CUMPLIMIENTO:
CT-CUM/A-36/2018
DERIVADO DEL CT-CI/A-20-2018

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 **trece de noviembre de dos mil dieciocho**.

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

I. Solicitud de información. El cinco de julio de dos mil dieciocho, se recibió en la Plataforma Nacional de Transparencia la solicitud tramitada bajo el folio 0330000135418, por la que se requirió información consistente en: "…*conocer el número de ataques cibernéticos que la dependencia federal ha recibido de enero de 2018 a la fecha. Favor de detallar por mes, tipo de ataque y lugar de origen*" [sic].

II. Informes de la instancia requerida. En seguimiento al trámite, el Director General de Tecnologías de la Información a grandes rasgos dijo que dar a conocer la información asociada a ciberataques podría comprometer la infraestructura tecnológica de este Alto Tribunal, por lo que clasificó como reservados los datos solicitados.

III. Resolución del Comité de Transparencia de la Suprema Corte de Justicia de la Nación. Concluido el procedimiento correspondiente, se integró el expediente de la clasificación de información CT-CI/A-20-2018, y el cinco de septiembre de dos mil dieciocho, este Comité de Transparencia, en lo que importa, resolvió:

> *"…esas consideraciones dan cuenta que, para efectos del acceso a la información, la supuesta alteración del esquema de seguridad de los sistemas tecnológicos sobre los que puede descansar la dinámica de comunicación y operación de los diversos sujetos obligados debe justificarse de manera concreta y estricta, sin que la mera posibilidad de ataques sea suficiente para ello. - - - Sobre todo porque el acceso a la información no puede entenderse sustentado en un principio de riesgo futuro o de malicia de quien acude a su ejercicio, de ahí que su eficacia no deba verse obstaculizada a partir de supuestas categorías y datos técnicos generales e hipotéticos, sino que, por el contrario, para su posible limitación se exige la precisión de datos objetivos que, dentro de un marco racional específico, demuestren de modo real y excepcional el daño que la divulgación de la información representaría, en términos de los artículos 104 y 113 de la Ley General, lo que no aconteció en la especie, sin que este Comité, en este momento, pueda pronunciarse al respecto. - - - (…) - - - Luego, conforme a lo anterior, ante la evidencia de la necesidad de proteger información que pudiere generar afectación a los sistemas de seguridad informática, que pudieren incidir en accesos no controlados ni permitidos de la información, tanto jurisdiccional como administrativa, de este Alto Tribunal, se exigiría que se precise y justifique de forma suficiente, desde la especifica prueba de daño, la reserva de información a que se ha venido haciendo mención o alguna otra. - - - (…) - - - Por tanto, de conformidad con lo dispuesto por el artículo 37, párrafos primero y segundo, de los Lineamientos (…), se* ***requiere*** *al Director General de Tecnologías de la Información, para que, en el plazo de cinco días hábiles, computados a partir del día siguiente al en que surta sus efectos la notificación de la presente resolución, justifique, desde la especifica prueba de daño, la reserva de información, de acuerdo a la causal o hipótesis respectiva de las encausadas en el artículo 113 de la Ley General…"*

IV. Respuesta en relación a la resolución del Comité de Transparencia. En respuesta al requerimiento formulado por este Comité de Transparencia, el Director General de Tecnologías de la Información, por oficio DGTI/DAPTI-1999-2018, recibido el veintiuno de septiembre del presente año, adjuntó como anexo un documento que da cuenta de la prueba de daño en el siguiente sentido:

"Diariamente a nivel mundial se registran miles de ataques informáticos dirigidos a realizar fraudes, generar denegación de servicios, distribución de códigos maliciosos, así como llevar a cabo el robo de información particular de Instituciones del sector público, privado y ciudadanos en general. - - - La ciberdelincuencia se encarga de hacer uso de diferentes herramientas y técnicas con la finalidad de obtener información que les permita acceder a los sistemas de cómputo de Instituciones públicas, privadas y personas físicas para realizar un ataque informático en contra de ellos. La información sensible que buscan es: claves de acceso, paswords, direcciones OP, tipos de sistemas, tipos de herramientas de seguridad informática, etc. - - - En la actualidad, una de las principales técnicas para obtener información es conocida como "Ingeniería Social", la cual consiste en el uso de habilidades sociales de forma consiente y muchas veces premeditada para obtener información sensible. Para el caso de sector público, a través de solicitudes de acceso a la información, se puede solicitar y en su caso proporcionar información sensible que pueda facilitar a la ciberdelincuencia un ataque contra los sistemas gubernamentales. - - - Cada pieza de información que sea proporcionada a un hacker haciéndose pasar por un ciudadano, aumenta el nivel de riesgos de cualquier plataforma informática, ya que mediante el uso de técnicas de hackeo dirigidas denominadas "exploits", aprovechan las vulnerabilidades informáticas presentes en los sistemas, los cuales son fáciles de identificar al contar con información del sistema informático al cual se desea atacar, como puede ser el tipo de sistema operativo, versiones de software, direccionamiento IP, software que usa, tipos y versión de las herramientas de seguridad que protegen, etc. - - - (…) - - - Considerando lo anterior, cabe reiterar que la información solicitada por el ciudadano debe ser considerada como restringida, toda vez que su divulgación puede proporcionar información sensible de la operación y seguridad de los servicios publicados en Internet de la SCJN, derivando en ataques informáticos, afectación y degradación de los servicios de información.

Escenario	*Implicación*	*Daño o afectación*
Dar a conocer los tipos de ataques recibidos a los portales web de la SCJN	*Cada una de las herramientas de seguridad informática tiene una clasificación propia para la identificación de cada uno de los tipos de ataques informáticos. Esto implica dar a conocer la marca de equipos de seguridad informática que hace uso la SCJN.* *Reconocimiento del tipo de ataques web que se han recibido y*	• *Aumento de ataques informáticos específicos contra las versiones y marca de los equipos de seguridad informática identificados.* • *Capacidad para identificar la versión de firmware del equipo de seguridad, con lo cual podrían explotar una vulnerabilidad y modificar sin autorización los portales web de la SCJN.* • *Recepción de ataques no recibidos o identificados en la infraestructura de*

	mitigado en los portales web.	*seguridad informática, llegando a afectar el contenido de los portales web.*
Dar a conocer la cantidad y periodo de ataques informáticos.	*Implicaría conocer la cantidad de peticiones web que puede soportar la infraestructura tecnológica de comunicaciones, seguridad y de servidores de la SCJN para sus portales web.*	• *Aumento de ataques informáticos dirigidos a superar la volumetría del canal de comunicación de los portales de Internet, toda vez que el ancho de banda tiene un límite de consumo, evitando con ello el acceso a los portales por parte de usuarios y servidores públicos.* • *Superar la capacidad de operación de los equipos servidores, de comunicaciones o de seguridad informática, lo que causaría la caída total del servicio.*
Dar a conocer el lugar de origen de los ataques web.	*Implica reconocer los lugares donde no se cuenta con un filtrado de peticiones, es decir que pueden llegar hasta la infraestructura de los portales web de la SCJN.*	• *Aumento de ataques informáticos desde regiones o zonas donde se tiene permitido el flujo de tráfico hacia los portales de Internet de la SCJN, lo que agotaría el enlace de comunicación de los portales web de la SCJN.*

***CONCLUSIONES**: El proporcionar la información solicitada, facilita a potenciales atacantes llamados "watering hole", conocer el nivel de vulnerabilidades de conexiones que existen en los sitios, el dar el número de ataques, permite a través de la estadística, identificar el estado que guarda nuestra infraestructura, lo cual no es recomendable, ni de uso cotidiano para la ciudadanía, solo expertos en la materia requieren información tan especializada." [sic]*

