COMITÉ DE TRANSPARENCIA

MX09.INFODF/6/CT/11.25/2021

ACTA DE LA CUARTA SESIÓN EXTRAORDINARIA DEL COMITÉ DE TRANSPARENCIA DEL INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA, PROTECCIÓN DE DATOS PERSONALES Y RENDICIÓN DE CUENTAS DE LA CIUDAD DE MÉXICO.

En la Ciudad de México, a 02 de septiembre de 2021, siendo las diecisiete horas, se reunió de manera remota por medio de la Plataforma "Microsoft Teams" el Comité de Transparencia del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, para celebrar la Cuarta Sesión Extraordinaria, encontrándose presentes los siguientes:

1. Hugo Erik Zertuche Guerrero, Secretario Técnico del Instituto. Presidente del Comité
2. Andrés Israel Rodríguez Ramírez, Responsable de la Unidad de Transparencia. Integrante
3. Yessica Paloma Báez Benítez, Directora de Asuntos Jurídicos. Integrante
4. Aarón Romero Espinosa, Órgano Interno de Control. Integrante
5. Gabriela Ángela Magdaleno del Río. Dirección de Datos Personales. Integrante
6. Arturo Iván Arteaga Huertero, Subdirector de Unidad de Transparencia, Información Pública y Datos Personales. Secretario Técnico del Comité
7. Raúl Llanos Samaniego, Director de Comunicación Social. Invitado
8. Hiriam Eduardo Pérez Vidal, Director de Tecnologías de Información. Invitado
9. Armando Tadeo Terán Ongay, Director de Vinculación y Proyección Estratégica. Invitado
10. Aldo Antonio Trapero Maldonado, Dirección de Estado Abierto, Estudios y Evaluación. Invitado
11. Brenda Trujillo Velázquez, Subdirectora de Archivos Institucionales. Invitada Permanente

I. **Lista de asistencia y verificación de quórum.** Una vez que quedó comprobada la asistencia de los integrantes del Comité de Transparencia, el Presidente declaró la existencia de quórum legal para sesionar.

II. **Lectura y, en su caso, aprobación del orden del día.** Acto seguido, el presidente del Comité sometió a consideración de sus integrantes, la siguiente Orden del Día:

1. Pase de lista y verificación del quórum legal.
2. Lectura, discusión y en su caso, aprobación del orden del día.
3. Análisis de las solicitudes de información con folio 3100000142221 y 3100000143221, con las respectivas propuestas de respuesta por parte de las diversas unidades administrativas de este Instituto.
4. Análisis de la solicitud de información con folio 3100000143321, con las respectivas propuestas de respuesta por parte de las diversas unidades administrativas de este Instituto.
5. Cierre de la sesión.

Por unanimidad de votos se aprobó el Orden del Día.

Desahogo del numeral tres del Orden del Día

AIRR/AIAH

3. Presentación, análisis y en su caso aprobación de las solicitudes de información con folio 3100000142221 y 3100000143221, con las respectivas propuestas de clasificación y respuesta por parte de las diversas unidades administrativas de este Instituto.

Antecedentes:

Los días 20 y 23 de agosto del presente año, el Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México recibió, a través del sistema Infomex las solicitudes con número de folio 3100000142221 y 3100000143221 respectivamente, donde solicitaron lo siguiente:

Solicitud con folio 3100000142221.

"Solicito el documento donde consten los roles y obligaciones respecto al tratamiento de datos personales"

Solicitud con folio 3100000143221.

"1. Solicito la versión pública del documento de seguridad de su sujeto obligado, en cumplimiento de lo establecido en el artículo 3, fracción XIV y 35 de la LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS. 2. Solicito copia del documento que contenga las políticas internas para la gestión y tratamiento de los datos personales emitidas o implementadas por su sujeto obligado, en cumplimiento del artículo 33 de la LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS. Requiero que la información antes descrita me sea entregada a través de la Plataforma Nacional de Transparencia o en caso de sobrepasar la capacidad de la misma, me sea proporcionada mediante correo electrónico o nube de almacenamiento. Al correo electrónico jesusdominguezl(arroba)outlook.com"

En consecuencia, la Unidad de Transparencia identificó que ambas solicitudes hacen referencia a los Documentos de Seguridad que poseen y detentan diversas Unidades Administrativas, por lo que turnó las solicitudes a cada Unidad, tal y como lo establece el artículo 211 de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México. Las Unidades Administrativas del Instituto consideraron que parte de la información solicitada, cumplía los criterios para considerarse información reservada, por lo que solicitaron al Comité del Instituto el estudio de la propuesta a fin de confirmar, modificar o revocar la clasificación propuesta.

Una vez planteados los antecedentes, el presidente del Comité cedió la palabra, a las personas titulares de las Unidades Administrativas, promoventes de las propuestas de clasificación en la modalidad de confidencial, quienes expusieron sus argumentos en el orden siguiente:

Participación. Hiriam Eduardo Pérez Vidal, Director de Tecnologías de Información:

- Estamos proponiendo una versión pública, reservando algunas partes del documento de seguridad en el sentido de que, su posible exposición, podría poner un riesgo de perjuicio toda vez que podría ir exponer información técnica que sea susceptible de vulnerabilidades aprovechadas para un ataque informático y que en consecuencia pudiese exponer la operación del sistema de infomex afectando el ejercicio de los derechos

principalmente arco y de acceso pero los datos personales de los solicitantes que se encuentren allí expuestos.-

Participación. Yessica Paloma Báez Benítez, Directora de Asuntos Jurídicos:

- Respecto a la unidad administrativa que corresponde a nosotros, respecto al sistema de datos personales nosotros estamos proponiendo la clasificación de la información como reservada, en este caso restringida en su calidad de modalidad reservada y evidentemente en nuestra propia ley de transparencia de la Ciudad de México en cuanto a acceso a la información pública y que están contenidas en el artículo 183 fracciones uno y tercero de nuestro marco normativo.

