**CLASIFICACIÓN DE INFORMACIÓN CT-CI/A-2-2020**

**INSTANCIA REQUERIDA:**

SECRETARÍA DEL COMITÉ DE TRANSPARENCIA

Ciudad de México. Resolución del Comité de Transparencia de la Suprema Corte de Justicia de la Nación, correspondiente al once de marzo de dos mil veinte.

**A N T E C E D E N T E S:**

**I. Solicitud de información.** El siete de febrero de dos mil veinte, se recibió en la Plataforma Nacional de Transparencia la solicitud tramitada con el folio 0330000047120:

> *"Solicito el documento de seguridad (elaborado por dicha dependencia), establecido en el artículo 3, fracción XIV, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. En caso de que el mismo, no pase por el sistema, se solicita se envíe al correo electrónico descrito."*

**II. Acuerdo de admisión de la solicitud.** En acuerdo de doce de febrero de dos mil veinte, la Unidad General de Transparencia y Sistematización de la Información Judicial, por conducto de su Subdirector General, una vez analizada la naturaleza y contenido de la solicitud, con fundamento en los artículos 123 y 124, de la Ley General de Transparencia y Acceso a la Información Pública, 124 y 125, de la Ley Federal de Transparencia y Acceso a la Información Pública y 7 del Acuerdo General de Administración 5/2015, la estimó procedente y ordenó abrir el expediente UT-A/0096/2020 (foja 3).

**III. Requerimiento de información.** Por oficio UGTSIJ/TAIPDP/0520/2020, el doce de febrero de dos mil veinte, el Titular de la Unidad General de Transparencia y Sistematización de la Información

Judicial solicitó a la Secretaría del Comité de Transparencia de este Alto Tribunal se pronunciara sobre la existencia y clasificación de la información solicitada (fojas 4 y 5).

**IV. Respuesta de la Secretaría del Comité de Transparencia.** El diecisiete de febrero de dos mil veinte, se recibió en la Unidad General de Transparencia el oficio CT-205-2020, en el que se informó (foja 5):

> (…)
> *"En sesión de 11 de septiembre de 2019, el Comité de Transparencia aprobó el Documento de Seguridad de la Suprema Corte de Justicia de la Nación, en cuyo contenido se describe el tipo de datos personales que se recaban y su tratamiento, los niveles de riesgo por tratamiento y las posibles medidas para evitar el incorrecto tratamiento de los datos personales.*
>
> *Cabe destacar que el Documento de Seguridad contiene información estratégica para el diseño y la ejecución de las medidas de seguridad necesarias para proteger los datos personales que posee este Alto Tribunal, en particular, las mediciones sobre los riesgos latentes por cada tratamiento (Anexo 6), así como los resultados derivados del análisis de brecha (anexo 9). Dicha información, en esencia, refleja las prácticas de seguridad de la información con las que cuenta en ese momento el sujeto obligado y las que deberían de tenerse con base en las mejores prácticas.*
>
> *En ese sentido, se estima **reservar parcialmente** el Documento de Seguridad respecto de los resultados obtenidos en los niveles de riesgo identificado y el análisis de brecha, pues su divulgación implica un riesgo real, demostrable e identificable en perjuicio al interés público, que actualiza las **fracciones I y VIII del artículo 113 de la Ley General de Transparencia** y Acceso a la Información Pública en relación con las **fracciones I y VII del artículo 110 de la Ley Federal de Transparencia** y Acceso a la Información Pública, en particular, por comprometer la seguridad pública y la obstrucción a la prevención de delitos.*
>
> *En efecto, la sola divulgación de los niveles de riesgo identificados por cada tratamiento y el análisis de brecha reflejarían el grado de vulnerabilidad de la institución en materia de seguridad de la información, así como las capacidades institucionales de reacción para mitigar los riesgos.*
>
> *Por lo anterior, se elaboró la versión pública del Documento de Seguridad para que sea puesto a disposición del particular sin costo alguno. Como lo solicitó amablemente, se remite el presente informe con un anexo al correo electrónico que tuvo a bien señalar en su oficio de cuenta."*
> (…)

