CLASIFICACIÓN DE INFORMACIÓN
CT-CI/A-7-2020

INSTANCIA REQUERIDA:
DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN

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

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

I. Solicitud de información. El catorce de mayo de dos mil veinte, se recibió la solicitud tramitada en la Plataforma Nacional de Transparencia con el folio 0330000152820, requiriendo:

> *"1. ¿Qué funciones tienen sus sistemas informáticos en el desarrollo de datos y procesamiento de los mismos?*
> *2. ¿Qué elementos contemplan en la protección de sus sistemas sistemas* (sic) *(amenazas y vulnerabilidades)?*
> *3. Sus políticas de seguridad implementadas para la prevención y solución de amenazas conforme a cada elemento para la protección de los sistemas.*
> *4. Cuerpos normativos y artículos a los que se vincula la seguridad informática de los sistemas de cómputo y/o bases de datos."*

(Numeración realizada en el acuerdo de admisión)

II. Acuerdo de admisión de la solicitud. En acuerdo de quince de mayo 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/0196/2020.

III. Requerimiento de información. El Titular de la Unidad General de Transparencia y Sistematización de la Información Judicial, a través del oficio UGTSIJ/TAIPDP/1312/2020, enviado mediante comunicación electrónica de dieciocho de mayo de dos mil veinte, solicitó a la Dirección General de Tecnologías de la Información que se pronunciara sobre la existencia y clasificación de la información materia de la solicitud.

IV. Informe de la Dirección General de Tecnologías de la Información. El dos de junio de dos mil veinte, se recibió en la cuenta de correo electrónico habilitada para tales efectos por la Unidad General de Transparencia, el oficio DGTI/430/2020 digitalizado, en el que la titular de esa dirección general señala que remite dos notas informativas con las que se da respuesta a lo requerido en la solicitud, las cuales se transcriben enseguida:

a) Nota informativa suscrita por la Subdirectora General de Sistemas Informáticos.

"1. ¿Qué funciones tienen sus sistemas informáticos en el desarrollo de datos y procesamiento de los mismos?

- *Captura de datos estructurados*
- *Integración de datos estructurados y no estructurados*
- *Almacenamiento de información*
- *Exportación de datos*
- *Publicación de datos*
- *Replicación de datos*

b) Nota informativa suscrita por el Director de Seguridad Informática, el Subdirector de Gobierno de Seguridad de la Información y por el Jefe de Departamento de Criptografía y Autentificación.

"2. ¿Qué elementos contemplan en la protección de sus sistemas sistemas (sic) (amenazas y vulnerabilidades)?

R.- Los elementos de protección que se contemplan son los siguientes:

- *Antivirus empresarial para protección de amenazas informáticas.*
- *Ejecución de análisis de vulnerabilidades a los sistemas informáticos.*

- *Certificados SSL para establecer canales seguros de comunicación.*
- *Uso de equipos de seguridad perimetral.*
- *Administración de políticas de seguridad y filtrado de contenido.*
- *Infraestructura de control de acceso físico a centros de datos.*
- *Administración de borrado seguro a equipos de cómputo.*
- *Respuesta a incidentes de seguridad de la información.*
- *Actualización de versiones de software.*
- *Controles de seguridad para el acceso lógico a los activos de información con base en la norma ISO27000.*

3. Sus políticas de seguridad implementadas para la prevención y solución de amenazas conforme a cada elemento para la protección de los sistemas.

R.- Se comunica que la información solicitada se considera reservada, de conformidad con lo dispuesto en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, ya que la divulgación de la misma:

- *Permitiría el acceso ilícito a sus sistemas y equipos informáticos, intentando la suplantación de los mismos;*
- *Potenciaría la posibilidad de vulnerar la seguridad de su infraestructura tecnológica;*
- *Establecería con un alto grado de precisión la información técnica referente a los protocolos de seguridad y las características de la infraestructura instalada;*
- *Pondría en un estado vulnerable a la institución, facilitando la intervención de las comunicaciones y permitiendo usurpar permisos requeridos en la red para obtener información;*
- *Daría a conocer puntos de vulnerabilidad para la seguridad de la infraestructura de cómputo;*
- *Vulneraría sus sistemas informáticos, así como la información contenida en éstos;*
- *Atentaría en contra de su infraestructura tecnológica, afectando el ejercicio de sus labores sustantivas; y*
- *Modificaría, destruiría o provocaría pérdida de información contenida en sus sistemas.*

Se advierte que la negativa de acceso a la información se motiva en pretender evitar o prevenir la comisión del delito de acceso ilícito a sus equipos y sistemas de informática.