V. Acuerdo de turno. Mediante proveído de veintiuno de septiembre de dos mil dieciocho, el Presidente del Comité de Transparencia de este Alto Tribunal ordenó integrar el expediente **CT-CUM/A-36/2018** y su remisión al Secretario Jurídico de la Presidencia de esta Suprema Corte de Justicia de la Nación, en su carácter de integrante de dicho órgano, por ser ponente en la clasificación de información CT-CI/A-20-2018, del cual deriva, para que conforme a sus

atribuciones procediera al estudio y propuesta de resolución respectiva, en términos de lo dispuesto en los artículos 44, fracción I, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General); 23, fracción I, y 27 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 LINEAMIENTOS 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" (Lineamientos Temporales)*.

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

I. Competencia. El Comité de Transparencia de la Suprema Corte de Justicia de la Nación es competente para pronunciarse sobre el debido cumplimiento a sus determinaciones; así como confirmar, modificar o revocar las clasificaciones de información, de conformidad con los artículos 6° de la Constitución Política de los Estados Unidos Mexicanos; 44, fracción II, de la Ley General; 65, fracción II, de la Ley Federal; 23, fracción II, y 37, de los Lineamientos Temporales.

II. Cumplimiento de la resolución del Comité de Transparencia. Corresponde analizar si se dio cumplimiento a la resolución de fecha cinco de septiembre de dos mil dieciocho, emitida dentro de la clasificación de información CT-CI/A-20-2018.

Ahora, se recuerda que en la resolución de mérito, este órgano colegiado identificó que no podía entenderse actualizada la causal de reserva que establece la fracción XI, de la Ley General, no obstante, también se dijo que ante la evidencia de la necesidad de proteger información que pudiere generar afectación a los sistemas de seguridad informática, se exigía precisión, desde la prueba de daño, a efecto de estar en la posibilidad de reservar la información solicitada.

Ello porque, como también se dijo al resolver la clasificación de información CT-CI/A-20-2018, 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].

---

[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)

De lo cual se obtiene que 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 propagación pueda derivarse perjuicio por causa de interés público y seguridad nacional o pública.

Conforme a esto, el Director General de Tecnologías de la Información, sin precisar causal de reserva alguna, a grandes rasgos dijo que la divulgación de los datos solicitados podría exponer la capacidad de reacción de los sistemas de seguridad informáticos y propiciar el aumento y especificidad de ataques cibernéticos, al proporcionar información sensible de la operación y seguridad de los servicios publicados en Internet de este Alto Tribunal, ya que implicaría lo siguiente:

- De la cantidad y periodo de peticiones o ataques soportados, ante el límite de consumo de banda, podría generar que se reciba una cantidad superior al volumen del canal de comunicación, y con ello se causaría la caída de los portales de Internet de la Institución;
- Sobre el tipo de ataques, permitiría aumentar los ataques informáticos de manera específica contra las versiones y marca de los equipos de seguridad, así como recepción de otros ataques no recibidos o identificados previamente;
- Del lugar, permitiría que se aumente el número de ataques desde regiones o zonas donde se tiene permitido el flujo de tráfico hacia los portales de Internet de este Alto Tribunal.

Con lo anterior, se tiene que se ha dado cumplimiento a lo ordenado por este órgano colegiado, por parte de la instancia requerida, correspondiendo ahora realizar el estudio concreto de la clasificación de información.

Así, dada la motivación que da el área, se arriba a la conclusión que, en su caso y como se verá, pesaría la reserva establecida en la fracción I, del artículo 113, de la Ley General, que establece lo siguiente:

> ***"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;…"*

Esto porque, desde una óptica general, el objeto de la restricción de la información, como se ha visto, comprende garantizar el buen funcionamiento de los sistemas de seguridad informáticos ante posibles ataques cibernéticos[2], que en general pondrían en riesgo la información de este Alto Tribunal (tanto del quehacer jurisdiccional como administrativo), y con ello daría lugar su posible extracción, modificación o alteración, lo que en última instancia comprometería el ejercicio de los derechos de las personas (acceso a la justicia), lo que es concordante con lo establecido en el artículo décimo octavo, párrafo primero, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de las versiones públicas emitidos por el Sistema Nacional de Transparencia[3].