**V. Segundo informe de la Secretaría Técnica del Comité de Transparencia.** Mediante oficio CT-206-2020, el dieciocho de febrero de dos mil veinte, se informó (foja 7):

(…)
*"Adicionalmente a la aprobación del Documento de Seguridad en sesión de 11 de septiembre de 2019, el Comité de Transparencia aprobó el Plan de Trabajo en materia de protección de datos personales en sesión de 12 de noviembre de esa anualidad. El Plan de Trabajo, además de ser una herramienta complementaria y de instrumentación del Documento de Seguridad, es un programa que contiene las políticas y acciones institucionales enfocadas en aplicar las medidas de seguridad necesarias para el tratamiento de los datos personales que posee la Suprema Corte de Justicia de la Nación.*

*En ese sentido, se estima* ***reservar parcialmente*** *el Plan de Trabajo en materia de protección de datos personales respecto de las medidas de seguridad y su forma de ejecución pues su divulgación implica un riesgo real, demostrable e identificable en perjuicio del interés público, que actualiza* ***las fracciones I y VIII del artículo 113 de la Ley General de Transparencia*** *y Acceso a la Información Pública, en relación con* ***las fracciones I y VII del artículo 110 de la Ley Federal de Transparencia*** *y Acceso a la Información Pública, en particular, por comprometer la seguridad pública y la obstrucción a la prevención de delitos.*

*En efecto, la divulgación de la información referida vulneraría la seguridad informática de este Alto Tribunal, pues se genera la expectativa razonable de que ocurra un ataque intrusivo que pudiera inhabilitar el uso y funcionamiento de las medidas de seguridad implementadas, lo cual afectaría el desempeño de la función jurisdiccional y de las áreas administrativas, además de que se pondría en peligro la confidencialidad e integridad de los datos personales que posee la institución.*

*En consecuencia, se pone a disposición del solicitante la versión electrónica del Plan de Trabajo en materia de protección de datos personales, misma que se remite al correo electrónico que tuvo a bien señalar en su oficio de requerimiento."*

En el expediente, a foja 9, se encuentra glosado un sobre que identifica los anexos de los oficios CT-205-2020 y CT-206-2020.

**VI. Vista a la Secretaría del Comité de Transparencia.** El veinticinco de febrero de dos mil veinte, el Titular de la Unidad General de Transparencia y Sistematización de la Información Judicial, a través del oficio UGTSIJ/TAIPDP/0732/2020, remitió el expediente UT-A/0096/2020 a la Secretaría del Comité de Transparencia, con la finalidad de que se dictara la resolución correspondiente.

**VII. Acuerdo de turno.** En proveído de veinticinco de febrero de dos mil veinte, la Presidencia del Comité de Transparencia de este Alto Tribunal, con fundamento en los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública, 23, fracción II y 27, del Acuerdo General de Administración 5/2015, ordenó integrar el expediente **CT-CI/A-2-2020** y, conforme al turno correspondiente, remitirlo al Contralor de este Alto Tribunal, a fin de que presentara la propuesta de resolución, lo que se hizo mediante oficio CT-280-2020 el veintisiete de febrero de este año.

**VIII. Ampliación del plazo.** En sesión de veintiséis de febrero de dos mil veinte, este órgano colegiado autorizó la ampliación del plazo ordinario para dar respuesta en este asunto.

## C O N S I D E R A C I O N E S:

**PRIMERO. Competencia.** El Comité de Transparencia de la Suprema Corte de Justicia de la Nación es competente para conocer y resolver el presente asunto, en términos de lo dispuesto en los artículos 6°, de la Constitución Política de los Estados Unidos Mexicanos, 4 y 44, fracciones I, II y III, de la Ley General de Transparencia y Acceso a la Información Pública, 65, fracciones I, II y III, de la Ley Federal de Transparencia y Acceso a la Información Pública, así como 23, fracciones II y III, del Acuerdo General de Administración 5/2015.

