, deberá de comunicarlo al solicitante, dentro de los **tres días posteriores a la recepción de la solicitud** y señalará al solicitante el o los sujetos obligados competentes.*

Si el sujeto obligado es competente para atender parcialmente la solicitud de acceso a la información, deberá de dar respuesta respecto de dicha parte. Respecto de la información sobre la cual es incompetente se procederá conforme a lo señalado en el párrafo anterior.

***Artículo 201**. Las Unidades de Transparencia están obligadas a garantizar las medidas y condiciones de accesibilidad para ejercer el derecho de Acceso a la Información Pública, a entregar información sencilla y comprensible a la persona o a su representante sobre los trámites y procedimientos que deben efectuarse, las autoridades o instancias competentes, la forma de realizarlos, la manera de llenar los formularios que se requieran, así como de las entidades ante las que se puede acudir para solicitar orientación o formular quejas, consultas o reclamos sobre la prestación del servicio o sobre el ejercicio de las funciones o competencias a cargo de la autoridad de que se trate.*

***Artículo 203**. Cuando la solicitud presentada no fuese clara en cuanto a la información requerida o no cumpla con todos los requisitos señalados en la presente ley, el sujeto obligado mandará requerir dentro de los tres días, por escrito o vía electrónica, al solicitante, para que en un plazo de diez días contados a partir del día siguiente en que se efectuó la notificación, aclare y precise o complemente su solicitud de información. En caso de que el solicitante no cumpla con dicha prevención, la solicitud de información se tendrá como no presentada. Este requerimiento interrumpirá el plazo establecido en el artículo 212 de esta ley. Ninguna solicitud de información podrá desecharse si el sujeto obligado omite requerir al solicitante para que subsane su solicitud.*

En el caso de requerimientos parciales no desahogados, se tendrá por presentada la solicitud por lo que respecta a los contenidos de información que no formaron parte de la prevención.

…

> ***Artículo 208**. **Los sujetos obligados deberán otorgar acceso a los Documentos que se encuentren en sus archivos o que estén obligados a documentar de acuerdo con sus facultades, competencias o funciones** en el formato en que el solicitante manifieste, de entre aquellos formatos existentes, conforme a las características físicas de la información o del lugar donde se encuentre así lo permita.*
>
> *En el caso de que la información solicitada consista en bases de datos se deberá privilegiar la entrega de la misma en Formatos Abiertos.*
> *…*
>
> ***Artículo 211.** Las Unidades de Transparencia deberán **garantizar que las solicitudes se turnen a todas las Áreas competentes que cuenten con la información o deban tenerla** de acuerdo a sus facultades competencias y funciones, con el objeto de que realicen una búsqueda exhaustiva y razonable de la información solicitada.*
> *...*
>
> ***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*
>
> *…" (**Sic**)*

De la normativa previamente citada, se desprende lo siguiente:

- El objeto de la Ley de la materia, es garantizar a toda persona el derecho de acceso a la información pública en posesión de cualquier autoridad, entidad, órgano y organismo del Poder Ejecutivo, Legislativo y Judicial, Órganos Autónomos, Órganos Político Administrativos, Alcaldías y/o Demarcaciones Territoriales, Organismos Paraestatales, Universidades Públicas, Partidos Políticos, Sindicatos, Fideicomisos y Fondos Públicos, así como de cualquier persona física o moral que reciba y ejerza recursos públicos, realice actos de autoridad o de interés público en la Ciudad de México.

- Toda la información generada, obtenida, adquirida, transformada o en posesión de los sujetos obligados es pública y accesible a cualquier persona en los términos y condiciones que se establezcan las leyes de la materia.

- Los sujetos obligados deben preservar los documentos y expedientes en archivos organizados y actualizados, asegurando su adecuado funcionamiento, con la finalidad de que la información se encuentre disponible, localizable, integra, sea expedita y se procure su conservación.