Al respecto, el Código Penal Federal dispone lo siguiente:

> ***Acceso ilícito y equipos de informática***
> *ARTICULO 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.*
> *Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.*
> *ARTICULO 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 de 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 de 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.*
> *…*
> *ARTICULO 211 bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno."*

De los preceptos antes citados, se advierte que comete el delito de acceso ilícito a sistemas y equipo de informática todo aquel que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, sean o no propiedad del Estado.

Asimismo, mencionan que, a quien 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 de multa.

De igual forma, la entrega de las políticas de seguridad informática, podría ocasionar lo siguiente:

- ✓ *Una posible intervención de sus comunicaciones,*
- ✓ *La usurpación de sus permisos,*
- ✓ *La suplantación de sus equipos y de la información que almacena en sus servidores;*
- ✓ *El robo de la información que obra en sus archivos digitales, y*
- ✓ *El detrimento de sus instalaciones tecnológicas.*

Cuestiones que se materializan con la comisión de delitos de carácter cibernético, que sin duda afectarían severamente el ejercicio de las labores cotidianas y sustantivas.

Con base en lo anterior, el riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda la información, ya que el resguardo de los datos requeridos por el solicitante implica la prevención del delito de acceso ilícito a sistemas y equipos de informática tipificando en el Código Penal Federal, lo cual cobra importancia si se considera que dicha conducta implica conocer, copiar, modificar, destruir o provocar la pérdida de información contenida en sistemas o equipos de informática.

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 la conducta antijurídica tipificada (acceso ilícito a sistemas y equipos de informática), misma que de llevarse a cabo podría permitir la realización de diversos ataques a la infraestructura tecnológica y de sistemas del sujeto obligado, los cuales podrían traer como consecuencia la inoperatividad de sus funciones, por un periodo indeterminado.

Por todo lo anterior, se advierte que difundir la información requerida incrementa sustancialmente la posibilidad de que aquella persona que conozca dicha información cometa algún ilícito, accediendo de forma no autorizada a los sistemas de datos que no son públicos en posesión del sujeto obligado, conociendo con un alto grado de precisión la información técnica referente a sus equipos de cómputo, los protocolos de seguridad y las características de la infraestructura instalada.

4. Cuerpos normativos y artículos a los que se vincula la seguridad informática de los sistemas de cómputo y/o bases de datos.'

R.- 1. Reglamento Orgánico en Materia de Administración de la Suprema Corte: Artículo 27 fracción XI.

2.- Acuerdo General de Administración IV/2008' (AGA IV/2008): Artículos 22, 28, 29, 36, 39, así como dentro de su 'TÍTULO SEXTO DE LA SEGURIDAD INFORMÁTICA', particularmente los artículos 61, 64, 65, 66 y 68

https://www.scjn.gob.mx/transparencia/obligaciones-de-transparencia/marco-normativo/disposiciones-scjn/acuerdos-administrativos?field_a6sa13s_tema_target_id=All&fecha=10"

V. Vista a la Secretaría del Comité de Transparencia. Mediante correo electrónico de diez de junio de dos mil veinte, el Titular de la Unidad General de Transparencia y Sistematización de la Información Judicial remitió el oficio UGTSIJ/TAIPDP/1455/2020 y el expediente electrónico UT-A/0196/2020 a la Secretaría del Comité de Transparencia, con la finalidad de que se dictara la resolución correspondiente.

VI. Acuerdo de turno. Mediante acuerdo de diez de junio de dos mil veinte, la Presidencia del Comité de Transparencia, con fundamento en los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública, así como 23, fracción II, y 27, del Acuerdo General de Administración 5/2015, ordenó integrar el expediente **CT-CI/A-7-2020** y, conforme al turno correspondiente, remitirlo al Contralor del Alto Tribunal, a fin de que presentara la propuesta de resolución, lo que se hizo mediante oficio

CT-403-2020, enviado mediante correo electrónico el once de junio de este año.

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 II y III, de la Ley General de Transparencia y Acceso a la Información Pública, 65, fracciones 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 información de la Suprema Corte de Justicia de la Nación, consistente en:

1. Tipo de funciones que se utilizan en los sistemas informáticos en el desarrollo y procesamiento de datos.
2. Elementos que se contemplan en la protección de los sistemas sobre amenazas y vulnerabilidades.
3. Las políticas de vulnerabilidad implementadas para la prevención y solución de amenazas conforme a cada elemento para la protección de los sistemas.
4. Normativa que se vincula con la seguridad informática de los sistemas de cómputo y bases de datos.