**SEGUNDO. Análisis.** En la solicitud se pide el documento de seguridad que prevé el artículo 3, fracción XIV, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, elaborado por la Suprema Corte de Justicia de la Nación.

La Secretaría Técnica del Comité de Transparencia, en un primer informe, refiere que el Documento de Seguridad fue aprobado por este

Comité el once de septiembre de dos mil diecinueve, pero que contiene información estratégica para el diseño y la ejecución de las medidas de seguridad necesarias para proteger los datos personales que posee la Suprema Corte de Justicia de la Nación, en particular, los riesgos latentes por cada tratamiento y los resultados del análisis de brecha, por lo que clasifica como reservada esa información y, por tanto, de forma parcial el Documento de Seguridad, con apoyo en los artículos 113, fracciones I y VII (aun cuando en el informe se aludió a la fracción VIII), de la Ley General de Transparencia y el artículo 110, fracciones I y VII, de la Ley Federal de la materia.

En un segundo informe, la Secretaría del Comité de Transparencia se refiere al Plan de Trabajo en materia de protección de datos personales, aprobado en sesión de doce de noviembre de dos mil diecinueve, por este órgano colegiado, señalando que además de ser una herramienta complementaria y de instrumentación del Documento de Seguridad, es un programa que contiene las políticas y acciones institucionales para aplicar las medidas de seguridad necesarias para el tratamiento de datos personales, por lo que clasifica como información reservada las *"medidas de seguridad y su forma de ejecución"* del citado Plan, con apoyo en los artículos 113, fracciones I y VII (aunque en el informe se refiere a la fracción VIII), de la Ley General de Transparencia y 110, fracciones I y VII, de la Ley Federal de la materia.

De la revisión que se hace a la versión pública del Documento de Seguridad que se pone a disposición, se advierte que, efectivamente, los datos que se protegen corresponden a: "Nivel de riesgo latente por tratamiento" y "Análisis de brecha", respecto de las medidas recomendadas y las medidas implementadas en cada uno de los tratamientos de datos personales. Por su parte, la versión pública del Plan de Trabajo en materia

de protección de datos personales, se testan “las medidas de seguridad administrativas, físicas y técnicas –complementarias a las políticas de seguridad generales de la SCJN– para los tratamientos de datos personales en la institución” y su forma de ejecución.

Conforme a lo anterior, toca verificar si, en el caso, cabe o no la clasificación de parcialmente reservada que se hace del Documento de Seguridad y del Plan de Trabajo que propone la Secretaría Técnica del Comité de Transparencia, por estimar actualizadas las hipótesis contenidas en los artículos 113, fracciones I y VII de la Ley General de Transparencia, y 110, fracciones I y VII de la Ley Federal de la materia, los cuales establecen:

> *“**Artículo 113.** Como información reservada podrá clasificarse aquella cuya publicación:*
> *I. Comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable;*
> (…)
> *VII. Obstruya la prevención o persecución de los delitos;”*
> (…)
> *“**Artículo 110.** Conforme a lo dispuesto por el artículo 113 de la Ley General, como información reservada podrá clasificarse aquella cuya publicación:*
> *I. Comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable;*
> (…)
> *VII. Obstruya la prevención o persecución de los delitos;”*
> (…)

Sobre el alcance de la fracción I de los preceptos transcritos, de acuerdo con los *“Lineamientos generales en materia de clasificación y desclasificación de la información”*, punto Décimo octavo[1], se considera un riesgo a la seguridad pública la divulgación de aquella información que

[1] *“**Décimo octavo.** De conformidad con el artículo 113, fracción I de la Ley General, podrá considerarse como información reservada, aquella que comprometa la seguridad pública, al poner en peligro las funciones a cargo de la Federación, la Ciudad de México, los Estados y los Municipios, tendientes a preservar y resguardar la vida, la salud, la integridad y el ejercicio de los derechos de las personas, así como para el mantenimiento del orden público.*

*Se pone en peligro el orden público cuando la difusión de la información pueda entorpecer los sistemas de coordinación interinstitucional en materia de seguridad pública, menoscabar o dificultar las estrategias contra la evasión de reos; o menoscabar o limitar la capacidad de las autoridades encaminadas a disuadir o prevenir disturbios sociales.*

*Asimismo, podrá considerarse como reservada aquella que revele datos que pudieran ser aprovechados para conocer la capacidad de reacción de las instituciones encargadas de la seguridad pública, sus planes, estrategias, tecnología, información, sistemas de comunicaciones.*

pueda poner en riesgo las funciones a cargo de la Federación tendientes a preservar y resguardar la vida, la salud, la integridad y el ejercicio de los derechos de las personas.