- Las Unidades de Transparencia de los sujetos obligados deben garantizar que las solicitudes se turnen a todas las Áreas competentes que cuenten con la información o normativamente deban tenerla, con el objeto de que se realice una búsqueda exhaustiva y razonable de la información solicitada.

- Los sujetos obligados deben otorgar acceso a los documentos que se encuentren en sus archivos o que estén obligados a documentar de acuerdo con sus facultades, competencias y funciones.

- Los sujetos obligados deberán señalar su incompetencia dentro los tres días posteriores a la recepción de la solicitud.

Toda vez que la inconformidad del particular se centra en que el Sujeto obligado indicó que los documentos de seguridad contienen información que no pueden proporcionar pues señalan las medidas de seguridad y protección de los sistemas de datos personales, nos allegaremos a diversos preceptos normativos con la finalidad de conocer las funciones y atribuciones del Sujeto obligado.

De la respuesta primigenia, es posible advertir que el Particular en su solicitud requirió los documentos de seguridad de las Secretarías de Gobierno, en este sentido, si bien es cierto que la Parte Recurrente no identificó las Secretarías de manera general, también es cierto que en su respuesta el Sujeto obligado tomó a literalidad la solicitud del particular por lo que le preció y orientó que sólo se cuenta con una Secretaría de Gobierno en la Ciudad de México.

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 entregar los documentos que se encuentren en sus archivos, la Secretaría de Administración y Finanzas debió entregar la versión pública de los documentos de seguridad con los que cuenta previa aprobación del Comité de Transparencia, de lo cual fue omiso.

Cabe señalar que, si bien la información peticionada por el Particular corresponde a información de carácter reservado, el Sujeto obligado debió hacer entrega de una versión pública de sus documentos de seguridad.

Aunado a lo anterior, este Órgano Garante también procedió a verificar las razones por las que el Sujeto Obligado debió sustentar 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 autentificación; 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 el documento denominado "Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales"[2], 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:

[2] Disponible para su consulta en: 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:

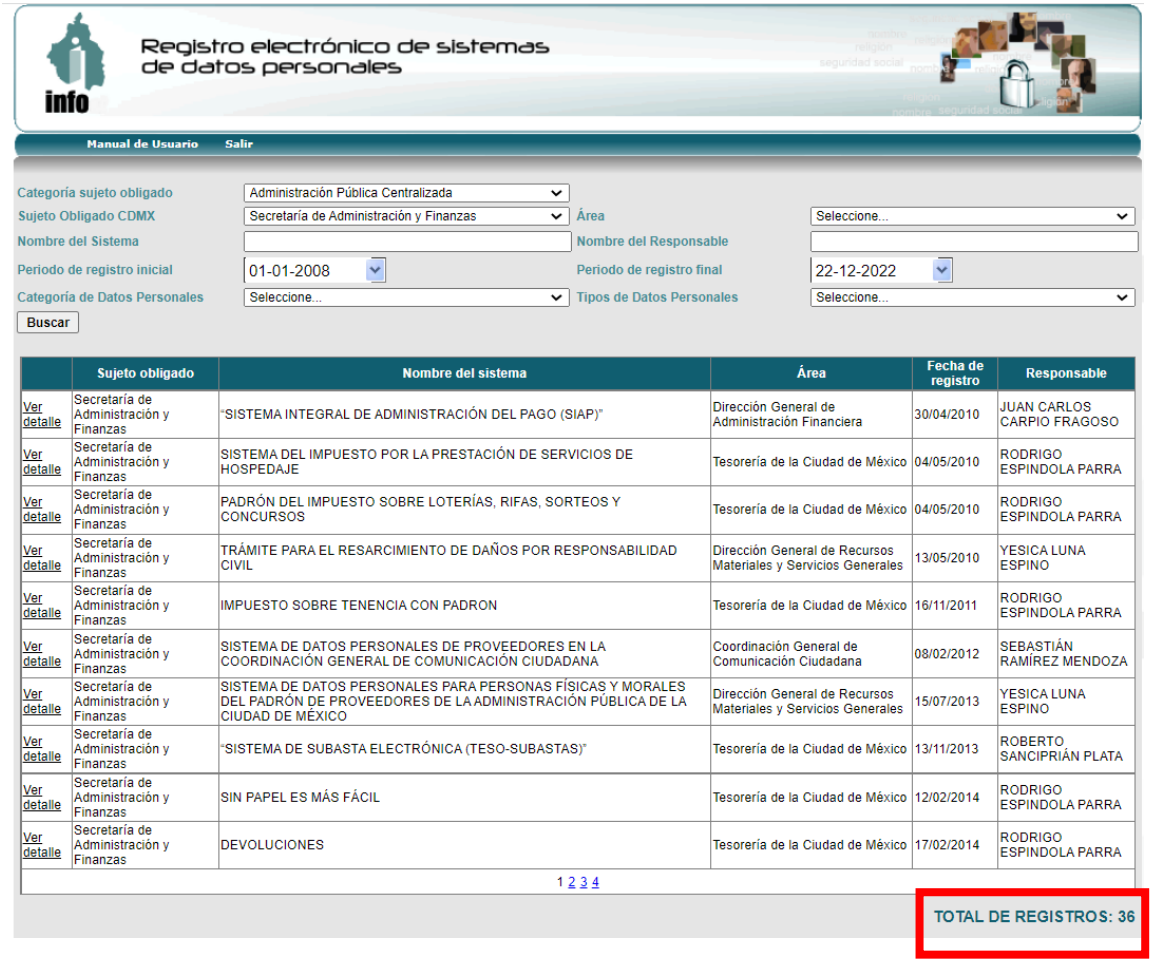
- Organizacionales.
- De procesos y procedimientos.
- De personal.
- Del ambiente físico.
- De la configuración de sistemas de información.