En ese sentido me permito de alguna manera como enlistar, los apartados que conforman el documento de seguridad de este sistema de datos personales, entre ellos el nombre de quien elaboró y de quien aprobó, la responsabilidad en la elaboración de este documento de seguridad, las medidas de seguridad, el catálogo de las formas de almacenamiento, las funciones y obligaciones de las personas que intervienen en este documento de seguridad, el registro de las incidencias, la identificación y autentificación, el control de acceso, gestión de soportes y copias de respaldo y por último, el análisis de riesgo, el de brecha, la responsabilidad de seguridad, el registro de acceso y los mecanismos de monitoreo, son los elementos mínimos que debe incluir un documento de seguridad para nosotros preservar el tema de los datos personales contenidos en estos sistemas.

Me permitiré solamente, hacer alusión respecto al sistema de datos personales de esta unidad administrativa que tengo a mi cargo, en nuestro caso son cuatro puntos importantes el primero es que los elementos contenidos en el listado anterior, pues evidentemente constituyen información confidencial, por tanto, nosotros como sujeto obligado estamos detectando impedidos para nosotros proporcionar esa información. Lo solicitado forma parte de los documentos de seguridad que contiene información que puede poner en riesgo la vida, la seguridad o la salud de una persona, en este caso no solamente lo relativo a los datos personales, sino también, lo relativo a la información que nosotros consideramos este puede poner alguna operación en cuanto procesos que nosotros llevamos como la parte contenciosa y representación legal del Instituto como sujeto obligado, entonces se considera de una forma que si nosotros revelamos esta información pues puede haber perjuicio respecto de si esta información se libera, por lo tanto viene la clasificación y lo único que proponemos en el plazo de la reserva los 2 años que también la propia ley de transparencia lo permite y sería de alguna manera como los cuatro puntos importantes relativos a la prueba de daño que se adjunta a continuación.-

Participación. Aarón Romero Espinosa, Órgano Interno de Control:

-Nos sumamos en el mismo sentido a la Dirección de Asuntos Jurídicos, el mismo tema de generar una versión pública de estas estos 3 documentos en el caso del órgano interno de control con la información clasificada como reservada igual en el 183 fracciones 1 y 2 de la ley de transparencia y también realizamos una prueba de daño en la prueba de daño quiero hacer énfasis en el tema de la divulgación, en nuestro punto de vista superaría este el interés público general este de perjuicio que supondría la divulgación supera el interés público general de que se difunda, sobre todo porque estos documentos de seguridad contienen el ABC de cómo protegemos en el tema de datos personales por lo tanto considero que gente hay un este ejercicio que supera el beneficio de divulgarlo y es por eso que hemos presentado en anexo 3 documentos de seguridad relativos a una versión, con la que ponemos a consideración de ustedes para que podamos responder con una versión pública.-

AIRR/AIAH

Participación. Raúl Llanos Samaniego, Director de Comunicación Social:

-Nosotros también someteremos a Comité nuestro documento de seguridad, en el mismo sentido que se ha presentado hasta ahora.

Participación. Armando Tadeo Terán Ongay, Director de Vinculación y Proyección Estratégica:

-Al analizar la información inherente a los documentos de seguridad, igualmente, consideramos que es necesario que la información se clasifica como reservada, dado que dar a conocer esta información podría vulnerar, poner en riesgo los datos de la información que recabamos.

Recabamos información de los concursos, es un requisito indispensable para participar e identificar a las personas y esa información la tenemos que resguardar en términos de la normativa aplicable y es por eso, por lo que en el mismo sentido, solicitamos que la información sea Clasificada y reservada.-

Participación. Hugo Erik Zertuche Guerrero, Secretario Técnico:

-La Secretaría Técnica somete a consideración de los integrantes de ese comité, el documento de seguridad que detenta, pues el mismo contiene información susceptible de ser Clasificada como reservada de conformidad con lo establecido en el artículo 183 fracciones primera y tercera de la ley de transparencia de la Ciudad de México, pues se considera que entregar la información pondría en riesgo la seguridad de diversos servidores públicos o bien entorpecer las actividades de esta unidad, por lo que se propone establecer un plazo de reserva de 2 años.

Al finalizar la Participación de los promoventes, se recapitulo y enlistaron los Documentos de Seguridad, cuya propuesta de clasificación en la modalidad de reservada se sometió a consideración del Comité. Los documentos referidos se muestran a continuación a manera de tabla.

UNIDAD ADMINISTRATIVA	NOMBRE DEL DOCUMENTO DE SEGURIDAD	NÚMERO DE FOJAS
SECRETARÍA EJECUTIVA	DOCUMENTO DE SEGURIDAD DEL SISTEMA DE DATOS PERSONALES DE LOS SERVICIOS DE ORIENTACIÓN, ASESORÍA Y SEGUIMIENTO DEL CENTRO DE ATENCIÓN TELEFÓNICA TEL-INFO	65
UNIDAD DE TRANSPARENCIA	DOCUMENTO DE SEGURIDAD DEL SISTEMA DE DATOS PERSONALES DEL REGISTRO DE BENEFICIARIOS DE LOS PROGRAMAS DE VINCULACIÓN CON LA SOCIEDAD CIVIL PARA EL ACCESO A LA INFORMACIÓN PÚBLICA Y LA PROTECCIÓN DE DATOS PERSONALES EN EL DISTRITO FEDERAL.	63
DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS	DOCUMENTO DE SEGURIDAD DEL SISTEMA DE DATOS PERSONALES DE LOS RECURSOS HUMANOS	81