Luego, sobre el alcance del artículo 110, fracción VII de la Ley Federal de Transparencia, cuyo contenido es idéntico al que hace referencia la Ley General de la materia en el artículo 113, fracción VII, se tiene presente lo resuelto por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales en el recurso de revisión RRA 10276/18, cumplimentada por este Comité en la resolución CT-CUM-R/A-2-2019, en la que se señaló que *"como información reservada podrá clasificarse aquella cuya publicación obstruya la prevención o persecución de delitos",* agregando que *"para que pueda acreditarse que la información requerida pudiera 'obstruir la prevención de los delitos', debe vincularse a la* ***afectación a 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"*** (página 98, vuelta de la resolución del recurso de revisión RRA 10276/18).

Además, se precisó que de esa causal de reserva se desprenden dos vertientes: una que se refiere a la prevención de los delitos y la otra a la persecución de los mismos, agregando: *"por definición de la palabra* ***prevención*** *se hace referencia a medidas y acciones dispuestas con anticipación con el fin de evitar o impedir que se presente un fenómeno peligroso para reducir sus efectos sobre la publicación",* de ahí que se considera prevención del delito *"tomar medidas y realizar acciones para evitar una conducta o un comportamiento que puedan dañar o convertir a la población en sujetos o víctimas de un ilícito"*, considerando que desde el punto de vista criminológico prevenir es *"conocer con anticipación la probabilidad de una conducta criminal disponiendo de los medios necesarios*

*para evitarla; es decir, no permitir que alguna situación llegue a darse porque ésta se estima inconveniente".*

En ese orden de ideas, se debe destacar que en el informe de la Secretaría Técnica de este Comité se señala, expresamente, que poner a disposición de manera íntegra, el Documento de Seguridad y el Plan de Trabajo en materia de protección de datos personales, implicaría dar a conocer los riesgos identificados en cada uno de los tratamientos de datos personales y que el "análisis de brecha" reflejaría el grado de vulnerabilidad de la Suprema Corte de Justicia de la Nación en materia de seguridad de la información.

Por lo anterior, este Comité de Transparencia estima necesario analizar cada uno de los documentos a la luz de las causales de reserva aludidas en la respuesta a la solicitud de información que nos ocupa.

Por lo que hace a la reserva de los apartados relativos a los resultados obtenidos en los niveles de riesgo identificado y el análisis de brecha del Documento de Seguridad este Comité considera acertado que se clasifique como reservada temporalmente esa información, en términos de la fracciones I y VII, del artículo 113 de la Ley General de Transparencia y 110, fracciones I y VII, de la Ley Federal de la materia, ya que de no reservarse, se vulnerarían las medidas de protección al divulgarse la información clasificada, generando la expectativa razonable de que ocurra un ataque intrusivo a las bases de datos personales en posesión de este Alto Tribunal, pudiendo, incluso, afectar el desempeño de la función jurisdiccional y de las áreas administrativas de este Alto Tribunal.

Esto es así, en tanto que el análisis de riesgo que se desarrolla en el Documento de Seguridad, identifica los diversos factores de riesgo a que están expuestos los tratamientos de datos personales y calcula el riesgo latente de cada uno de ellos; y, en el análisis de brecha, consiste en

identificar la distancia que existe entre las medidas recomendadas y las medidas implementadas por cada uno de los tratamientos reportados, cuyos resultados da sustento a las políticas y mecanismos institucionales en materia de protección de datos personales.