- 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.**

Aunado a lo anterior, este Instituto de Transparencia llevó a cabo la búsqueda de los Sistemas de Datos Personales con los que cuenta la Secretaría de Administración y Finanzas, tal y como se ilustra a continuación:



Registro electrónico de sistemas de datos personales

info

Manual de Usuario Salir

Categoría sujeto obligado: Administración Pública Centralizada

Sujeto Obligado CDMX: Secretaría de Administración y Finanzas

Área: Seleccione...

Nombre del Sistema:

Nombre del Responsable:

Periodo de registro inicial: 01-01-2008

Periodo de registro final: 22-12-2022

Categoría de Datos Personales: Seleccione...

Tipos de Datos Personales: Seleccione...

Buscar

	Sujeto obligado	Nombre del sistema	Área	Fecha de registro	Responsable
Ver detalle	Secretaría de Administración y Finanzas	"SISTEMA INTEGRAL DE ADMINISTRACIÓN DEL PAGO (SIAP)"	Dirección General de Administración Financiera	30/04/2010	JUAN CARLOS CARPIO FRAGOSO
Ver detalle	Secretaría de Administración y Finanzas	SISTEMA DEL IMPUESTO POR LA PRESTACIÓN DE SERVICIOS DE HOSPEDAJE	Tesorería de la Ciudad de México	04/05/2010	RODRIGO ESPINDOLA PARRA
Ver detalle	Secretaría de Administración y Finanzas	PADRÓN DEL IMPUESTO SOBRE LOTERÍAS, RIFAS, SORTEOS Y CONCURSOS	Tesorería de la Ciudad de México	04/05/2010	RODRIGO ESPINDOLA PARRA
Ver detalle	Secretaría de Administración y Finanzas	TRÁMITE PARA EL RESARCIMIENTO DE DAÑOS POR RESPONSABILIDAD CIVIL	Dirección General de Recursos Materiales y Servicios Generales	13/05/2010	YESICA LUNA ESPINO
Ver detalle	Secretaría de Administración y Finanzas	IMPUESTO SOBRE TENENCIA CON PADRON	Tesorería de la Ciudad de México	16/11/2011	RODRIGO ESPINDOLA PARRA
Ver detalle	Secretaría de Administración y Finanzas	SISTEMA DE DATOS PERSONALES DE PROVEEDORES EN LA COORDINACIÓN GENERAL DE COMUNICACIÓN CIUDADANA	Coordinación General de Comunicación Ciudadana	08/02/2012	SEBASTIÁN RAMÍREZ MENDOZA
Ver detalle	Secretaría de Administración y Finanzas	SISTEMA DE DATOS PERSONALES PARA PERSONAS FÍSICAS Y MORALES DEL PADRÓN DE PROVEEDORES DE LA ADMINISTRACIÓN PÚBLICA DE LA CIUDAD DE MÉXICO	Dirección General de Recursos Materiales y Servicios Generales	15/07/2013	YESICA LUNA ESPINO
Ver detalle	Secretaría de Administración y Finanzas	"SISTEMA DE SUBASTA ELECTRÓNICA (TESO-SUBASTAS)"	Tesorería de la Ciudad de México	13/11/2013	ROBERTO SANCIPRIÁN PLATA
Ver detalle	Secretaría de Administración y Finanzas	SIN PAPEL ES MÁS FÁCIL	Tesorería de la Ciudad de México	12/02/2014	RODRIGO ESPINDOLA PARRA
Ver detalle	Secretaría de Administración y Finanzas	DEVOLUCIONES	Tesorería de la Ciudad de México	17/02/2014	RODRIGO ESPINDOLA PARRA

1 2 3 4

TOTAL DE REGISTROS: 36

Por lo anterior es posible advertir que el sujeto obligado cuenta con un total de 36 registros de sistemas de datos personales, por lo que debió realizar la entrega de 36 versiones públicas de documentos de seguridad previa aprobación del Comité de Transparencia.

