CUMPLIMIENTO CT-CUM/A-37-2018
Derivado del expediente CT-CI/A-21-2018

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 catorce de noviembre de dos mil dieciocho.

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

I. Solicitud de información. El uno de agosto de dos mil dieciocho, se recibieron en la Plataforma Nacional de Transparencia las solicitudes tramitadas con los folios 0330000142318 y 0330000142418, requiriendo:

> *"1. Los nombres de dominio cuya titularidad ostenta el sujeto obligado, proporcionando en formato electrónico evidencia de su adquisición, sea contrato o cualquier otro documento, y de sus posteriores renovaciones.*
>
> *2. De haber sufrido ciberocupación, ocupación ilegítima o realizaran alguna reclamación sobre un nombre de dominio, solicito la demanda ante el proveedor de servicios de disputa de nombres de dominio en formato electrónico, correos electrónicos de comunicación y notificaciones, así como la resolución recaída, así como los comprobantes de cualquier erogación realizada por ese concepto.*
>
> *3. La lista de los nombres de dominio que han sido adquiridos desde 1990 hasta la fecha de la solicitud, desglosado por nombre de dominio, fecha de adquisición, si sigue activo o se perdió y la evidencia de su adquisición, así como las razones por las que aún se conservan o se han perdido,*
>
> *En caso de que la información no pudiera ser entregada vía PNT, solicito sea entregada mediante el correo electrónico que aparece en el detalle de la solicitud."*

II. Resolución del Comité de Transparencia de la Suprema Corte de Justicia de la Nación. En sesión de cinco de septiembre de dos mil dieciocho, este Comité de Transparencia emitió resolución en el expediente CT-CI/A-21-2018, conforme se transcribe y subraya en lo conducente:

*"**II. Análisis.** Como se aprecia del antecedente I, en la solicitud de origen se pide diversa información sobre los "nombres de dominio" de la Suprema Corte de Justicia de la Nación.*

En respuesta a lo anterior, la Dirección General de Tecnologías de la Información informó que la divulgación de esa información podría comprometer, en distintos aspectos, la infraestructura tecnológica de este Alto Tribunal, de ahí que procedió a su reserva en términos del artículo 113, fracción XI de la Ley General de Transparencia.

Sobre esa base, el punto a dilucidar a través del caso que nos ocupa radica en determinar si sobre la información requerida se actualiza o no la reserva identificada por el área instada a su divulgación y, en su caso, si aquella puede o no ser proporcionada en los términos solicitados.

(…)

Trasladado al caso, como se vio en el apartado de antecedentes, para sustentar la reserva debatida, el área manifestó expresamente que divulgar lo solicitado pondría en riesgo la información de la institución porque:

- *Los nombres de dominio están asociados a una dirección "IP", la cual permite determinar la ubicación física de los equipos principales y de respaldo, así como las capacidades de funcionamiento de los portales "web" del Alto Tribunal.*
- *En los dominios se almacena información para los ciudadanos, justiciables y áreas internas de la Suprema Corte.*
- *Los dominios de respaldo sirven de apoyo para los casos en que el dominio principal sufra caídas, fallas o intermitencias y con ello garantizar la continuidad de las operaciones de la institución.*
- *Dar a conocer el nombre de dominio implicaría dejar al descubierto y expuesta la ubicación física de los equipos en que se alojan los portales web del Alto Tribunal y con ese dato se comprometería la disponibilidad e integridad de dichos portales, al enviar constantes peticiones (ataques) a los nombre de dominio principales y de respaldo, generando con ello saturación por la alta demanda de peticiones permanentes y, con ello, generar fallas en el servicio.*
- *Se cuenta con un plan de recuperación de desastres para los portales de Internet del Alto Tribunal con esquemas de continuidad y de recuperación a través de sus dominios, pero ante ataques simultáneos se pueden afectar, de manera directa, tanto los dominios principales, como los secundarios.*
- *Proporcionar cualquier dato relacionado con los dominios vulnera la seguridad y operatividad de la infraestructura tecnológica que sirve como apoyo a la operación de las áreas del Alto Tribunal; además, en dichos dominios se publica "El Sistema Electrónico del Poder Judicial" en el que los justiciables ingresan promociones en juicios que no han causado estado, pudiendo afectar las funciones sustantivas de la Suprema Corte de Justicia de la Nación.*