Por tanto, con la reserva se busca proteger la información y las bases de datos personales, evitando exponerlas a un ataque que pudiera conseguir vulnerarlas u obtenerlas para beneficiarse de ellas, lo que pondría en riesgo la privacidad de las personas titulares y podría ser causa de responsabilidad de la Suprema Corte de Justicia de la Nación, en términos de los deberes y las causas de incumplimiento de las obligaciones, especialmente de las vulneraciones previstas en los artículos 38 y 41 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Por lo tanto, su divulgación representa un riesgo real, demostrable e identificable de perjuicio significativo a la seguridad de la información y al derecho de protección de datos personales de los titulares de dicha información, ante lo cual no puede prevalecer el interés particular del peticionario, sino un interés mayor de proteger esa información.

A mayor abundamiento, se estima que se actualiza el supuesto de reserva previsto en la fracción I del artículo 113 de la Ley General de Transparencia, pues divulgar “los niveles de riesgo identificados” y “el análisis de brecha” contenidos tanto en el Documento de Seguridad, podría vulnerar el derecho a la protección de datos personales en posesión de la Suprema Corte de Justicia de la Nación, ya que se conocería el nivel y las medidas de protección implementadas por este Alto Tribunal para cada uno de los tratamientos de datos personales que se encuentran bajo su resguardo.

Por otro lado, divulgar el análisis de la brecha que existe entre las medidas de seguridad recomendadas y las que realmente se encuentran implementadas, reflejaría el grado de vulnerabilidad de la institución en materia de seguridad de la información, así como las capacidades institucionales de reacción para enfrentar el mal uso de los datos personales que se encuentran bajo resguardo de este Alto Tribunal, lo que actualiza el supuesto de reserva contenido en la fracción VII del artículo 113 de la citada Ley General de Transparencia.

Por lo que toca a la reserva de las “medidas de seguridad administrativas, física y técnicas” del Plan de Trabajo en materia de protección de datos personales. Del análisis de dicha información, se advierte que se refiere a un catálogo descriptivo de diversas medidas de seguridad, pero que no alude a información que podría poner en riesgo las bases de datos personales bajo resguardo de este Alto Tribunal, en tanto esa información no se encuentra relacionada con los tratamientos o con su nivel de riesgo o porcentaje de brecha.

Es decir, se trata de un “Catálogo de medidas de seguridad para los tratamientos de datos personales” que, de manera genérica señala las políticas y medidas de seguridad que, en su caso, se deben implementar por parte de las áreas de la Suprema Corte de Justicia de la Nación para garantizar la protección de los datos personales a saber: medidas de seguridad administrativas, medidas de seguridad físicas y medidas de seguridad técnicas, sin que, se reitera, de su contenido se aprecie que se den a conocer datos específicos de tales áreas que puedan poner en riesgo los tratamientos de datos personales que tienen bajo su responsabilidad, por lo que las citadas medidas de seguridad no constituyen información que por su contenido deba ubicarse en los supuestos normativos de clasificación de la información.

No obstante, también se advierte que, en el Plan de Trabajo en materia de protección de datos personales, se incluyen los principales resultados del análisis de brecha antes citado, en donde se detallan los niveles de cumplimiento de los tratamientos de datos personales. Por tanto, derivado de las consideraciones antes desarrolladas para confirmar la reserva del citado análisis en el Documento de Seguridad, dicha reserva también devendría en este apartado del Plan de Trabajo.

Atendiendo a las consecuencias que podría tener la difusión de esa información, en el caso concreto, debe arribarse a una conclusión que permita la adecuada armonización del derecho de acceso a la información y frente a un posible riesgo a la seguridad de las personas de quienes se tienen en resguardo sus datos personales, incluso, su salud o su vida, sin que ello implique restringir en mayor o menor medida el derecho de acceso a la información, para proteger un interés superior del peticionario, sino fijar sus límites atendiendo a las particularidades del caso concreto.

**Análisis específico de la prueba de daño.**

La clasificación de reservada antes expuesta se corrobora al realizar la prueba de daño prevista en el artículo 104 de la Ley General de Transparencia, dado que existe un riesgo identificado que supera el interés público general de que se difunda la información.