Ahora bien, de conformidad con 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 tratara 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 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 autentificación 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 autentificación 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 autentificación 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

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 autentificación dentro del documento de seguridad del Sistema de Datos Personales, **no obstante es necesario precisar que, dicho listado es enunciativo más no limitativo, por lo que, si la Unidad administrativa responsable del documento de seguridad de la Secretaría de Administración y Finanzas en el análisis del procedimiento de clasificación identifica alguna, ésta debe incluirse.**

Por lo anteriormente dicho, el agravio del particular deviene **fundado**, ya que como ha quedado de manifiesto el sujeto obligado **incumplió con el procedimiento de atención de solicitudes de información**, previsto en la Ley de Transparencia, toda vez que el Sujeto obligado no dio el trámite correcto a la solicitud materia del presente recurso, en suma, no realizó la búsqueda de la información y tampoco fundó y motivó adecuadamente el porqué no podría entregar la versión pública de los documentos solicitados ni otorgó las versiones públicas de sus documentos de seguridad previa aprobación del Comité de Transparencia.

En consecuencia, por todo lo aquí expuesto, este Órgano Colegiado determina que la respuesta emitida **no brinda certeza al particular, ni es exhaustiva ni está fundada ni motivada, por lo que fue violatoria del derecho de acceso a sus datos personales que detenta el recurrente, así como de lo establecido en el artículo 6, fracciones VIII, IX y X**, de la Ley de Procedimiento

Administrativo de la Ciudad de México, de aplicación supletoria a la Ley de Transparencia que a la letra establece:

> ***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;*
>
> ***IX****. Expedirse de conformidad con el procedimiento que establecen los ordenamientos aplicables y en su defecto, por lo dispuesto en esta Ley; y*
>
> ***X****. Expedirse de manera congruente con lo solicitado y* ***resolver expresamente todos los puntos propuestos por los interesados*** *o previstos por las normas.*

Como puede observarse en los fundamentos legales citados, todo acto administrativo debe ser expedido de conformidad con el procedimiento que establece el ordenamiento aplicable, que en este caso es la Ley de Transparencia, pues esta regula la atención y trámite a las solicitud de información pública; y que dicho acto debe contar con la debida y suficiente fundamentación y motivación; entendiéndose por **FUNDAMENTACIÓN** el señalamiento de manera precisa de los artículos o preceptos jurídicos en los que descansa su determinación y que sirvan de base legal para sustentar la misma; y por **MOTIVACIÓN**, el señalamiento y acreditación de los motivos, razones o circunstancias en las cuales el sujeto obligado apoya su determinación; situación que no aconteció en el presente caso.