I. Información que se pone a disposición.

Por cuanto a la información que se solicita en el punto 1, relativa al tipo de funciones que se utilizan para el desarrollo y procesamiento de datos, en la nota de la Subdirectora General de Sistemas Informáticos de la Dirección

General de Tecnologías de la Información se precisa que se trata de los siguientes: captura de datos estructurados; integración de datos estructurados y no estructurados; almacenamiento de información; exportación de datos; publicación de datos y replicación de datos; por lo tanto, se estima que con dicha información se tiene por atendido lo requerido en ese numeral.

Por otro lado, en la nota del Director de Seguridad Informática, del Subdirector de Gobierno de Seguridad de la Información y del Jefe de Departamento de Criptografía y Autentificación, de la Dirección General de Tecnologías de la Información, se precisan los diversos elementos que se contemplan en la protección de los sistemas informáticos de este Alto Tribunal, con lo cual se atiende lo solicitado en el punto 2 de la solicitud; además, se proporciona la liga electrónica en la que se puede consultar el marco normativo que prevé la seguridad informática de los sistemas de cómputo y bases de datos de este Alto Tribunal, señalando los preceptos del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación y del Acuerdo General de Administración IV/2008 que se refieren a esos aspectos, lo cual da respuesta a lo planteado en el punto 4 de la solicitud.

De conformidad con lo expuesto, se estima que con la información proporcionada por la Dirección General de Tecnologías de la Información en las notas a que se ha hecho referencia, se atienden los aspectos planteados en los puntos 1, 2 y 4 de la solicitud que nos ocupa y, en consecuencia, la Unidad General de Transparencia deberá hacer del conocimiento del peticionario lo informado al respecto por dicha instancia.

II. Información reservada.

Por cuanto a las políticas de vulnerabilidad implementadas para la prevención y solución de amenazas conforme a cada elemento para la protección de los sistemas que se requiere en el punto 3 de la solicitud, la Dirección General de Tecnologías de la Información clasifica dicha información

como reservada, aduciendo que con su acceso se ponen en riesgo los sistemas de datos de este Alto Tribunal que no son públicos, ya que se daría a conocer información técnica sobre los equipos de cómputo, los protocolos de seguridad y las características de la infraestructura instalada.

Para llevar a cabo el análisis correspondiente, se tiene en cuenta que, en el esquema de nuestro sistema constitucional, el derecho de acceso a la información encuentra cimiento en lo dispuesto en el artículo 6º, apartado A, de la Constitución Política de los Estados Unidos Mexicanos, cuyo contenido deja claro que, en principio, todo acto de autoridad (todo acto de gobierno) es de interés general y, por ende, es susceptible de ser conocido por todos.

Sin embargo, como lo ha interpretado el Pleno del Alto Tribunal en diversas ocasiones, el derecho de acceso a la información no puede caracterizarse como uno de contenido absoluto, en tanto su ejercicio se encuentra acotado en función de ciertas causas e intereses relevantes, así como frente al necesario tránsito de las vías adecuadas para ello[1].

En atención al dispositivo constitucional antes referido, la información que tienen bajo su resguardo los sujetos obligados del Estado encuentra como excepción aquella que sea temporalmente reservada o confidencial en los términos establecidos por el legislador federal o local, cuando de su

---

[1] ***DERECHO A LA INFORMACIÓN. SU EJERCICIO SE ENCUENTRA LIMITADO TANTO POR LOS INTERESES NACIONALES Y DE LA SOCIEDAD, COMO POR LOS DERECHOS DE TERCEROS****. El derecho a la información consagrado en la última parte del artículo 6o. de la Constitución Federal no es absoluto, sino que, como toda garantía, se halla sujeto a limitaciones o excepciones que se sustentan, fundamentalmente, en la protección de la seguridad nacional y en el respeto tanto a los intereses de la sociedad como a los derechos de los gobernados, limitaciones que, incluso, han dado origen a la figura jurídica del secreto de información que se conoce en la doctrina como "reserva de información" o "secreto burocrático". En estas condiciones, al encontrarse obligado el Estado, como sujeto pasivo de la citada garantía, a velar por dichos intereses, con apego a las normas constitucionales y legales, el mencionado derecho no puede ser garantizado indiscriminadamente, sino que el respeto a su ejercicio encuentra excepciones que lo regulan y a su vez lo garantizan, en atención a la materia a que se refiera; así, en cuanto a la seguridad nacional, se tienen normas que, por un lado, restringen el acceso a la información en esta materia, en razón de que su conocimiento público puede generar daños a los intereses nacionales y, por el otro, sancionan la inobservancia de esa reserva; por lo que hace al interés social, se cuenta con normas que tienden a proteger la averiguación de los delitos, la salud y la moral públicas, mientras que por lo que respecta a la protección de la persona existen normas que protegen el derecho a la vida o a la privacidad de los gobernados. Época: Novena Época. Registro: 191967. Instancia: Pleno. Tipo de Tesis: Aislada. Fuente: Semanario Judicial de la Federación y su Gaceta. Tomo XI, Abril de 2000. Materia(s): Constitucional Tesis: P. LX/2000. Página: 74)*