DIRECCIÓN DE ASUNTOS JURÍCOS	DOCUMENTO DE SEGURIDAD DEL SISTEMA DE DATOS PERSONALES RELATIVO A LOS EXPEDIENTES CONFORMADOS POR LA DIRECCIÓN DE ASUNTOS JURÍDICOS CON MOTIVO DE LOS PROCESOS CONTENCIOSOS EN LOS QUE EL INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y RENDICIÓN DE CUENTAS DE LA CIUDAD DE MÉXICO FORMA PARTE.	119
DIRECCIÓN DE DATOS PERSONALES	DOCUMENTO DE SEGURIDAD DEL SISTEMA DE DATOS PERSONALES DE LOS EXPEDIENTES RELATIVOS A LAS VISITAS DE INSPECCIÓN EN MATERIA DE DATOS PERSONALES • DOCUMENTO DE SEGURIDAD DEL SISTEMA DE DATOS PERSONALES DE LOS EXPEDIENTES RELATIVOS A LAS SOLICITUDES DE INVESTIGACIÓN REALIZADAS POR EL PRESUNTO INCUMPLIMIENTO A LA LEY DE PROTECCIÓN DE DATOS EN POSESIÓN DE SUJETOS OBLIGADOS DE LA CIUDAD DE MÉXICO. DOCUMENTO DE SEGURIDAD DEL SISTEMA DE DATOS PERSONALES DE LOS EXPEDIENTES RELATIVOS AL PROCEDIMIENTO DE VERIFICACIÓN REALIZADO EN CUMPLIMIENTO A LO ESTABLECIDO EN EL ARTÍCULO 112 FRACCIÓN IV DE LA LEY DE PROTECCIÓN DE DATOS EN POSESIÓN DE SUJETOS OBLIGADOS DE LA CIUDAD DE MÉXICO.	195
DIRECCIÓN DE COMUNICACIÓN SOCIAL	DOCUMENTO DE SEGURIDAD DEL SISTEMA DE DATOS PERSONALES DE LA ENTREGA DE MATERIALES DE DIFUSIÓN	70
DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN	SISTEMA DE DATOS PERSONALES DEL SISTEMA INFOMEX	59
DIRECCIÓN DE VINCULACIÓN Y PROYECCIÓN ESTRATÉGICA	DOCUMENTO DE SEGURIDAD DEL SISTEMA DE DATOS PERSONALES DE LOS PARTICIPANTES EN CONCURSOS ORGANIZADOS POR EL INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA, PROTECCIÓN DE DATOS PERSONALES Y RENDICIÓN DE CUENTAS DE LA CIUDAD DE MÉXICO	5
ÓRGANO INTERNO DE	DOCUMENTO DE SEGURIDAD DEL SISTEMA DE DATOS	

CONTROL	PERSONALES SOBRE DECLARACIONES PATRIMONIALES Y DE CONFLICTO DE INTERESES DE LOS SERVIDORES PÚBLICOS DEL INFODF DOCUMENTO DE SEGURIDAD DEL SISTEMA DE DATOS PERSONALES DE LOS EXPEDIENTES RELATIVOS A QUEJAS, DENUNCIAS, PROCEDIMIENTOS ADMINISTRATIVOS DE RESPONSABILIDAD, RECURSOS DE REVOCACIÓN E INCONFORMIDADES, SUSTANCIADOS POR LA CONTRALORÍA DEL INSTITUTO DE ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DEL DISTRITO FEDERAL. DOCUMENTO DE SEGURIDAD DEL SISTEMA DE DATOS PERSONALES DE ACTAS DE ENTREGA RECEPCIÓN DE LOS RECURSOS DEL INSTITUTO DE ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DEL DISTRITO FEDERAL.	135
SECRETARÍA TÉCNICA	DOCUMENTO DE SEGURIDAD DEL SISTEMA DE DATOS PERSONALES RELATIVOS A RECURSOS DE REVISIÓN, REVOCACIÓN, RECUSACIÓN, DENUNCIAS Y ESCRITOS INTERPUESTOS ANTE EL INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA, PROTECCIÓN DE DATOS PERSONALES Y RENDICIÓN DE CUENTAS DE LA CIUDAD DE MÉXICO.	62

Así mismo, las Unidades Administrativas presentaron la siguiente Prueba de Daño, con la finalidad de dar cabal cumplimiento a lo establecido en los artículos 173 y 174 de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México.

PRUEBA DE DAÑO
LA DIVULGACIÓN DE LA INFORMACIÓN REPRESENTA UN RIESGO REAL, DEMOSTRABLE E IDENTIFICABLE DE PERJUICIO SIGNIFICATIVO AL INTERÉS PÚBLICO.
En vista de que los **documentos de seguridad enlistados en el cuerpo de la presente, contienen datos que**

pueden poner en riesgo la vida, seguridad o salud de una persona, o bien, obstruir la prevención o persecución de un delito, se considera que el otorgar acceso a los datos enlistados, representa un riesgo real e identificable, pues causaría una afectación al interés público permitir acceder a dicha información.

En ese sentido, debe reiterarse que de la lectura del **artículo 183, fracciones I y III,** de la Ley de citada, se advierte que el legislador local considera que sería mayor el daño ocasionado al revelar información en donde se pueda **poner en riesgo la vida, seguridad o salud de una persona, o bien, obstruir la prevención o persecución de un delito.**

EL RIESGO DE PERJUICIO QUE SUPONDRÍA LA DIVULGACIÓN SUPERA EL INTERÉS PÚBLICO GENERAL DE QUE SE DIFUNDA.

Este supuesto se justifica, toda vez que lo solicitado forma parte de **documentos de seguridad**, en donde se contiene información que puede **poner en riesgo la vida, seguridad o salud de una persona, o bien, obstruir la prevención o persecución de un delito.** y por ello, se actualiza las causales establecidas en las fracciones **I y III**, del artículo 183 de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México, ya que de dar a conocer dicha información se pondría en riesgo el principio de **Confidencialidad**, puesto que 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 de 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.

Dicho en otras palabras, se considera que el beneficio que pudiera provocar la revelación del contenido de los **documentos de seguridad enlistados en el cuerpo de la presente,** al público en general, lesionaría la integridad de las personas involucradas, así como la secrecía en el resguardo de la información sensible.

LA LIMITACIÓN SE ADECUA AL PRINCIPIO DE PROPORCIONALIDAD Y REPRESENTA EL MEDIO MENOS RESTRICTIVO DISPONIBLE PARA EVITAR EL PERJUICIO.