---

[2] *Según el Instituto Nacional de Estándares y Tecnologías (NIST, por sus siglas en inglés), ataque cibernético o "ciberataque", podría comprender "un intento de obtener acceso no autorizado a servicios, recursos o información, o un intento de comprometer la integridad, disponibilidad o confidencialidad del sistema" (visible en la siguiente página: https://csrc.nist.gov/Glossary/?term=3015#AlphaIndexDiv).*
Inclusive se encuentra tipificado como delito por el artículo 211 bis 2, del Código Penal Federal.

[3] *"**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*

Aunado a que resulta imperante que se cuenten con sistemas de seguridad basados, entre otros elementos, en una gestión que considere la prevención, detección y respuesta inmediata a los incidentes que afecten a los sistemas en general, tal y como lo disponen los principios 7 y 8 de las Directrices para la seguridad de sistemas y redes de información: hacia una cultura de seguridad[4] (directrices), de la OCDE (por sus siglas en inglés: *Organisation for Economic Co-operation and Development*).

Por otra parte, una vez identificada la causal de reserva, debe tenerse en cuenta que de conformidad con lo dispuesto en los artículos 100, último párrafo de la Ley General[5], en relación con el 17, párrafo

---

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…"

[4] *"**7) Diseño y realización de la seguridad.***
Los participantes deben incorporar la seguridad como un elemento esencial de los sistemas y redes de información.
Los sistemas, las redes y las políticas deberán ser diseñados, ejecutados y coordinados de manera apropiada para optimizar la seguridad. Un enfoque mayor pero no exclusivo de este esfuerzo ha de encontrarse en el diseño y adopción de mecanismos y soluciones que salvaguarden o limiten el daño potencial de amenazas o vulnerabilidades identificadas. Tanto las salvaguardas técnicas como las no técnicas así como las soluciones a adoptar se hacen imprescindibles, debiendo ser proporcionales al valor de la información de los sistemas y redes de información. La seguridad ha de ser un elemento fundamental de todos los productos, servicios, sistemas y redes; y una parte integral del diseño y arquitectura de los sistemas. Para los usuarios finales el diseño e implementación de la seguridad radica fundamentalmente en la selección y configuración de los productos y servicios de sus sistemas.
8) Gestión de la Seguridad.
Los participantes deben adoptar una visión integral de la administración de la seguridad.
La gestión de la seguridad debe estar basada en la evaluación del riesgo y ser dinámica, debiendo comprender todos los niveles de las actividades de los participantes y todos los aspectos de sus operaciones. Asimismo ha de incluir posibles respuestas anticipadas a riesgos emergentes y considerar la prevención, detección y respuesta a incidentes que afecten a la seguridad, recuperación de sistemas, mantenimiento permanente, revisión y auditoría. Las políticas de seguridad de los sistemas y redes de información, así como las prácticas, medidas y procedimientos deben estar coordinadas e integradas para crear un sistema coherente de seguridad. Las exigencias en materia de gestión de seguridad dependerán de los niveles de participación, del papel que desempeñan los participantes, del riesgo de que se trate y de los requerimientos del sistema…"

[5] ***"Artículo 100.*** *…*

primero, de los Lineamientos Temporales[6], es competencia del titular de la instancia que tiene bajo su resguardo la información requerida, determinar su disponibilidad y clasificarla conforme a los criterios establecidos en la normativa aplicable.

Conforme a lo anterior, se tiene que la Dirección General de Tecnologías de la Información es la área técnica que cuenta con el personal especializado para velar por la seguridad de la información y de los sistemas tecnológicos del Alto Tribunal, en términos de lo establecido por el artículo 27, fracción I, del Reglamento Orgánico en Materia Administrativa de la Suprema Corte de Justicia de la Nación[7].

