Comité de Transparencia

CT-0026-2022

Ciudad de México, a 04 de mayo de 2022

Visto: Para resolver el expediente **CT-026-2022**, respecto a la propuesta de reserva parcial, presentada por la Unidad de Transparencia, y, en su caso la aprobación de la versión pública del Documento de Seguridad de Aeropuertos y Servicios Auxiliares, para cumplimiento a las obligaciones señaladas en los artículos 247 y 248 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

ANTECEDENTES

I. Con fecha veintiséis de enero de dos mil dieciocho, se publicó en el Diario Oficial de la Federación el Acuerdo mediante el cual se aprueban los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

De conformidad con lo dispuesto en el artículo 3 de los citados Lineamientos, se advierte que los mismos son aplicables a este Organismo, Aeropuertos y Servicios Auxiliares, en su calidad de Sujeto Obligado, en los siguientes términos:

"Ámbito de validez subjetivo
Artículo 3. *Los presentes Lineamientos generales serán aplicables a cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, fideicomisos y fondos públicos, del ámbito federal y partidos políticos que en el ejercicio de sus atribuciones y funciones lleven a cabo tratamientos de datos personales de personas físicas, en términos de lo dispuesto en la Ley General y los presentes Lineamientos generales, así como al Instituto y los organismos garantes en lo que respecta a la sustanciación de los recursos de inconformidad.*

Los fideicomisos y fondos públicos del orden federal considerados como entidades paraestatales, de conformidad con la legislación aplicable, deberán dar cumplimiento por sí mismos a las obligaciones previstas en la Ley General y los presentes Lineamientos generales, a través de sus propias áreas.
..."

II. El veinticinco de noviembre de dos mil veinte, se publicó en el Diario Oficial de la Federación, el Acuerdo mediante el cual se aprueba la adición de un Título Décimo a los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Conforme a los artículos 247, 248 y 250 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, Aeropuertos y Servicios Auxiliares deberá contar con un apartado virtual de protección de datos personales y se someterá a los instrumentos técnicos que emita el Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales mediante los cuales verificarán el desempeño respecto al cumplimiento de las obligaciones previstas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, dichos preceptos legales a la letra disponen lo siguiente:

> *"Instrumentos técnicos de evaluación* ***Artículo 247****.*
> *El Instituto aprobará los Instrumentos Técnicos de Evaluación que sean necesarios para medir el desempeño de los responsables respecto al cumplimiento de las obligaciones previstas en la Ley General y demás disposiciones aplicables en la materia los cuales contemplarán, al menos, el tipo de evaluación, la metodología, los criterios, formatos y los indicadores de cumplimiento que permitan la realización del ejercicio evaluación que corresponda.*
>
> *Obligatoriedad de los instrumentos técnicos de evaluación*
> ***Artículo 248****. El cumplimiento de las disposiciones contenidas en los instrumentos técnicos de evaluación es obligatorio para los responsables del ámbito federal a que se refiere el artículo 1 de los presentes Lineamientos generales.*
>
> *Apartado virtual de Protección de Datos Personales en los sitios de Internet de los responsables*
> ***Artículo 250****. Los responsables deberán habilitar en su portal de Internet, un apartado denominado "Protección de datos personales", el cual debe contar cuando menos, con el o los avisos de privacidad integrales aplicables a los tratamientos de datos del sujeto obligado, datos de contacto de la Unidad de Transparencia, así como en su caso, Oficial de Protección de Datos, e información relevante en materia de protección de datos personales. La publicación en dicho apartado podrá servir a los responsables como un medio para acreditar el cumplimiento de sus obligaciones en materia de protección de datos personales, de conformidad con lo dispuesto en los artículos 16, 45, 54, 72, 107 Y 118 de los presentes Lineamientos generales. Dicho apartado será el medio idóneo que servirá a los responsables para rendir cuentas a los titulares y al Instituto sobre el*

tratamiento de los datos personales en su posesión, permitiendo evaluar el cumplimiento de los principios, deberes y obligaciones; atendiendo a la obligatoriedad que les corresponde como responsables, en términos de lo previsto en los artículos 26, 29 Y 30 de la Ley General. Este apartado será repositorio también, de los medios de verificación documentales q e se utilicen en los ejercicios de evaluación, cuyas características y contenido se establece en los instrumentos técnicos de evaluación y en el Programa Anual, respectivamente.