Este supuesto se justifica, debido a que la reserva de la información, representa el medio menos restrictivo disponible para evitar el perjuicio a las personas que actúan dentro de los **documentos de seguridad enlistados en el cuerpo de la presente,** siendo proporcional al hecho de que, la integridad de las personas involucradas, así como la debida protección a la información sensible, es mayor a la de su divulgación a través del acceso a la información pública.

Plazo de Reserva

El plazo de reserva que se **fija es de DOS AÑOS**, pero, en caso de que desaparezca la causa que motivó la reserva, la información que ahora se reserva se considerará pública de conformidad con lo dispuesto por el artículo 171, de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México, debiendo protegerse en todo caso la información confidencial que pudiera tener.

Partes del documento que se reservan, y autoridad responsable de su conservación, guarda y custodia.

Los documentos que se reservan es la parte del **documento de seguridad de mérito que a continuación se enlistan:**

1. Nombre de quien elaboró y de quien aprobó
2. Responsable de la elaboración del documento de seguridad
3. Medidas de seguridad
4. Catálogo de las formas de almacenamiento
5. Funciones y obligaciones de las personas que intervengan en el tratamiento de los sistemas de datos personales
6. Registro de incidencias
7. Identificación y autentificación
8. Control de acceso, gestión de soportes y copias de respaldo y recuperación
9. Análisis de riesgos
10. Análisis de brecha

11. Responsable de seguridad
12. Registro de acceso y telecomunicaciones
13. Mecanismos de monitoreo y revisión de las medidas de seguridad
14. Plan de trabajo

Los cuales se encuentran en custodia de las Unidades Administrativas del Instituto de Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México.

Una vez realizadas las exposiciones por parte de los titulares de las Unidades Administrativas promoventes, y al no haber participaciones, el presidente considero a los integrantes del Comité de Transparencia del Instituto sobre el Proyecto de Clasificación de la información en su carácter de reservada, por un plazo de 2 años, por lo que instruyó al Secretario Técnico del Comité someter a votación la propuesta, el proyecto se aprobó por unanimidad a través del acuerdo 004/SE/CT-02-09-2021.

IV. Desahogo del numeral cuatro del Orden del Día

4. Análisis de la solicitud de información con folio 3100000143321, con las respectivas propuestas de respuesta por parte de las diversas unidades administrativas de este Instituto.

Antecedentes:

El día 23 de agosto del presente año, el Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México recibió a través del sistema Infomex la solicitud de Folio 3100000143321, en donde se solicitó lo siguiente:

"Buen día, Desde la integración del Pleno actual a la fecha, requiero, todos los correos electrónicos enviados y recibidos desde y en las cuentas de correo electrónico institucional de todo el personal de la institución, lo anterior, con fundamento en el criterio 06/2021, aprobado en la 12a. Sesión Ordinaria del Pleno del INFO CDMX.
Favor de hacerlos llegar en carpeta comprimida por cada persona servidora pública, mediante los correos electrónicos necesarios.
Gracias."

En consecuencia, la Unidad de Transparencia, turnó la solicitud a las Unidades Administrativas correspondientes, tal y como lo establece el artículo 211 de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México. Las Unidades Administrativas del Instituto consideraron que parte de la información solicitada, cumplía los criterios para considerarse información confidencial, por lo que solicitaron al Comité del Instituto que estudiara la propuesta a fin de confirmar, modificar o revocar la clasificación propuesta.

Una vez planteados los antecedentes, el presidente del Comité cedió la palabra, a las personas titulares de las Unidades Administrativas, promoventes de las propuestas de clasificación en la modalidad de confidencial, quienes expusieron sus argumentos en el orden siguiente:

Participación. Aarón Romero Espinosa, Órgano Interno de Control:

-Después de la búsqueda exhaustiva, por parte de cada una de las personas servidoras públicas adscritas a la Unidad Administrativa, identificaron que los correos solicitados contienen Datos Personales, por tanto, son sujetos a estudio, por lo que se propone al Comité la clasificación de estos en su modalidad de confidencial, el Inventario de datos personales a clasificar como confidencial, que propone esta Unidad Administrativa es el siguiente:

· CORREO ELECTRÓNICO PERSONAL

· NOMBRE DE PERSONA DENUNCIANTE

· NOMBRE DE PERSONA QUEJOSA

· NOMBRE DE PERSONA SOLICITANTE

· DOMICILIO

· FIRMA

· EDAD

· NACIONALIDAD

· HUELLA DACTILAR

· CURP

· RFC

· TELÉFONO CELULAR

· TELÉFONO PARTICULAR

· DATOS LABORALES

· DATOS CLÍNICOS

· DATOS ACADÉMICOS

· IDENTIFICACIONES PARTICULARES

Así como información relativa al acceso del sistema electrónico de declaraciones declara infoDF, conflicto de interés, clave de elector y procedimientos administrativos abiertos -

Participación. Yessica Paloma Báez Benítez, Directora de Asuntos Jurídicos:

-Después de la búsqueda exhaustiva, por parte de cada una de las personas servidoras públicas adscritas a la Unidad Administrativa, identificaron que los correos solicitados contienen Datos Personales, por tanto, son sujetos a estudio, por lo que se propone al Comité la clasificación de estos en su modalidad de confidencial, el Inventario de datos personales a clasificar como confidencial, que propone esta Unidad Administrativa es el siguiente:

AIRR/AIAH

· NOMBRE

· CORREO ELECTRÓNICO

· DOMICILIO

· FIRMA

· IDENTIFICACIÓN OFICIAL

· EDAD

· NACIONALIDAD

· HUELLA DACTILAR DE PARTICULARES

Esa sería la lista por parte de la dirección de asuntos jurídicos muchas gracias. -

Participación. Armando Tadeo Terán Ongay, Director de Vinculación y Proyección Estratégica:

-Después de la búsqueda exhaustiva, por parte de cada una de las personas servidoras públicas adscritas a la Unidad Administrativa, identificaron que los correos solicitados contienen Datos Personales, por tanto, son sujetos a estudio, por lo que se propone al Comité la clasificación de estos en su modalidad de confidencial, el Inventario de datos personales a clasificar como confidencial, que propone esta Unidad Administrativa es el siguiente:

· NOMBRE

· CORREOS ELECTRÓNICOS DE

· DOMICILIO

· NACIONALIDAD

· EDAD TODOS

· TELÉFONO

· RFC

· CURP

Sería nuestra propuesta de clasificación de Datos-

Participación. Aldo Antonio Trapero Maldonado, Dirección de Estado Abierto, Estudios y Evaluación.