Para comprender lo anterior, se tiene en cuenta que el derecho de acceso a la información pública, en su vertiente social o institucional, es un instrumento de control ciudadano del funcionamiento del Estado y la gestión pública; para la participación ciudadana en asuntos públicos a través del ejercicio informado de los derechos políticos y, en general, para la realización de otros derechos fundamentales. Consecuentemente, el pleno ejercicio del derecho de acceso a la información es una garantía

indispensable para evitar abusos de los funcionarios públicos, promover la rendición de cuentas y la transparencia en la gestión estatal y prevenir la corrupción y el autoritarismo[2]

De igual forma, se tiene en cuenta que la Suprema Corte de Justicia de la Nación ha entendido que en un Estado constitucional la regla general es que los poderes públicos no están autorizados para mantener secretos y reservas frente a los ciudadanos en el ejercicio de las funciones estatales que tienen asignadas, salvo las excepciones legalmente tasadas que operan cuando la revelación de datos sea susceptible de afectar la seguridad pública u obstruya la prevención o persecución de los delitos.

En esta línea, preservar la seguridad pública y prevenir la comisión de delitos constituye una razón de peso para acotar el derecho de acceso a la información, pues, en todo caso, lo que una sociedad democrática desea conocer son datos que permitan evaluar la gestión de sus servidores públicos, tales como lo que establece la Ley General de Transparencia en su artículo 70.

En consecuencia, se estima que en el presente caso se supera el interés público general de que se difunda la información materia de análisis.

Aunado a lo expuesto, al estar en presencia de una limitación del derecho de acceso a la información pública, corresponde examinar la implementación de la reserva en el caso particular. Para ello, debe analizarse si la limitación (i) persigue una finalidad constitucionalmente imperiosa, (ii) si es idónea para satisfacer en alguna medida su propósito constitucional, (iii) si existen medidas alternativas igualmente idóneas para lograr dicho fin, pero que sean menos lesivas para el derecho fundamental, y (iv) si el grado de realización del fin perseguido es mayor al grado de afectación provocado al derecho de acceso a la información por la reserva.

[2] Corte I.D.H., Caso Claude Reyes y otros. Sentencia de 19 de septiembre de 2006. Serie C No. 151, párrs. 86 y 87.

Como se estableció previamente, la reserva de la información busca proteger la seguridad de la información y al derecho de protección de datos personales de los titulares de dicha información, ante lo cual no puede prevalecer el interés particular del peticionario, sino un interés mayor de proteger esa información, por lo que la medida cuenta con una finalidad válida, ya que busca tutelar otros valores de rango constitucional.

La reserva es idónea, porque con ello se contribuye a la vulneración o indebido tratamiento que pudieran recibir los datos personales que tiene en resguardo este Alto Tribunal, comprometiendo con ello la seguridad de la información y el derecho a la protección de sus datos personales de los titulares, pues la difusión de dicha información puede poner en peligro la integridad y el ejercicio de los derechos de las personas, de ahí que la reserva es apta y contribuye al fin perseguido.

Por cuanto a la necesidad, debe señalarse que la reserva se refiere al “análisis de riesgo” y el “análisis de brecha” contenidos en el Documento de Seguridad, así como al análisis de brecha mencionado en el Plan de Trabajo. Se estima que la **divulgación** de esa información sí puede vulnerar el derecho a la protección de datos personales en posesión de este Alto Tribunal, pues como ya se señalaba, podría poner en riesgo la estrategia de seguridad implementadas para proteger los datos personales que se encuentran bajo su resguardo, al divulgarse los niveles de riesgo identificados en los tratamiento de datos personales y con el análisis de la brecha se daría a conocer el grado de vulnerabilidad de esta institución en materia de seguridad de protección de datos personales, lo que, se reitera, representa un riesgo real para la seguridad pública y de las personas.