La información contenida en dicho apartado deberá estar disponible de forma permanente y actualizarse conforme lo determinen los criterios contenidos en los instrumentos técnicos de evaluación."

III. Con fecha veintiséis de noviembre de dos mil veintiuno, se publicó en el Diario Oficial de la Federación, el ACUERDO mediante el cual se aprueban los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Conforme a la "*Metodología, criterios, formatos e indicadores en materia de evaluación del desempeño de los responsables respecto al cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones que resulten aplicables en la materia*", publicado en el citado acuerdo por el cual se aprueban los Instrumentos Técnicos; el **Documento de Seguridad** deberá publicarse en el Apartado de Protección de Datos Personales del Portal de ASA, específicamente en la sección denominada "Información relevante en materia de protección de datos personales", al respecto en el formato 2.1 de dicha metodología, el cual se denomina: "*Deber de seguridad*", se señala lo siguiente:

Ejercicio (año) del que se presenta la información		(AAAA)
Fecha de publicación de la información		(DD/MM/AAAA)
Fecha de la última actualización		(DD/MM/AAAA)
No.	**Criterio**	**Medio de verificación**
1.	Hipervínculo a la **versión pública** del documento de seguridad del responsable, testando únicamente lo relativo al plan de trabajo que contiene, además, el análisis de riesgo y brecha **Por ningún motivo debe incluirse en este apartado el documento de seguridad integro con el que cuenta el responsable. El documento de seguridad deberá**	

	publicarse protegiendo el plan de trabajo, el análisis de riesgo y el análisis de brecha respectivos; lo que implica que en caso de que se dejen visibles, sin excepción, será considerado como incumplimiento al presente criterio	
2.	Hipervínculo al documento que contiene las políticas internas de gestión y tratamiento de los datos personales	

IV. Con fecha veintiséis de marzo de dos mil veintidós, mediante correo electrónico se envió una consulta al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, para conocer si era necesario omitir el plan de trabajo, análisis de riesgo y análisis de brecha del Documento de Seguridad y cuál sería el fundamento o motivo para solicitar al Comité de Transparencia la reserva de la información.

V. Con fecha primero de abril de dos mil veintidós, se recibió la respuesta del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, en los siguientes términos:

En primer lugar, agradecemos en nombre de la Dirección General de Evaluación, Investigación y Verificación su interés para el cumplimiento de la implementación del Título Décimo de los Lineamientos Generales, así como de las disposiciones contenidas en los instrumentos técnicos de evaluación.

Sobre la consulta que señala en su comunicación electrónica, me permito indicar que el Pleno de este Instituto ya se ha pronunciado en diversas ocasiones en relación con la posibilidad de entregar en versión pública el documento de seguridad, por lo cual a continuación se le presenta una tabla que pudiera ser de ayuda para ese sujeto obligado, considerando el contenido que pudiera tener el documento de seguridad de ese sujeto obligado.

Al respecto en los asuntos señalados a modo de ejemplo, se modifica la clasificación invocada por los sujetos obligados y se ordena la entrega de dicho documento, al tenor de las consideraciones:

RECURSO	SOLICITUD	RESPUESTA	SENTIDO Y ALCANCE
RRA 2462/21	"Solicito la versión pública de todos los documentos, en formato de datos abiertos, que contengan los	Clasificación con fundamento en lo dispuesto por los artículos	**MODIFICAR** la respuesta emitida por el ente recurrido, e instruirle a efecto de que entregue al particular **versión pública** del documento de seguridad peticionado, **testando**