*Lo antes reseñado fue clasificado como información **reservada**, al estimar actualizada la hipótesis del artículo 113, fracción XI de la Ley General de Transparencia, en virtud de que se podría vulnerar la seguridad y operatividad de la infraestructura tecnológica que sirve de apoyo a la operación de las áreas del Alto Tribunal, lo que podría afectar las funciones sustantivas de la Suprema Corte de*

Justicia de la Nación porque en los dominios se publica "El Sistema Electrónico del Poder Judicial". Dicho artículo establece:

(…)

Al respecto, el contraste entre la justificación proporcionada por el área requerida y los supuestos contenidos en el precepto transcrito, permiten evidenciar que dicha motivación resulta indebida, ya que si bien es cierto que, en principio, como este Comité ha sostenido en otros asuntos[2], la posible afectación de los sistemas tecnológicos de este Alto Tribunal podría generar un acceso no controlado y no permitido a la información de los expedientes judiciales o procedimientos administrativos seguidos en forma de juicio, también lo es que junto a la tarea sustantiva de este Tribunal Constitucional, que se traduce en la emisión de sentencias dentro de los diversos expedientes de los que toca conocer, prevalecen múltiples actividades administrativas para su debido desarrollo, sobre cuya vigencia, en este caso, no podría entenderse actualizada la hipótesis ya descrita.

En efecto, como se dijo al resolver la clasificación de información CT-CI/A-3-2018, en sesión de dieciocho de abril de presente año, "no todo el cúmulo de herramientas o instrumentos tecnológicos con los que opera la Suprema Corte de Justicia de la Nación se encuentran vinculados o referenciados con los expedientes judiciales, sino que también prevalecen sistemas orientados a la gestión de su administración (recursos humanos, adquisiciones, contabilidad, etcétera), de ahí que, por tal motivo, en estos casos la materialización de la causa de reserva no puede predicarse de manera general o abstracta, siendo que, además, tal supuesto limita al espacio de los expedientes judiciales.

En otro orden de ideas, 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.

Ello, de conformidad con lo dispuesto en los artículos 100, último párrafo de la Ley General[3], en relación con el 17, párrafo primero de los Lineamientos Temporales[4], en tanto 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, además de que es la única área técnica que cuenta con el personal especializado para velar por la

---

[2] Tal como fue el CT-CI/A-7-2018, de treinta de mayo de este año.
[3] (…)
[4] (…)

seguridad de la información y de los sistemas tecnológicos del Alto Tribunal, en términos de lo dispuesto por el artículo 27, fracción XI del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación[5].

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.

Junto a lo anterior, y solo a manera de ejemplo, se tiene que algunos sujetos obligados, como es el caso del Banco de México[6] y el Centro de Investigación y Seguridad Nacional "Cisen"[7], han informado, en mayor o menor medida, sobre los ciberataques de los que han sido objeto, lo que refuerza la idea de que se explique con mayor precisión, para cada punto planteado en la solicitud de acceso, porqué podría determinarse la reserva, o bien, porqué sería factible la divulgación.

Por tanto, de conformidad con lo dispuesto por el artículo 37, párrafos primero y segundo, de los Lineamientos Temporales[8], 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.*

Por lo expuesto y fundado; se,

R E S U E L V E:

ÚNICO. *Se requiere al Director General de Tecnologías de la Información, en términos de lo expuesto en esta resolución."*

III. Requerimiento para cumplimiento. Mediante oficio CT-1393-2018, notificado el trece de septiembre último, el Secretario de este Comité de Transparencia notificó a la Dirección General de Tecnologías de la Información la resolución antes transcrita.

IV. Informe de la Dirección General de Tecnologías de la Información. El veinticuatro de septiembre de dos mil dieciocho, se recibió en la Secretaría del Comité de Transparencia el oficio DGTI/DAPTI-2004-2018, con el que se remitió un documento titulado ***"Nombre de Dominio, Prueba de Daño"***, en el que se informa:

---

[5] (…)
[6] (…)
[7] (…)
[8] (…)

"Para poder acceder a un servicio publicado en internet se hace uso de una dirección web, la cual está asociada a un dominio o subdominio. Con el nombre de dominio se puede identificar de manera fácil y sencilla un servicio web, sin nombres de dominio, las direcciones web serían una serie de números, o direcciones IP, casi imposibles de recordar.