Además, no existe un medio alternativo que pudiera garantizar el derecho de acceso a la información respecto de la información reservada, sin que implique en alguna medida un riesgo para los valores protegidos por la misma. No obstante, la entrega de la versión pública de dichos documentos se erige como el medio menos restrictivo que consigue balancear el derecho de acceso a la información y los valores protegidos por la reserva.

Por último, se estima que la reserva es proporcional a la acotación del acceso a la información pública, pues se busca proteger las bases de datos personales que obran en resguardo de este Alto Tribunal, evitando exponerlas a un ataque que pudiera conseguir vulnerarlas u obtenerlas para beneficiarse de ellas, lo que podría poner en riesgo la privacidad de las personas titulares, ante lo cual debe rendirse el interés público de acceso a esa información en particular.

Por las anteriores consideraciones, lo procedente es confirmar la reserva al actualizarse el supuesto de las fracciones I y VII del artículo 113 de la Ley General de Transparencia y artículo 110, fracciones I y VII de la Ley Federal de la materia, quedando reservada la siguiente información antes analizada:

- Del Documento de Seguridad: los apartados relativos al análisis de riesgo y al análisis de brecha; y,
- Del Plan de Trabajo en materia de protección de datos personales: los resultados del análisis de brecha.

Es oportuno precisar que conforme a los artículos 101, párrafo segundo y 109 de la Ley General de Transparencia, así como 100 de la Ley Federal de Transparencia, atendiendo a las causas que dan origen a la reserva de parte de la información contenida en el Documento de Seguridad y en el Plan de Trabajo en materia de protección de Datos Personales, se

determina que el plazo de reserva de la información es de cinco años, en la inteligencia de que al concluir dicho plazo será necesario analizar si resulta procedente la divulgación de dicha información, ya que tales documentos se relacionan con las medidas de seguridad para el tratamiento de los datos personales que posee la Suprema Corte de Justicia de la Nación.

Finalmente, se encomienda a la Secretaría Técnica de este Comité que entregue directamente a la Unidad General de Transparencia la versión pública del Documento de Seguridad y del Plan de Trabajo en materia de protección de datos personales con base en los parámetros de esta resolución, para que se ponga a disposición del peticionario y así tener por satisfecha la solicitud de acceso.

Por lo expuesto y fundado; se,

**R E S U E L V E:**

**PRIMERO.** Se tiene por atendida la solicitud en términos de lo expuesto en la presente resolución.

**SEGUNDO.** Se confirma la clasificación de información reservada, de acuerdo con lo expuesto en esta resolución.

**TERCERO.** Se requiere a la Secretaría Técnica del Comité de Transparencia que realice las acciones señaladas en esta resolución.

**CUARTO.** Se requiere a la Unidad General de Transparencia para que realice las acciones señaladas en esta resolución.

Notifíquese al solicitante, a la instancia requerida y a la Unidad General de Transparencia.

Por unanimidad de votos lo resolvió el Comité de Transparencia de la Suprema Corte de Justicia de la Nación, integrado por el licenciado Juan Sebastián Francisco de Asís Mijares Ortega, Director General de Asuntos Jurídicos y Presidente del Comité, maestro Christian Heberto Cymet López Suárez, Contralor del Alto Tribunal, y maestro Julio César Ramírez Carreón, Titular de la Unidad General de Investigación de Responsabilidades Administrativas; quienes firman con el secretario del Comité que autoriza.

**LICENCIADO JUAN SEBASTIÁN FRANCISCO DE ASÍS MIJARES ORTEGA**
**PRESIDENTE DEL COMITÉ**

**MAESTRO CHRISTIAN HEBERTO CYMET LÓPEZ SUÁREZ**
**INTEGRANTE DEL COMITÉ**

**MAESTRO JULIO CÉSAR RAMÍREZ CARREÓN**
**INTEGRANTE DEL COMITÉ**

**LICENCIADO ARIEL EFRÉN ORTEGA VÁZQUEZ**
**SECRETARIO DEL COMITÉ**

Esta hoja corresponde a la última de la resolución dictada por el Comité de Transparencia de la Suprema Corte de Justicia de la Nación en el expediente CT-CI/A-2-2020. **Conste.-**