En ese sentido, tratándose de cuestiones que atañen a la protección específica de los rubros que involucran aspectos vinculados con la infraestructura se seguridad informática del Alto Tribunal, es claro que cuando el área enteramente responsable ubica el surgimiento de elementos que inciden en la dimensión ya señalada, el órgano encargado de conocer del acceso sólo debe limitarse a entender y/o valorar la razonabilidad de la clasificación expresada para efecto de su confirmación o no.

Precisado lo anterior, corresponde ahora analizar, desde la razonabilidad de la motivación expresada por el área, si los datos

---

Los titulares de las Áreas de los sujetos obligados serán los responsables de clasificar la información, de conformidad con lo dispuesto en esta Ley, la Ley Federal y de las Entidades Federativas."

[6] ***"Artículo 17***
De la responsabilidad de los titulares y los enlaces
En su ámbito de atribuciones, los titulares de las instancias serán responsables de la gestión de las solicitudes, así como de la veracidad y confiabilidad de la información…"

[7] "***Artículo 27.*** *El Director General de Tecnologías de la Información tendrá las siguientes atribuciones:*
I. Administrar los recursos en materia de tecnologías de la información y comunicación y proveer los servicios que se requieran en la materia;…"

específicamente requeridos (número, tipo y lugar de origen de los ataques cibernéticos que se hubieren presentado en esta Suprema Corte de Justicia de la Nación) darían lugar o no a la clasificación total de la información solicitada.

a) Tipo y lugar de origen de los ataques cibernéticos. Por cuanto estos datos, ante la razón desprendida de los informes presentados por el área requerida y responsable, este Comité de Transparencia identifica, como se ha venido señalando, que se pretende proteger, desde un esquema global, la infraestructura de seguridad informática de este Alto Tribunal, en tanto que se podrían involucrar negativamente aspectos de seguridad pública, y con ello facilitar un ataque cibernético, con repercusiones como son, por una parte, facilitar la extracción, modificación o alteración de información sensible de los expedientes jurisdiccionales, lo que incide directamente en su tarea sustantiva, y por otra parte, comprometerse la información administrativa, que generaría un probable riesgo a las personas en lo particular como son trabajadores y proveedores, al hacerse patente un acceso no autorizado ni controlado a los datos personales que se tengan registrados, e inclusive información contable o bancaria, por solo citar algunos casos.

Con base en lo hasta aquí dicho, este Comité estima que la clasificación antes advertida también se sustenta, desde la especificidad que en aplicación de la prueba de daño mandatan los artículos 103 y 104 de la Ley General, cuya delimitación, como se verá enseguida, necesariamente debe responder a la propia dimensión del supuesto de reserva con el que se relaciona su valoración.

Lo anterior, porque, se podrían poner en riesgo cuestiones de seguridad pública, pues según se refirió previamente, a partir de la información solicitada, si se divulgara, sería posible perfeccionar un ataque cibernético, o bien intentos de otros no recibidos o identificados hasta el momento, al contar con factores de reconocimiento sobre la infraestructura de seguridad informática de la Suprema Corte de Justicia de la Nación, a partir de los ataques registrados y mitigados, lo que evidentemente si pesa sobre la capacidad de respuesta.

En ese orden de ideas, como se anunciaba previamente, lo que se impone es **confirmar** la determinación del área, para efecto de confirmar la reserva de la información solicitada, por un plazo de cinco años en atención a lo establecido por el artículo 101[8], de la Ley General.

b) Número de ataques cibernéticos. Sobre este apartado, se tiene que el área responsable dijo que dar a conocer la cantidad y

---

[8] ***"Artículo 101.*** *Los Documentos clasificados como reservados serán públicos cuando:*

I. Se extingan las causas que dieron origen a su clasificación;
II. Expire el plazo de clasificación;
III. Exista resolución de una autoridad competente que determine que existe una causa de interés público que prevalece sobre la reserva de la información, o
IV. El Comité de Transparencia considere pertinente la desclasificación, de conformidad con lo señalado en el presente Título.