Sirviendo de sustento a lo anteriormente determinado, las jurisprudencias emitidas por el Poder Judicial de la Federación, cuyos rubros señalan:

FUNDAMENTACION Y MOTIVACION.[3]**; FUNDAMENTACIÓN Y MOTIVACIÓN. EL CUMPLIMIENTO DE TALES REQUISITOS NO SE LIMITA A LAS RESOLUCIONES DEFINITIVAS O QUE PONGAN FIN AL PROCEDIMIENTO**[4]**; COMPETENCIA DE LAS AUTORIDADES ADMINISTRATIVAS. EN EL MANDAMIENTO ESCRITO QUE CONTIENE EL ACTO DE MOLESTIA, DEBE SEÑALARSE CON PRECISIÓN EL PRECEPTO LEGAL QUE LES OTORGUE LA ATRIBUCIÓN EJERCIDA Y, EN SU CASO, LA RESPECTIVA FRACCIÓN, INCISO Y SUBINCISO**[5]**; y COMPETENCIA. SU FUNDAMENTACION ES REQUISITO ESENCIAL DEL ACTO DE AUTORIDAD.**[6]

Por otra parte, todo acto administrativo también debe emitirse en plena observancia de 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**

[3] Consultable en Semanario Judicial de la Federación y su Gaceta, Época: Novena Época; Registro: 203143; Instancia: Tribunales Colegiados de Circuito; Tomo III, Marzo de 1996; Tesis: VI.2o. J/43; Página: 769

[4] Consultable en Semanario Judicial de la Federación y su Gaceta, Época: Novena Época; Registro: 197923; Instancia: Tribunales Colegiados de Circuito; Tomo VI, Agosto de 1997; Tesis: XIV.2o. J/12; Página: 538

[5] Consultable en Semanario Judicial de la Federación y su Gaceta, Época: Novena Época; Registro: 188432; Instancia: Segunda Sala; Tomo XIV, Noviembre de 2001; Tesis: 2a./J. 57/2001; Página: 31

[6] Consultable en Semanario Judicial de la Federación y su Gaceta, Época: Octava Época; Registro: 205463; Instancia: Pleno; Núm. 77, Mayo de 1994; Tesis: P./J. 10/94; Página: 12

contenidos de información requeridos por el recurrente, a fin de satisfacer la solicitud correspondiente; circunstancia que en el presente recurso no aconteció, en virtud de que el sujeto obligado no dio el tratamiento que por ley estaba obligado a dar a la solicitud de acceso a la información que nos atiende, no proporcionando la información solicitada por la persona hoy recurrente.

Sirviendo de apoyo a lo anterior, las jurisprudencias emitidas por el Poder Judicial de la Federación, cuyo rubro señalan "**CONGRUENCIA Y EXHAUSTIVIDAD, PRINCIPIOS DE. SUS DIFERENCIAS Y CASO EN QUE EL LAUDO INCUMPLE EL SEGUNDO DE ELLOS**" y "**GARANTÍA DE DEFENSA Y PRINCIPIO DE EXHAUSTIVIDAD Y CONGRUENCIA. ALCANCES**".