propagación pueda derivarse perjuicio por causa de interés público y seguridad nacional.

Ahora bien, para sustentar la clasificación de reserva que hace la Dirección General de Tecnologías de la Información, se cita el artículo 110, fracción VII, de la Ley Federal de Transparencia, manifestando que su divulgación:

- Permitiría el acceso ilícito a los sistemas y equipos, ejerciendo la suplantación de estos.
- Potenciaría la posibilidad de vulnerar la infraestructura tecnológica.
- Establecería con alto grado de precisión la información técnica sobre los protocolos de seguridad y las características de la infraestructura instalada.
- Se pondría en estado vulnerable a la Suprema Corte de Justicia de la Nación, porque se facilitaría la intervención de las comunicaciones, permitiendo usurpar los permisos requeridos en la red para obtener información.
- Daría a conocer puntos de vulnerabilidad para la seguridad de la infraestructura de cómputo.
- Vulneraría los sistemas informáticos y la información contenida en éstos.
- Atentaría contra la infraestructura tecnológica, afectando el ejercicio de las labores sustantivas.
- Modificaría, destruiría o provocaría pérdida de información contenida en los sistemas informáticos.

La clasificación como **reservada** de dicha información, como se señaló, se sustenta en el artículo 110, fracción VII, de la Ley Federal de Transparencia, en virtud de que al poner en riesgo cuestiones de seguridad y conectividad de los sistemas informáticos y bases de datos de la Suprema Corte de Justicia de

la Nación se obstruiría la prevención de delitos, específicamente, delito de acceso ilícito a sus equipos y sistemas de informática.

En ese tenor, es importante destacar que el informe que se analiza lo emite el área técnica que, conforme a sus atribuciones, es responsable en la Suprema Corte de Justicia de la Nación de los sistemas informáticos de los que se pide la información, por lo que considerando lo resuelto por este Comité en el cumplimiento CT-CUM-R/A-2-2019, se arriba a la conclusión de que sobre la información requerida sí pesa la reserva establecida en la fracción VII del artículo 110, de la Ley Federal de Transparencia que establece:

> ***"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;"*
> (…)

Sobre el alcance del artículo 110, fracción VII, de la Ley Federal de Transparencia, se tienen en cuenta que su contenido es idéntico al que dispone la Ley General de Transparencia en el artículo 113, fracción VII, razón por la que 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, cumplimentado por este Comité en la citada resolución CT-CUM-R/A-2-2019, ya 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, en dichas resoluciones se precisa 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 prevención del delito significa *"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"* y 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".*

También se señaló que conforme al Código Penal Federal *"comete el **delito de acceso ilícito a sistemas y equipos de informática** todo aquel que **sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad**, sean o no propiedad del Estado. Asimismo, 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"* (foja 100 vuelta de la resolución del recurso de revisión RRA 10276/18).

Adicionalmente, es de destacar que, en la resolución emitida por el Instituto Nacional de Transparencia se invocan, como hecho notorio, las respuestas que la Dirección General de Tecnologías de la Información de ese Instituto emitió en respuesta a las consultas que se le formularon sobre información similar a la que es materia de la solicitud que da origen a este asunto[2].