Secretaría de Agricultura y Desarrollo Social	análisis de riesgos y/o reportes de riesgos en los sistemas protección de datos personales con que este Sujeto Obligado cuenta..."	110, fracciones I y V de la LFTAIP y 113, fracciones I y V, de la LGTAIP	**únicamente lo relativo a al plan de trabajo que contiene, además, el análisis de riesgo y brecha del documento de seguridad**, lo anterior con fundamento en el **artículo 110, fracción VII.**
RRA 6431/20 Centro Nacional de Equidad de Género y Salud Reproductiva	"Solicito el documento de seguridad (en su caso, la versión pública) establecido en el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. En caso de que la respuesta rebase los límites de carga de la Plataforma Nacional de Transparencia, se requiere se remita al correo electrónico descrito en la solicitud de mérito."	Clasificación con fundamento en el artículo **110, fracciones I, V y VII de la LFTAIP**	**Modifica** y ordena la entrega de la **versión pública** del documento, en el que sólo deberá testarse, con fundamento en lo dispuesto por el **artículo 110 fracción VII de la LFTAIP**, lo relativo al **plan de trabajo que contiene, además, el análisis de riesgo y brecha del documento de seguridad.**

No omito señalar que ambos precedentes fueron votados por unanimidad y en los mismos términos; es decir, el mismo fundamento de clasificación y con plena coincidencia respecto a los elementos que deben ser testados de la versión pública que se ordena entregar, a saber: plan de trabajo del documento y el análisis de riesgo y brecha del instrumento.

Por otro lado, cabe destacar que la precisión establecida en el Documento Técnico de Evaluación referente al testado del plan de trabajo, así como de los análisis de riesgo y brecha, respectivamente; obedece a que, generalmente, los responsables incluyen

información técnica sensible relativa a sus sistemas de gestión en los Documentos de seguridad lo que en la práctica, podría implicar la vulnerabilidad de dichos sistemas y, específicamente de los datos personales en posesión del sujeto obligado; no obstante, si teniendo en consideración lo anterior, a juicio del responsable considera que las versiones con las que cuenta son publicables de manera íntegra y, por tanto, no se encuentran en el supuesto de vulnerabilidad referido, puede publicarlos sin necesidad de testarlo.

Sin embargo, si ese sujeto obligado considera que en efecto la información contenida en su documento de seguridad es de carácter clasificado, deberá atender lo establecido en el artículo 140 de la Ley Federal de Transparencia y Acceso a la Información Pública, el cual señala que, en caso de que los sujetos obligados consideren que los documentos o la información requerida deban ser clasificados, deberá seguirse el procedimiento previsto en el Capítulo I del Título Séptimo de la Ley General, que se refiere al procedimiento de acceso a la información.

En ese sentido, el área deberá remitir la solicitud, así como un escrito en el que funde y motive la clasificación al Comité de Transparencia, mismo que deberá resolver para:

a) Confirmar la clasificación;
b) Modificar la clasificación y, otorgar total o parcialmente el acceso a la información, o
c) Revocar la clasificación y conceder el acceso a la información.
... [sic]

VI. Con fecha dieciocho de abril de dos mil veintidós, la Unidad de Transparencia recibió la petición de la **Unidad de Transparencia**, mediante oficio ASA/B121/0158/2022 , para poner a consideración del Comité de Transparencia **el Documento de Seguridad en Versión Pública**, que deberá publicarse en el Apartado Virtual de Protección de Datos Personales del Organismo, para lo cual resulta necesario que dicho Órgano colegiado confirme su clasificación como parcialmente reservada y apruebe su versión pública. Para lo cual remite un análisis y la respectiva prueba de daño de conformidad con el artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública.

VII. La Prueba de daño referida en el antecedente VI, se presentó en los siguientes términos:

"Con fundamento en los artículos 103 y 104 de la Ley General de Transparencia y Acceso a la Información Pública, y 102 de la Ley Federal de Transparencia y Acceso a la Información Pública; si bien a través del derecho de acceso la información previsto en el

artículo 6, Apartado A, fracción 1 constitucional, así como en la Ley General de Transparencia y Acceso a la Información Pública; cualquier persona puede tener acceso a la información en posesión de los sujetos obligados, existen determinadas restricciones al respecto, mismas que se refieren a la Información reservada y a la información confidencial.