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.

Excepcionalmente, los sujetos obligados, con la aprobación de su Comité de Transparencia, podrán ampliar el periodo de reserva hasta por un plazo de cinco años adicionales, siempre y cuando justifiquen que subsisten las causas que dieron origen a su clasificación, mediante la aplicación de una prueba de daño.

Para los casos previstos por la fracción II, cuando se trate de información cuya publicación pueda ocasionar la destrucción o inhabilitación de la infraestructura de carácter estratégico para la provisión de bienes o servicios públicos, o bien se refiera a las circunstancias expuestas en la fracción IV del artículo 113 de esta Ley y que a juicio de un sujeto obligado sea necesario ampliar nuevamente el periodo de reserva de la información; el Comité de Transparencia respectivo deberá hacer la solicitud correspondiente al organismo garante competente, debidamente fundada y motivada, aplicando la prueba de daño y señalando el plazo de reserva, por lo menos con tres meses de anticipación al vencimiento del periodo."

periodo de ataques informáticos podría generar un aumento dirigido a superar la volumetría del canal de comunicación.

Sin embargo, se considera que es factible dar a conocer, de forma global, el número de ataques cibernéticos que ha recibido este Alto Tribunal del uno de enero al cinco de julio de este año.

Lo anterior en virtud de que, por una parte, si bien es cierto que la volumetría posiblemente influiría en la cantidad de ataques cibernéticos, ello no trascendería en la forma o base de éstos, que podría repercutir en su perfeccionamiento, aunado a que la determinación del número de intentos puede erigirse por la simple voluntad de los actores.

Por otra parte, y sobre todo, debe tomarse en cuenta que, conforme a los principios 1, 3 y 5, de las directrices[9], la seguridad de los

---

[9] "***1) Concienciación***
Los participantes deberán ser conscientes de la necesidad de contar con sistemas y redes de información seguros, y tener conocimiento de los medios para ampliar la seguridad.
El conocimiento de los riesgos y de los mecanismos disponibles de salvaguardia, es el primer paso en la defensa de la seguridad de los sistemas y redes de información. Estos sistemas y redes de información pueden verse afectados tanto por riesgos internos como externos. Los participantes deben comprender que los fallos en la seguridad pueden dañar significativamente los sistemas y redes que están bajo su control. Deben asimismo ser conscientes del daño potencial que esto puede provocar a otros derivados de la interconexión y la interdependencia. Los participantes deben tener conocimiento de las configuraciones y actualizaciones disponibles para sus sistemas, así como su lugar que ocupan dentro de las redes, las prácticas a ejecutar para ampliar la seguridad, y las necesidades del resto de los participantes.
3) Respuesta
Los participantes deben actuar de manera adecuada y conjunta para prevenir, detectar y responder a incidentes que afecten la seguridad.
Al reconocer la interconexión de los sistemas y de las redes de información, así como el riesgo potencial de un daño que se extienda con rapidez y tenga una [sic] alcance amplio, los participantes deben actuar de manera adecuada y conjunta para enfrentarse a los incidentes que afecten la seguridad. Asimismo han de compartir información sobre los riesgos y vulnerabilidades y ejecutar procedimientos para una cooperación rápida y efectiva que permita prevenir, detectar y responder a incidentes que afecten a la seguridad. Cuando sea posible, estas actuaciones habrán de suponer un intercambio de información y una cooperación transfronteriza.
5) Democracia.

sistemas y redes de información habrán de ser consistentes con los valores de *concienciación, respuesta y democracia*, es decir, partir del conocimiento de los riesgos potenciales para actuar de forma adecuada, lográndose de manera consistente con la garantía de derechos reconocidos como son la protección de la información personal, la apertura y la transparencia.