---

[2] *"Sin embargo, añadió que **cuando se proporciona un conjunto de datos informáticos de TIC sensibles y que además se encuentran correlacionados, como los peticionados**, con tal información cualquier persona con **fines malintencionados**, podría utilizar sus conocimientos para 'hackear' (acción de entrar de forma abrupta y sin permiso a un*

En virtud de lo anterior, en la resolución del Instituto Nacional de Transparencia se argumenta que *"derivado de la naturaleza y el grado de especificidad del tipo de información que se requiere, y que se trata de un elemento relevante al ponderar cualquier posible vulneración a la seguridad de la infraestructura tecnológica de la autoridad obligada, es que se colige que dar a conocer la misma facilitaría que personas expertas en informática* ***perturben el sistema de la infraestructura tecnológica*** *de la Suprema Corte de Justicia de la Nación, ejecuten programas informáticos perjudiciales que modifiquen o destruyan información relevante; situación que pondría en un estado vulnerable la información que en ella se contiene, facilitando la intervención de las comunicaciones y permitiendo usurpar permisos requeridos en la red para obtener información"*.

De conformidad con lo expuesto, atendiendo a los argumentos señalados por el Instituto Nacional de Transparencia en el recurso de revisión RRA 10276/18 y que fueron retomados en la resolución CT-CUM-R/A-2-2019, este Comité de Transparencia **confirma la clasificación de reserva** de la información relativa a las políticas de vulnerabilidad implementadas para la prevención y solución de amenazas conforme a cada elemento para la protección de los sistemas de la Suprema Corte de Justicia de la Nación (punto 3 de la solicitud), con fundamento en los artículos 113, fracción VII, de la Ley General de Transparencia y 110, fracción VII, de la Ley Federal de la materia,

---

sistema de cómputo o una red) o crackear (literalmente traducido como rompedor, del inglés ' to track', que significa romper o quebrar) se utiliza para referirse a las personas que rompen o vulneran algún sistema de seguridad, los sistemas informáticos objetivo y de alguna manera correlacionan la información para ***vulnerar la seguridad de los equipos informáticos así como afectar los servicios informáticos del sujeto obligado"*** (foja 101 vuelta).

Respecto del cuestionamiento *"¿Dar a conocer si los archivos almacenados están cifrados, y los nombres comerciales de los programas informáticos para el cifrado utilizados por el sujeto obligado, representan un riesgo a los sistemas, redes o equipos del sujeto obligado?"*, la dirección general en comento refirió (foja 102):

> *"Cuando se proporciona un conjunto de datos informáticos de TIC sensibles y que además se encuentran correlacionados como por ejemplo:* ***nombres comerciales de los programas informáticos para cifrar****, método de cifrado, tipo de cifrado, longitud de las llaves, etc., con tal información* ***cualquier persona con fines malintencionados, podría utilizar sus cocimientos o contratar alguna persona con capacidades y conocimientos en materia de hackear"***
> (…)

dado que, como se mencionó, considerando que la Dirección General de Tecnologías de la Información es el área técnica para pronunciarse sobre la naturaleza de la información solicitada y dicha área señaló que al entregar esos datos se podría comprometer la seguridad informática de los sistemas y equipos de este Alto Tribunal, porque se pondría en riesgo la seguridad operativa de la infraestructura tecnológica que permite la operación de las diversas áreas del Alto Tribunal.

Así, conforme a la argumentación sostenida en la resolución del Instituto Nacional de Transparencia la reserva de dicha información permite prevenir la comisión del delito de acceso ilícito a sistemas y equipos de informática tipificados en el Código Penal Federal, pues al dar a conocer la información solicitada, no sólo se *"comprometería la información que obra en los archivos digitales del sujeto obligado, sino que menoscabaría la seguridad y certeza de los ciudadanos que acuden a éste para otorgar certeza respecto de la impartición de justicia y control constitucional".*

Por lo tanto, se confirma se confirma la reserva de la información materia de este apartado, con fundamento en los artículos 110, fracción VII, de la Ley Federal de Transparencia y 113, fracción VII, de la Ley General de Transparencia.

Análisis específico de la prueba de daño. De acuerdo con el alcance de la causa de reserva prevista en el artículo 110, fracción VII, de la Ley Federal de Transparencia, acorde con lo señalado por el Instituto Nacional de Transparencia al resolver el recurso de revisión RRA 10276/18 y por este Comité en la resolución de cumplimiento CT-CUM-R/A-2-2019, se determina que la divulgación de la información solicitada conllevaría un riesgo real, demostrable e identificable, en tanto que colocaría a la Suprema Corte de Justicia de la Nación en un estado de vulnerabilidad, facilitando una posible intervención de las comunicaciones; usurpación de permisos; suplantación de

equipos y de la información almacenada en los servidores; robo de información que obran en los archivos digitales, así como el detrimento de las instalaciones tecnológicas.