-Después de la búsqueda exhaustiva, por parte de cada una de las personas servidoras públicas adscritas a la Unidad Administrativa, identificaron que los correos solicitados contienen Datos Personales, por tanto, son sujetos a estudio, por lo que se propone al Comité la clasificación de estos en su modalidad de confidencial, el Inventario de datos personales a clasificar como confidencial, que propone esta Unidad Administrativa es el siguiente:

· NOMBRE

· EDAD

· SEXO

· CURP

· RFC

· CÉDULAS

· DIRECCIONES ELECTRÓNICAS PRIVADAS

· DIRECCIONES PARTICULARES DE DOMICILIO

· CORREOS Y

· TELÉFONOS PRIVADOS

Son los Datos que identificamos en Estado Abierto.

Participación. Raúl Llanos Samaniego, Director de Comunicación Social:

-En nuestro caso del análisis que se hizo, tenemos nosotros esta postura de clasificar como confidencial, por los correos que nosotros tenemos:

· NOMBRE DE LOS REPORTEROS Y REPORTERAS

· CORREO ELECTRÓNICO PERSONAL

· NÚMEROS TELEFÓNICOS PERSONALES

Básicamente son los datos que encontramos-

Participación. Andrés Israel Rodríguez Ramírez, Responsable de la Unidad de Transparencia:

-El fundamento es artículo 186 de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México y derivado de una búsqueda y análisis de información que se encontró en los correos electrónicos de esta Secretaría Ejecutiva y de la Unidad de Transparencia un total de 41,806 correos electrónicos, mismos que debido, al análisis realizado se detectó que contaban con diversa información susceptible de clasificarse como confidencial en este momento, por contener:

www.infodf.org.mx La Morena No. 865, Col. Narvarte, Alcaldía Benito Juárez, C.P. 03020 Tel. +52 (55) 5636-2120

NOMBRE DE LA PERSONA SOLICITANTE, NOMBRE DE LA PERSONA RECURRENTE, NOMBRE DE LA PERSONA DENUNCIANTE, CORREO ELECTRÓNICO PERSONAL, DOMICILIO, FIRMA, EDAD, NACIONALIDAD, HUELLA DACTILAR DE LOS PARTICULARES, CURP, RFC, TELÉFONO CELULAR, TELÉFONO PARTICULAR, CLAVE DE ELECTOR, ASÍ COMO FOTOGRAFÍAS DE PARTICULARES.

Los datos anteriores tanto en las solicitudes de información, documentos anexos y complementarios, así como en Recursos de Revisión, sus documentos anexos y complementarios.

Estos serían los datos que estamos sometiendo a consideración de este Comité de Transparencia, para que se clasifiquen como confidenciales y poder elaborar la versión pública por correo electrónico en su momento, para garantizar la debida protección de los datos y poder hacer la entrega de la información.-

Participación. Hugo Erik Zertuche Guerrero, Secretario Técnico:

-Por lo que hace esta Secretaría Técnica detectamos en las cuentas de correo institucional de los servidores públicos adscritos a esta unidad, así como en las de las comisionadas y los comisionados ciudadanos y sus equipos de trabajo los siguientes datos: CORREOS DE PARTICULARES, NOMBRE DE PERSONAS FÍSICAS, CONTRASEÑAS, TELÉFONOS DE PARTICULARES, FOTOGRAFÍA, FIRMA DE PARTICULARES, COPIA DIGITAL DE LA CREDENCIAL PARA VOTAR EXPEDIDA POR EL INE DE PARTICULARES, ACTAS DE NACIMIENTO, ACTA DE DEFUNCIÓN DE PARTICULARES, NÚMERO DE CUENTA BANCARIA, DOMICILIO Y SEXO.

Una vez realizadas las exposiciones por parte de los titulares de las Unidades Administrativas promoventes, y al no haber participaciones, el presidente considero a los integrantes del Comité de Transparencia del Instituto sobre el Proyecto de Clasificación de la información en su carácter de confidencial, por lo que instruyó al Secretario Técnico del Comité someter a votación la propuesta, el proyecto se aprobó por unanimidad a través del acuerdo 005/SE/CT-02-09-2021.

Con relación a la misma solicitud (Folio 3100000143321), las Direcciones de Datos Personales y Tecnologías de Información sometieron a consideración del Comité de Transparencia de este Instituto, la RESERVA PARCIAL de la información atendiendo a la necesidad de dar respuesta a dicha solicitud.

Por lo que el Presidente del Comité les concedió la palabra a las personas Titulares de ambas Direcciones, expusieron lo siguiente:

Participación. Gabriela Ángela Magdaleno del Río. Dirección de Datos Personales

-La justificación por la cual estamos sometiendo a reservas algunos correos de los integrantes de la dirección de datos personales, algunos correos de la dirección, tienen información sobre las verificaciones que pueden iniciarse de oficio cuando el Instituto cuenta con indicios que hagan presumir fundada y motivada la existencia de violaciones a las leyes correspondientes, por denuncia del titular cuando considere que ha sido afectado, por actos del responsable que puedan ser contrarios a lo dispuesto por la presión de ley y demás normativa aplicable, por cualquier persona cuando tenga conocimiento de presuntos incumplimientos a las obligaciones previstas en la presente ley y demás disposiciones que resulten aplicables en la materia y para verificar el cumplimiento de los principios, el tratamiento de los datos personales y la gestión de los sistemas de datos personales en posesión del responsable, para tal efecto el Instituto presenta un programa anual de verificación esto establecido en el artículo 112 de la ley de datos personales de la Ciudad de México por lo cual particularmente en los correos hay datos sobre, el nombre del sujeto obligado, el número de sistemas de datos personales, la justificación de la verificación, las medidas de seguridad, asimismo, como los nombres de los denunciantes y sus correos personales.