En este punto resulta importante destacar lo siguiente:

- *El **análisis de riesgos** contiene entre otros, los requerimientos regulatorios, el valor de los datos personales que son tratados, su ciclo de vida y el valor y exposición de los activos involucrados en el tratamiento de los mismos.*

- *El **análisis de brecha** contiene información relativa a las medidas de seguridad existentes, las faltantes, y las nuevas que pudieran remplazar a uno o más controles implementados actualmente.*

- *Y el **Plan de Trabajo** describe cronológicamente las acciones de seguridad a implementar en el organismo señalando las medidas de seguridad más relevantes y urgentes a establecer, es decir las vulnerabilidades de ASA en la materia.*

Por lo que publicar la información referida colocaría al Organismo en un estado de vulnerabilidad en cuanto a las medidas de seguridad de los datos personales que posee, permitiendo el acceso ilícito a sus sistemas y equipos informáticos, facilitando:

a. Accesos no autorizados a los sistemas.
b. Robos de información.
c. Suplantación de identidades.

En ese sentido, el riesgo de publicar la información referida cumple con los supuestos jurídicos de reserva en los siguientes términos:

- ***La divulgación de la información representa un potencial riesgo real, demostrable e identificable.***

El riesgo es **real**, puesto que ASA efectivamente trata datos personales y en ese sentido, de conformidad con lo que establece el artículo de la Ley General de Protección de Datos Personales en Posesión de los sujetos Obligados, deberá establecer y mantener las medidas de seguridad que permitan proteger los datos personales, contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado.

Es **demostrable**, a través de dos mecanismos, a) la revisión de los sistemas, bases de datos y archivos físicos o digitales que obran en el Organismo y que contienen los datos personales de los trabajadores, colaboradores, usuarios y proveedores de este Organismo. b) la normativa que regula su tratamiento, tal es el caso de la Ley General de Transparencia y Acceso a la Información Pública y la Ley General de Protección de Datos Personales en Posesión de Particulares.

Y es **identificable** porque no se trata de datos personales genéricos o abstractos, sino que los mismos existen efectivamente en los archivos de este Organismo, los cuales se localizan en Avenida 602, Núm. 161, Col. Zona Federal Aeropuerto Internacional Ciudad de México, C.P. 15620, Alcaldía Venustiano Carranza, CDMX.

- ***El riesgo de perjuicio que supondría la divulgación supera al interés público.***

Aeropuertos y Servicios Auxiliares como sujeto obligado, acorde al artículo 31 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, tiene por objeto esencial 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.

La difusión del análisis de riesgo, análisis de brecha y plan de trabajo del Documento de Seguridad, ocasionaría un perjuicio irreversible en cuanto a la protección de los datos personales que posee, máxime que si bien es cierto que, de conformidad con el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados no se advierte que dichos documentos contengan datos personales, lo cierto es que el proporcionar los mismos, ocasionaría que una persona ajena a al Organismo, pudiera tener acceso a los datos personales almacenados en los sistemas tecnológicos, como podrían ser los datos personales de los trabajadores, licitantes y educandos, vulnerando así el derecho humano .denominado, derecho a la intimidad que es aquel que tiene toda persona a ser protegida respecto de injerencias arbitrarias en su vida privada, su familia, su domicilio, sus posesiones o su correspondencia.

El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda la información, ya que el resguardo del plan de trabajo que contiene, además, el análisis de riesgo y brecha del Documento de Seguridad con que cuenta el Sujeto Obligado, implica llevar a cabo acciones de prevención de diversos delitos tipificados en el Código Penal Federal (accesos no autorizados a los sistemas, robos de información, suplantación de identidades), lo cual cobra importancia si se considera que dichas conductas implican

vulnerar las medidas de seguridad de los datos personales que posee, motivo por el cual se considera que la limitación propuesta, se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio.

En ese sentido, divulgar la información referida vulneraría el derecho humano de la intimidad de muchas personas, y generaría desconfianza, incertidumbre y minaría la legitimidad del Estado Mexicano para solicitar y tratar datos personales, perjuicios superiores para el interés público, al que puede tener un ciudadano en acceder a los datos personales ajenos.