En ese sentido, el perjuicio significativo al **interés público** resulta **menos restrictivo**, porque se pondría en riesgo la responsabilidad fundamental del Alto Tribunal en la defensa del orden establecido en la Constitución Federal, mediante los medios de control constitucional.

Por lo anterior, acorde con las resoluciones a que se ha hecho referencia, el riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda la información, ya que el resguardo de los datos requeridos en la solicitud implica llevar a cabo la prevención del delito de acceso ilícito a sistemas y equipos de informática tipificado en el Código Penal Federal, lo cual cobra importancia si se considera que dicha conducta implica conocer, copias, modificar, destruir o provocar la pérdida de información contenida en sistemas o equipos de informática, por lo que revelar las políticas de vulnerabilidad implementadas para la prevención y solución de amenazas conforme a cada elemento para la protección de los sistemas de la Suprema Corte de Justicia de la Nación *“no sólo se comprometería la información que obra en los archivos digitales del sujeto obligado, sino que menoscabaría la seguridad y certeza de los ciudadanos que acuden a éste para otorgar certeza respecto de la impartición de justicia y control constitucional”.*

Ahora bien, dicha clasificación de reserva *“**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 la conducta antijurídica tipificada** (acceso ilícito a sistemas y equipos de informática)”,* de llevarse a cabo podría permitir la ejecución de diversos **ataques** a la infraestructura tecnológica y de sistemas con que cuenta este Alto Tribunal, ya que la difusión

de las políticas de vulnerabilidad implementadas para la prevención y solución de amenazas de los sistemas informáticos *"**incrementa sustancialmente la posibilidad de que aquella persona que conozca dicha información cometa algún ilícito"***, pues tendría acceso a información con un alto grado de precisión técnica, así como a los protocolos de seguridad y las características de la infraestructura instalada.

Plazo de reserva. En términos de lo señalado en el artículo 101[3], párrafo segundo, de la Ley General de Transparencia, se determina que el plazo de reserva será por cinco años, ya que por las consideraciones expuestas en la resolución del Instituto Nacional de Transparencia a que se hacho mención y en la de cumplimiento CT-CUM-R/A-2-2019, mismas que se retoman en esta determinación, *"dicho plazo es proporcional a la naturaleza y el grado de especificidad del tipo de información de que se trata".*

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 el considerando segundo de la presente resolución.

SEGUNDO. Se confirma la clasificación de reservada, de la información a que se hace referencia en el apartado II del segundo considerando de esta resolución.

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

---

[3] ***"Artículo 101.*** *Los Documentos clasificados como reservados serán públicos cuando:*
…
La información clasificada como reservada, según el artículo 113 de esta Ley, podrá permanecer con tal carácter hasta por un periodo de cinco años. El periodo de reserva correrá a partir de la fecha en que se clasifica el documento…"

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

Ariel Efrén Ortega Vázquez, Secretario del Comité de Transparencia, con fundamento en el artículo 26, fracción XI, del ACUERDO GENERAL DE ADMINISTRACIÓN 05/2015 DEL TRES DE NOVIEMBRE DE DOS MIL QUINCE, DEL PRESIDENTE DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, POR EL QUE SE EXPIDEN LOS LINEAMENTOS TEMPORALES PARA REGULAR EL PROCEDIMIENTO ADMINISTRATIVO INTERNO DE ACCESO A LA INFORMACIÓN PÚBLICA, ASÍ COMO EL FUNCIONAMIENTO Y ATRIBUCIONES DEL COMITÉ DE TRANSPARENCIA DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN----------

----------**CERTIFICA**----------

Que, acorde con lo dispuesto en el ACUERDO PLENARIO 3/2020 del diecisiete del presente, de este Alto Tribunal, que suspende actividades jurisdiccionales para proteger la salud en relación con la enfermedad que causa el coronavirus COVID-19 y de conformidad con la RESOLUCIÓN adoptada sobre el particular por el Comité de Transparencia de la Suprema Corte de Justicia de la Nación en su Sesión Extraordinaria del 18 de marzo del presente, el referido órgano colegiado celebró su Décima Segunda Sesión Ordinaria el 17 de junio de 2020 a través de videoconferencia y con la participación de todos sus integrantes, quienes aprobaron por unanimidad la resolución dictada en el expediente de la **clasificación de información CT-CI/A-7-2020** por unanimidad de votos. Ciudad de México, a diecisiete de junio de dos mil veinte. **CONSTE.**