AIRR/AIAH

La Dirección de Protección de Datos Personales presentó la siguiente prueba de daño:

Por lo que refiere al cumplimento de la atribución prevista en las fracciones V y VII del artículo 25 de del Reglamento Interior, los servidores públicos adscritos a la Dirección de Datos Personales han enviado y recibido correos electrónicos a través de sus cuentas institucionales, con información que da cuenta de las evaluaciones del cumplimiento de los sujetos obligados respecto de las obligaciones previstas en la Ley de Datos local derivado del Programa Anual de Verificaciones 2019, 2020 y 2021 o en su caso de la atención de las verificaciones que se realizan con motivo de las denuncias presentadas por particulares. Esta información contiene: el nombre de los sujetos obligados, el ámbito al que pertenecen, el número de sistemas que detentan, la fecha estimada del desarrollo de las actividades programadas, la justificación de la verificación a cada sujeto obligado programado, la descripción de la verificación y el objeto de la verificación.

En ese orden de ideas, las acciones antes mencionadas se encuentran protegidas bajo los siguientes sistemas de datos personales:

- Sistema de datos personales de los expedientes relativos a las solicitudes de investigación realizadas por el presunto incumplimiento a la Ley de Protección de Datos en Posesión de Sujetos Obligados de la Ciudad de México.

- Sistema de datos personales de los expedientes relativos al procedimiento de la Ley de protección de Datos en Posesión de Sujetos Obligados de la Ciudad de México" en la gaceta oficial de la ciudad de México

Por lo anterior, en caso de poner a disposición la información concerniente de los anexos del Programa Anual de Verificaciones 2021 se revelarían los sujetos obligados que están programados para verificación. Además, las verificaciones de este programa no han sido concluidas, situación que pudiera obstruir las actividades proyectadas.

Así como también, el conocer la información relacionada con el desarrollo de estas, revelaría los puntos débiles de los sujetos obligados, lo que propiciaría una vulneración a la integridad y seguridad de sus sistemas de datos personales, vulnerando a las personas titulares de estos datos.

Lo anterior encuadra en lo establecido en el artículo 183, fracción II, de la Ley de Transparencia local, el cual establece que podrá clasificarse como información reservada aquella que obstruya las actividades de verificación, inspección y auditoría relativas al cumplimiento de las leyes.

Asimismo, se estaría bajo los supuestos que establece el artículo 31 de la Ley de Datos local, referente a las vulneraciones que pueden sufrir los sujetos obligados respecto de los sistemas que detentan, el cual establece:

> *Artículo 31. Además de las que señalen las leyes respectivas y la normatividad aplicable, se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:*
>
> *I. La pérdida o destrucción no autorizada;*
> *II. El robo, extravío o copia no autorizada;*

AIRR/AIAH

III. El uso, acceso o tratamiento no autorizado; o
IV. El daño, la alteración o modificación no autorizada."

Por lo que refiere a la información que revela los mecanismos implementados por los sujetos obligados verificados para la adecuada ejecución de las medidas de seguridad, se estima que la difusión de la información referida en el párrafo anterior actualiza lo dispuesto en el artículo 183, fracción III, de la Ley de Transparencia local, a saber:

> ***Artículo 183.*** *Como información reservada podrá clasificarse aquella cuya publicación: (…)*
> *III. Obstruya la prevención o persecución de los delitos; (…)"*

Así como lo que se establece en el artículo 3, fracciones XXII, XXIII, XXIV y XXV, de la Ley de Datos local, referente a las medidas de seguridad que deben adoptar los responsables de sistemas de datos personales para garantizar el adecuado tratamiento de los datos de carácter personal que tienen en su poder, cito:

> *"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: […]*
> *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*

www.infodf.org.mx La Morena No. 865, Col. Narvarte, Alcaldía Benito Juárez, C.P. 03020 Tel. +52 (55) 5636-2120

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

Lo anterior es así, dado que la información contenida en los correos electrónicos de las cuentas institucionales del personal de la Dirección de Datos Personales, contienen información sobre la descripción de los procesos, las fases o las actividades operativas de los sistemas que tienen en su posesión los sujetos obligados verificados que involucran el tratamiento de datos personales, la tecnología que utilizan para efectuar el tratamiento, las medidas de seguridad físicas, técnicas o administrativas y la identificación, el análisis y las observaciones de la gestión de los sistemas de datos personales.

Asimismo, se considera que para obstruir la prevención de los delitos es necesario que la divulgación de la información afecte las acciones de las autoridades encargadas de la procuración de seguridad y prevención del delito, limitando la capacidad de éstas, supuesto que encuadra en el cumplimiento de los principios rectores, establecidos en el artículo 9 de la Ley de Datos local, principalmente el de confidencialidad y licitud, como se describen:

Artículo 9. El responsable del tratamiento de Datos Personales deberá observar los principios de:
[…]
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.
[…]
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."

Al respecto, el artículo 213 del Código Penal para el Distrito Federal contempla que comete el delito de revelación de secretos el que sin consentimiento de quien tenga derecho a otorgarlo y en perjuicio de alguien, revele un secreto o comunicación reservada, que por cualquier forma haya conocido o se le haya confiado, o lo emplee en provecho propio o ajeno.

Por su parte, el artículo 223 del Código Penal para el Distrito Federal establece que comete delito de robo respecto de documentos que se conserven en oficinas públicas, cuando la sustracción afecte el servicio público o cause daño a terceros. Si el delito lo comete un servidor público que labore en la dependencia donde cometió el robo, se le impondrá, además, destitución e inhabilitación de uno a cinco años para desempeñar otro empleo, cargo o comisión públicos.

En ese sentido, esta Dirección considera que el acceso a la información que detenta y procesa esta unidad administrativa, y que se encuentra contenida en el correo institucional de su personal, podría revelar aspectos privados de cada sujeto obligado como puede ser: el espacio físico en el que se encuentran custodiados los datos personales de cada uno de los sistemas de datos personales, así como revelar alguna brecha en la infraestructura tecnológica de los sistemas informáticos de los sujetos obligados verificados. No cual podría derivar en la comisión de alguno de los delitos referidos, dando como resultado la afectación al ejercicio de las atribuciones de dichos sujetos obligados y, de manera indirecta, afectar los derechos fundamentales de las personas que forman parte de los sistemas de datos personales de los responsables.