Consecuentemente este órgano resolutor llega a la conclusión de que el actuar y la respuesta emitida por el sujeto obligado deviene desapegada a derecho; por tanto, resulta **fundado del agravio** esgrimido por la persona recurrente; razón por la cual, se determina con fundamento en la fracción V del artículo 244 de la Ley de la materia, el **REVOCAR** la referida respuesta e instruir al Sujeto Obligado, a efecto de que:

- **Elabore y entregue las versiones públicas de los documentos de seguridad con los que cuenta previa aprobación del Comité de Transparencia.**
- **Todo lo anterior, debiéndose notificar a la persona recurrente, a través del medio de notificación que este haya señalado para oír y recibir notificaciones en el presente medio de impugnación.**

Lo anterior en un plazo que no deberá exceder los 10 días a partir de que le sea notificada la presente resolución. Lo anterior, de conformidad con el artículo 244 último párrafo de la Ley de Transparencia.

CUARTO. En el caso en estudio esta autoridad no advierte que personas servidoras públicas del Sujeto Obligado hayan incurrido en posibles infracciones a la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México, por lo que no ha lugar a dar vista a la Secretaría de la Contraloría General de la Ciudad de México.

Finalmente, en cumplimiento de lo dispuesto por el artículo 254 de la Ley de Transparencia, se informa a la persona recurrente que en caso de estar inconforme con la presente resolución, la podrá impugnar ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales o ante el Poder Judicial de la Federación, sin poder agotar simultáneamente ambas vías.

Por todo lo expuesto y fundado, el Pleno del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México:

R E S U E L V E

PRIMERO. Por las razones señaladas en la consideración cuarta de la presente resolución, y con fundamento en el artículo 244, fracción V, de la Ley de

Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México, se **REVOCA** la respuesta emitida por el sujeto obligado y se le ordena que emita una nueva, en el plazo de diez días y conforme a los lineamientos establecidos en la consideración inicialmente referida.

SEGUNDO. Con fundamento en los artículos 257 y 258, de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México, se instruye al sujeto obligado para que informe a este Instituto por escrito, sobre el cumplimiento a lo ordenado en el punto Resolutivo Primero, al día siguiente de concluido el plazo concedido para dar cumplimiento a la presente resolución, anexando copia de las constancias que lo acrediten. Con el apercibimiento de que, en caso de no hacerlo, se procederá en términos de la fracción III, del artículo 259, de la Ley de la materia.

TERCER. 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 persona 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.

CUARTO. Se pone a disposición de la persona recurrente el teléfono **55 56 36 21 20** y el correo electrónico **ponencia.enriquez@infocdmx.org.mx** para que comunique a este Instituto cualquier irregularidad en el cumplimiento de la presente resolución.

QUINTO. Este Instituto dará seguimiento a la presente resolución llevando a cabo las actuaciones necesarias para asegurar su cumplimiento y, en su momento, informará a la Secretaría Técnica.

SEXTO. Notifíquese la presente resolución a la persona recurrente en el medio señalado para tal efecto y al sujeto obligado en términos de Ley.

Así lo acordó, en Sesión Ordinaria celebrada el once de enero de dos mil veintitrés, por **unanimidad de votos**, de los integrantes del Pleno del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, integrado por las Comisionadas y los Comisionados Ciudadanos, que firman al calce, ante Hugo Erik Zertuche Guerrero, Secretario Técnico, de conformidad con lo dispuesto en el artículo 15, fracción IX del Reglamento Interior de este Instituto, para todos los efectos legales a que haya lugar.

MSD/MJPS/LIEZ

ARÍSTIDES RODRIGO GUERRERO GARCÍA
COMISIONADO PRESIDENTE

JULIO CÉSAR BONILLA GUTIÉRREZ
COMISIONADO CIUDADANO

LAURA LIZETTE ENRÍQUEZ RODRÍGUEZ
COMISIONADA CIUDADANA

MARÍA DEL CARMEN NAVA POLINA
COMISIONADA CIUDADANA

MARINA ALICIA SAN MARTÍN REBOLLOSO
COMISIONADA CIUDADANA

HUGO ERIK ZERTUCHE GUERRERO
SECRETARIO TÉCNICO