- ***La limitación se adecua al principio de proporcionalidad.***

La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir las conductas antijurídicas tipificadas (accesos no autorizados a los sistemas, robos de información, suplantación de identidades), mismas que de llevarse a cabo podrían permitir la realización de diversos ataques a la infraestructura tecnológica y de sistemas que lo integran, con la consecuencia directa de la violación al principio de responsabilidad.

De acuerdo con el principio de proporcionalidad; tenemos que la restricción (reserva) al derecho de acceso a la información, tiene como fin legítimo y regulado jurídicamente, de la preservación del interés público, de acuerdo con lo previsto en el artículo 6, Apartado A. constitucional. En el caso concreto, este fin legitimo se refiere a la obstrucción de la prevención de delitos, lo cual obedece precisamente a la necesidad de su salvaguarda.

Esta restricción es la idónea, en virtud de que constituye la única medida posible para proteger las medidas de seguridad de los datos personales bajo resguardo de este Organismo y con ello, el interés público, además de que no vulnera el derecho de acceso a la información pública de los ciudadanos.

Es necesario que la información relativa al análisis de riesgo, análisis de brecha y Plan de Trabajo de los datos personales de este Organismo, este fuera del conocimiento público, a efecto de no vulnerar su protección, por lo que tal reserva se protege el interés público. De acuerdo con el principio de proporcionalidad el riesgo que podría traer la divulgación de la información, es mayor que el interés público de que se difunda, por lo que en este caso debe prevalecer la reserva de información, puesto que ello representa el medio menos restrictivo disponible para evitar un perjuicio al interés público.

Asimismo, la limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir las conductas antijurídicas tipificadas (accesos no autorizados a los sistemas, robos de información, suplantación de identidades), mismas que de llevarse a cabo podrían permitir la realización de diversos ataques a la infraestructura tecnológica y de sistemas que lo integran, con la consecuencia directa de la violación al principio de responsabilidad.

Así de conformidad con señalado en el artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, se concluye que la difusión de la información implicaría un riesgo real, demostrable e identificable que obstruiría la prevención de delitos relacionados con las medidas de seguridad de los datos personales bajo resguardo de este Organismo.

Por lo antes expuesto, se considera que es procedente que se confirmé la clasificación de información reservada, por un periodo de **cinco años**, por parte del Comité de Transparencia, con fundamento en los artículos 113, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública, y 110 fracción VIII de la Ley Federal de Transparencia y Acceso a la Información Pública.
... [sic]

Derivado del análisis de la información proporcionada por la Unidad de Transparencia, se pudo advertir que, el documento de Seguridad contiene información susceptible de reservarse. Lo anterior de conformidad con lo dispuesto en los artículos 113, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública, y 110 fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública. Por lo que:

CONSIDERANDO

1. Que la Unidad de Transparencia, solicita la aprobación de la versión pública del Documento de Seguridad con la reserva de la información contenida en los análisis de riesgos, análisis de brecha y plan de trabajo los cuales están contenidos en los anexos 02-A, 02-B, 03 y el Capítulo V del Documento de Seguridad. Mediante el cual se expone que la negativa del acceso a dicha información se motiva en evitar o prevenir la comisión del delito al vulnerar las medidas de seguridad de este Organismo con relación a los datos personales.

2. Que la divulgación de la información contenida en el análisis de riego, análisis de brecha y plan de trabajo, colocaría al Organismo en un estado de vulnerabilidad en cuanto a las medidas de seguridad de los datos personales que posee, permitiendo el acceso ilícito a sus sistemas y equipos informáticos, facilitando los accesos no autorizados a los sistemas; robos de información y suplantación de identidades.

3. Que el riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda la información, ya que el resguardo del plan de trabajo que contiene, además, el análisis de riesgo y brecha del Documento de Seguridad con que cuenta el Sujeto Obligado, implica llevar a cabo acciones de prevención de diversos delitos tipificados en el Código Penal Federal (accesos no autorizados a los sistemas, robos de información, suplantación de identidades), lo cual cobra importancia si se considera que dichas conductas implican vulnerar las medidas de seguridad de los datos personales que posee.