AIRR/AIAH

De igual forma, es de relevancia precisar que a pesar de que algunos de los procedimientos de verificación ya han concluido, estos se encuentran aún en etapa de seguimiento de las observaciones determinadas, o recomendaciones que el Pleno determina, las cuales no han sido solventadas de acuerdo con los plazos y términos establecidos.

En ese sentido, de conformidad con lo dispuesto por el artículo 183, fracción IV, de la Ley de Transparencia local, podrá clasificarse como información reservada aquella cuya publicación contenga opiniones, recomendaciones o puntos de vista que formen parte del proceso deliberativo de las personas servidoras públicas, hasta en tanto no sea emitida la decisión definitiva, cito:

"***Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México***

> ***Artículo 183.*** *Como información reservada podrá clasificarse aquella cuya publicación: (…)*
> ***IV.*** *La que contenga las opiniones, recomendaciones o puntos de vista que formen parte del proceso deliberativo de las personas servidoras públicas, hasta en tanto no sea emitida la decisión definitiva, la cual deberá estar documentada;*
> *(…)"*

En ese sentido se actualiza el supuesto establecido en el artículo 183, fracción IV, de la Ley de Transparencia local, ya que al acceder a la información que contienen los documentos generados respecto de los procedimientos y verificaciones que esta Dirección realiza, revelaría opiniones, recomendaciones y puntos de vista

Ahora bien, se informa que en cumplimento a la atribución prevista en la fracción XVIII del artículo 25 del Reglamento Interior los servidores públicos adscritos a la Dirección de Datos Personales han enviado y recibido correos electrónicos a través de sus cuentas institucionales, los cuales contienen información sobre procedimientos de verificación derivados de una investigación previa, de los cuales no se ha emitido la resolución correspondiente por el Pleno de este Instituto.

Ahora bien, lo anteriormente expuesto se deriva del cumplimiento de lo que establecen los artículos 79 fracciones VIII, IX, XVI, XIX y XXI; 112 de la Ley de Datos local:

> *Artículo 79. El Instituto tendrá las siguientes atribuciones:*
> *[…]*
> *VIII. Hacer del conocimiento de las autoridades competentes, la probable responsabilidad derivada del incumplimiento de las obligaciones previstas en la presente Ley y en las demás disposiciones que resulten aplicables;*
> *IX. Vigilar, en el ámbito de su competencia, el cumplimiento de la presente Ley y demás disposiciones que resulten aplicables en la materia;*
> *[…]*
> *XVI. Realizar el registro de los sistemas de datos personales en posesión de los sujetos obligados de la Ciudad de México;*
> *[…]*
> *XIX. Verificar el registro y los mecanismos para garantizar los niveles de seguridad aplicables a los sistemas de datos personales en posesión de los sujetos obligados; […]*
> *XXI. Evaluar las políticas, acciones y el cumplimiento de los principios de la presente Ley por parte de los responsables, mediante la verificación periódica;*

Artículo 112. La verificación podrá iniciarse:

I. De oficio cuando el Instituto cuenten con indicios que hagan presumir fundada y motivada la existencia de violaciones a las leyes correspondientes,
II. Por denuncia del titular cuando considere que ha sido afectado por actos del responsable que puedan ser contrarios a lo dispuesto por la presente Ley y demás normativa aplicable,
III. Por cualquier persona cuando tenga conocimiento de presuntos incumplimientos a las obligaciones previstas en la presente Ley y demás disposiciones que resulten aplicables en la materia;
IV. Para verificar el cumplimiento de los principios, el tratamiento de los datos personales y la gestión de los sistemas de datos personales en posesión del responsable, para tal efecto el Instituto presentará un programa anual de verificación.

La denuncia establecida en la fracción II del presente artículo, se resolverá de conformidad con el Procedimiento que para tal efecto emita el Instituto.

El derecho a presentar una denuncia precluye en el término de un año contado a partir del día siguiente en que se realicen los hechos u omisiones materia de la misma.

Cuando los hechos u omisiones deriven de un acto reiterado, el término empezará a contar a partir del día hábil siguiente al último hecho realizado.

La verificación no procederá en los supuestos de procedencia del recurso de revisión previstos en la presente Ley.

Para el programa anual de verificación el Instituto presentará en el primer trimestre de cada año el programa de verificación y los puntos a verificar."

Asimismo, de la información que genera esta Dirección, existe aquella que da cuenta de algunos procedimientos que ya cuentan con la correspondiente resolución del Pleno. Sin embargo, no han causado ejecutoria. Lo cual refiere al supuesto establecido en el artículo 183, fracción VII, de la Ley de Transparencia local, respecto de que podrá clasificarse como información reservada aquella que trate de expedientes judiciales o de los procedimientos administrativos seguidos en forma de juicio, mientras la sentencia o resolución de fondo no haya causado ejecutoria.

"***Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México***

Artículo 183. *Como información reservada podrá clasificarse aquella cuya publicación: (…)*
VII. Cuando se trate de expedientes judiciales o de los procedimientos administrativos seguidos en forma de juicio, mientras la sentencia o resolución de fondo no haya causado ejecutoria. Una vez que dicha resolución cause estado los expedientes serán públicos, salvo la información reservada o confidencial que pudiera contener;
(…)"

En ese sentido se advierte que resulta inviable el acceso en cualquier modalidad a la información que genera y detenta esta Dirección de Datos Personales, ya que puede vulnerar de manera significativa el quehacer de los responsables de sistemas de datos personales, así como, poner en riesgo la vida,

www.infodf.org.mx La Morena No. 865, Col. Narvarte, Alcaldía Benito Juárez, C.P. 03020 Tel. +52 (55) 5636-2120

seguridad o salud de una persona física, por estar directamente relacionado con las medidas de seguridad de la información de los sistemas, o vulnerar el ejercicio de sus derechos, al no guardar confidencialidad respecto de los procesos que se llevan a cabo.