Así, el factor de conocimiento del número de ataques si es viable de entrega, dado que es relevante que la sociedad y las personas que en concreto se relacionan con este Alto Tribunal (por ser trabajadores, proveedores o usuarios del sistema judicial, por citar algunos casos) tengan un parámetro de entendimiento y confianza sobre la seguridad de resguardo de sus datos, conforme a la capacidad de afrontar los riesgos de ciberataques, de ahí que, como se dijo en la clasificación de información CT-CI/A-20-2018: "*el acceso a la información no puede entenderse sustentado en un principio de riesgo futuro o de malicia de quien acude a su ejercicio*".

En consecuencia, se **revoca** la clasificación efectuada por el área con relación al número de ataques cibernéticos que ha recibido este Alto Tribunal del uno de enero al cinco de julio de este año.

Por tanto, de conformidad con lo dispuesto por el artículo 37, párrafo quinto, de los Lineamientos Temporales[10], se **requiere** al

---

La seguridad de los sistemas y redes de información debe ser compatible con los valores esenciales de una sociedad democrática.
La seguridad debe lograrse de manera consistente con garantía de los valores reconocidos por las sociedades democráticas, incluyendo la libertad de intercambio de pensamiento e ideas, así como el libre flujo de información, la confidencialidad de la información y la comunicación y la protección apropiada de información personal, apertura y transparencia."

[10] "***Artículo 37***
Del cumplimiento de las resoluciones
(…)

Director General de Tecnologías de la Información, para que en el plazo de dos días hábiles, computados a partir del día siguiente al en que surta sus efectos la notificación de la presente resolución, remita a la Unidad General de Transparencia y Sistematización de la Información Judicial, el informe de forma global, sobre el número de ataques cibernéticos que ha recibido este Alto Tribunal del uno de enero al cinco de julio de este año, para ésta a su vez comunique el dato a la persona solicitante.

Por lo expuesto y fundado; se,

R E S U E L V E:

PRIMERO. Se tiene por atendido el requerimiento efectuado a la Dirección General de Tecnologías de la Información.

SEGUNDO. Se confirma la clasificación de información, en términos de lo expuesto en el considerando II, inciso a), de la presente resolución.

TERCERO. Se revoca la clasificación de información según se expuso en el considerando II, inciso b), de esta determinación.

CUARTO. Se requiere a la Dirección General de Tecnologías de la Información y a la Unidad General de Transparencia y

---

Cuando el dictamen aprobado por el Comité determine incumplida la resolución, se apercibirá a la instancia respectiva para que, en un plazo no mayor a dos días hábiles, cumpla con la resolución del Comité e informe tal circunstancia al Secretario. Advirtiéndole que en caso de un nuevo incumplimiento se dará vista a la Contraloría de la Suprema Corte…"

Sistematización de la Información Judicial para que realicen las acciones referidas en la parte final de esta resolución.

Notifíquese al solicitante, a la instancia requerida y en su oportunidad, archívese como asunto concluido.

Así, por unanimidad de votos, lo resolvió el Comité de Transparencia de la Suprema Corte de Justicia de la Nación, y firman los licenciados Alejandro Manuel González García, Secretario Jurídico de la Presidencia, Presidente; Magistrado Constancio Carrasco Daza, Titular de la Unidad General de Enlace con los Poderes Federales; y Juan Claudio Delgado Ortiz Mena, Contralor del Máximo Tribunal, integrantes del Comité, ante el Secretario del Comité, que autoriza y da fe.

LICENCIADO ALEJANDRO MANUEL GONZÁLEZ GARCÍA
PRESIDENTE DEL COMITÉ

MAGISTRADO CONSTANCIO CARRASCO DAZA
INTEGRANTE DEL COMITÉ

LICENCIADO JUAN CLAUDIO DELGADO ORTIZ MENA
INTEGRANTE DEL COMITÉ

LICENCIADO LUIS RAMÓN FUENTES MUÑOZ
SECRETARIO DEL COMITÉ