4. Que la Ley General de Transparencia y Acceso a la Información Pública, dispone en sus artículos 68 fracción VI, y 113 fracción VII, en torno al caso que nos ocupa, lo siguiente:

"**Artículo 68.** Los sujetos obligados serán responsables de los datos personales en su posesión y, en relación con éstos, deberán:

...

VI. Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado.

Los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información de acuerdo a la normatividad aplicable. Lo anterior, sin perjuicio a lo establecido por el artículo 120 de esta Ley.

...

Artículo 113. Como información reservada podrá clasificarse aquella cuya publicación:

...

VII. Obstruya la prevención o persecución de los delitos.

..."

5. Que el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a Información Pública, a la letra dice:

"**Artículo 110.** Conforme a lo dispuesto por el artículo 113 de la Ley General como información reservada podrá clasificarse aquella cuya publicación:

...

VII. Obstruya la prevención o persecución de los delitos.

..."

Que el lineamiento Vigésimo sexto, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, a la letra señala:

"Vigésimo sexto. De conformidad con el artículo 113, fracción VII de la Ley General, podrá considerarse como información reservada, aquella que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos.
..."

6. Que la publicación de la información del análisis de riesgo y el análisis de brecha sobre las medidas de seguridad para la protección de datos personales podría implicar una vulneración a dichas medidas. La divulgación podría obstruir la prevención de los delitos, conforme al citado artículo 211 Bis 2 del Código Penal Federal, el cual a la letra dice:

"**Artículo 211 bis 2.-** Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá, además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.
..."
La publicación de la información del análisis de riesgo y el análisis de brecha sobre las medidas de seguridad para la protección de datos personales podría implicar una vulneración a dichas medidas. Dicha divulgación podría obstruir la prevención de los delitos, conforme al citado artículo 211 Bis 2 del Código Penal Federal.

De este modo, se considera procedente la reserva del plan de trabajo que contiene, además, el análisis de riesgo y brecha del documento de seguridad de la Aeropuertos y Servicios Auxiliares, de conformidad con lo previsto en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Por lo expuesto y fundado se:

RESUELVE

ÚNICO. Una vez que se tuvo a la vista el expediente de mérito, los miembros de este Comité de Transparencia de Aeropuertos y Servicios Auxiliares, **CONFIRMAN LA RESERVA PARCIAL** de la información prevista en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública; 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública; y en el Lineamiento Sexto, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas, del Documento de Seguridad, particularmente por lo que hace a la información contenida en los Anexos 02-A Análisis de Riesgos, Anexo 02-B Análisis de Riesgos, Anexo 03 Análisis de Brecha y el Plan de Trabajo contenido en el capítulo V del Documento de Seguridad.

Así lo resolvieron por unanimidad los Miembros del Comité de Transparencia presentes; Joel Manríquez Novelo, Jefe de Área de Análisis de Factibilidad en suplencia del presidente del Comité de Transparencia con fundamento en el artículo 6 de los Lineamientos para el funcionamiento del Comité de Transparencia de Aeropuertos y Servicios Auxiliares, el Lic. Carlos Bravo Solís, Titular del Área de Quejas, Denuncias e Investigaciones, en suplencia de la Titular del Órgano Interno de Control en Aeropuertos y Servicios Auxiliares y el Ing. Mario Cesar Espejel Trujillo, encargado de la Jefatura de Almacén y Activo Fijo en suplencia de la Coordinadora de Archivos; con fundamento en los artículos 44, fracción II de la Ley General de Transparencia y Acceso a la Información Pública y 65, fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública.

Joel Manríquez Novelo
Jefe de Área de Análisis de Factibilidad en suplencia del Titular de la Unidad de Transparencia y Presidente del Comité de Transparencia

Lic. Carlos Bravo Solís
Titular del Área de Quejas, Denuncias e Investigaciones, en suplencia de la Titular del Órgano Interno de Control en Aeropuertos y Servicios Auxiliares

Ing. Mario Cesar Espejel Trujillo
Encargado de la Jefatura de Almacén y Activo Fijo en suplencia de la Coordinadora de Archivos

Esta hoja de firmas corresponde a la Resolución CT-0026-2022.