Por lo anteriormente expuesto se solicita, someter a consideración del Comité de Transparencia de este Instituto la presente solicitud por parte de la Dirección de Datos Personales, atendiendo a la necesidad de dar respuesta a la solicitud de información pública con número de folio 3100000143321, por un **PLAZO DE RESERVA de 3 años con ampliación a 2 años más** de acuerdo a lo que establece el artículo 171 de la Ley de Transparencia local, siendo la autoridad responsable de la conservación, guarda y custodia esta Dirección de Datos Personales del Instituto de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México-

Participación. Hiriam Eduardo Pérez Vidal, Director de Tecnologías de Información:

- Las personas servidoras públicas adscritas a esta Dirección de Tecnologías de Información, reservamos exclusivamente aquellos que pudiesen contener claves de usuario y contraseñas de acceso a los sistemas que están custodiados por esta dirección, las claves y licencias de software otorgadas a las personas servidoras públicas y a los sujetos obligados en su caso los códigos de activación de licenciamiento de la infraestructura tecnológica y de los mecanismos de seguridad que cuenta el centro de procesamiento de datos incluyendo la parte de los accesos que se pudiesen dar a los proveedores de tecnologías y servicios, los diagramas técnicos que soportan nuestra infraestructura tecnológica y seguridad, los datos y claves de activación de nuestra estructura tecnológica, las visitas de monitoreo de la infraestructura y de sus sistemas, así como las claves de usuario y contraseña de todos los componentes de nuestra infraestructura; con fundamento en el artículo 183 fracción III

Es importante mencionar que estamos reservando sólo aquellos correos que pudiesen contener esta información, toda vez que su fusión podría exponer posibles vulnerabilidades, información técnica que pudiesen ser aprovechadas por un ataque informático, para exponer la operación de los sistemas institucionales, la seguridad de las infraestructuras y lo que devenga finalmente en el ejercicio de los derechos de acceso tutelados por esta institución se propone un plazo de reserva de 3 años, así mismo se pone a consideración de los Integrantes, la presente prueba de daño:

Reservada	Fundamento
Claves de usuario y contraseñas, de acceso a los sistemas institucionales que los sujetos obligados requieren a esta Dirección de Tecnologías de la Información, derivados de la rotación de personal, y el cual brinda acceso a Sistemas de Datos Personales para el tratamiento de Solicitudes de Información y Recursos de Revisión.	Artículo 183, fracción III Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México.
Claves y Licencias de uso de software,	Artículo 183, fracción III Ley de

www.infodf.org.mx La Morena No. 865, Col. Narvarte, Alcaldía Benito Juárez, C.P. 03020 Tel. +52 (55) 5636-2120

Reservada	Fundamento
otorgadas a las personas servidoras públicas del Instituto.	Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México.
Códigos de activación del licenciamiento de infraestructura tecnológica y de seguridad con que cuenta el Instituto en su Centro de Procesamiento de Datos, que son proporcionados por los Proveedores de servicios.	Artículo 183, fracción III Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México.
Diagramas y datos técnicos que soportan la infraestructura tecnológica y su seguridad.	Artículo 183, fracción III Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México.
Datos y claves de activación de elementos de la infraestructura tecnológica, que habilita servicios a las personas servidoras públicas del Instituto y los Sujetos Obligados	Artículo 183, fracción III Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México.
Bitácoras de monitoreo de la infraestructura tecnológica y de sistemas.	Artículo 183, fracción III Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México.
Claves de usuario y contraseñas, de acceso a la infraestructura tecnológica.	Artículo 183, fracción III Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México.

El presidente considero a los integrantes del Comité de Transparencia del Instituto sobre el Proyecto de Acta e instruyó al Secretario Técnico del Comité someter a votación la propuesta, al no haber participaciones u observaciones, el proyecto se aprobó por unanimidad mediante ACUERDO 006/SE/CT-02-09-2021, se confirmó la solicitud de reserva, por un plazo de 3 años de aquella información que podría vulnerar la seguridad informática del Instituto o poner en riesgo a las personas servidoras públicas en sus labores.

Desahogo del numeral cinco del Orden del Día

V. Asuntos Generales

En el Orden del Día no se enlistó ningún asunto general. Por lo tanto, y no habiendo otro asunto que tratar, se dio por concluida la Cuarta Sesión Extraordinaria del Comité de Transparencia de este Instituto a las diecisiete horas con treinta y seis minutos del dos de septiembre del dos mil veintiuno.

Firman al calce y al margen los que en ella intervinieron

Hugo Erik Zertuche Guerrero

Secretario Técnico del Instituto
Presidente del Comité

Andrés Israel Rodríguez Ramírez

Responsable de la Unidad de Transparencia
Integrante

Yessica Paloma Báez Benítez

Directora de Asuntos Jurídicos

Integrante

Aarón Romero Espinosa

Órgano Interno de Control Integrante

Integrante

AIRR/AIAH

COMITÉ DE TRANSPARENCIA

MX09.INFODF/6/CT/11.25/2021

Gabriela Ángela Magdaleno del Río

Dirección de Datos Personales

Integrante

Arturo Iván Arteaga Huertero

Subdirector de Unidad de Transparencia, Información Pública y Datos Personales

Secretario Técnico del Comité

Raúl Llanos Samaniego

Director de Comunicación Social

Invitado

Brenda Trujillo Velázquez

Subdirectora de Archivos Institucionales

Invitada Permanente

Armando Tadeo Terán Ongay

Director de Vinculación y Proyección Estratégica

Invitado

Hiriam Eduardo Pérez Vidal

Director de Tecnologías de Información

Invitado

Aldo Antonio Trapero Maldonado

Director de Estado Abierto Estudios y Evaluación

Invitado

AIRR/AIAH

www.infodf.org.mx La Morena No. 865, Col. Narvarte, Alcaldía Benito Juárez, C.P. 03020 Tel. +52 (55) 5636-2120