A fin de ejemplificar, para poder acceder al portal web de la SCJN se hace uso del nombre de subdominio www.scjn.gob.mx el cual este (sic) *compuesto del dominio principal de la SCJN* ***scjn.gob.mx*** *y de un subdominio donde se ubica el servicio de publicación denominado* ***www****.*

Para que un equipo de cómputo obtenga la dirección IP del nombre del dominio o subdominio del servicio web que se desea consultar, se hace uso de un servicio denominado DNS (Domain Name System), este sistema se encarga de interpretar el nombre del dominio y de indicarle al equipo de cómputo cuál es el valor numérico del dominio correspondiente.

La SCJN cuenta con un servicio de DNS propio, mediante este servicio se atienden todas las consultas de los justiciables y servidores públicos que requieran acceder a los servicios internos y portales web de la SCJN. En caso de falla o afectación de este servicio no se podrá acceder a ningún portal web de esta (sic) *Alto Tribunal, teniendo repercusiones legales derivados de los marcos normativos de la Ley de Amparo y demás leyes aplicables para los servicios de FIREL y de los Portales web de la SCJN.*

La SCJN hace uso de nombres de dominios para el acceso de servicios internos y servicios externos, los cuales se clasifican de la siguiente manera:

Servicios internos:

- *Servicios de videoconferencia.*
- *Servicios de telefonía IP*
- *Servicios de comunicación Lync (Skype Empresarial)*
- *Servicios de antivirus*
- *Servicios de correo electrónico*
- *Servicios de DNS*
- *Servicios de continuidad de operación*
- *Servicios de conexión remota (VPN para conexión remota a la SCJN)*

Servicios externos:

- *Portales web de la SCJN*
- *Portales web del PJF*
- *Sistema Electrónico del PJF*

Los nombres de dominios de los portales web son de uso público y pueden ser consultados desde cualquier navegador web, los servicios internos son de uso exclusivo para los servidores públicos de la SCJN, toda vez que implican servicios que provee la SCJN únicamente a su personal interno; adicionalmente dentro de los nombre (sic) *de dominio para servicios internos de la SCJN existen aquellos que únicamente son consultados entre sistemas, por lo que únicamente el personal técnico de la SCJN está autorizado a su uso y configuración.*

En internet cada día se hace uso de diferentes técnicas, herramientas, malware y ataques para obtener información sensible de usuarios, empresas e instituciones. Esta información puede ser usada para extorsión, robo de información, divulgación, o simplemente para la obtención de una remuneración.

Entre estas técnicas se tiene la técnica denominada 'Phisihing', la cual consiste en suplantar la identidad de una personal, (sic) *empresa o institución para obtener información sensible de su víctima. Este tipo de ataques puede ser realizados* (sic) *vía internet, correo electrónico, mensajes de teléfono, llamadas telefónicas, etc.*

Entre los casos más difundidos se encuentra el caso de un correo proveniente de la Comisión Federal de Electricidad (CFE), el cual proviene de un dominio de la dependencia servicioalcliente@cfe.gob.mx, en el cual se exhorta al cliente a ingresar a una liga web con la finalidad de recibir un descuento sobre una deuda del consumidor, este correo se hace pasar por CFE y tratar de obtener de manera ilícita información sensible del usuario. Referencia http://www.eluniversal.com.mx/cartera/finanzas/cfe-alerta-sobre-correo-electronico-falso

Ahora bien, dar a conocer al público los dominios de la SCJN, podría traer como consecuencia que la ciberdelincuencia realice ataques de Phishing en nombre de este Alto Tribunal, tal y como sucedió con CFE, donde a partir del nombre de dominio de correo electrónico o de sus servicios internos, realicen una suplantación de identidad de la SCJN; tal podría ser el caso del Sistema de la FIREL, el cual en caso de ser suplantado podría robar la firma electrónica de los usuarios, así como sus claves de acceso del Sistema Electrónico, teniendo como consecuencia el acceso no autorizado a los expedientes electrónicos de los justiciables, así como a los procesos jurídicos de la SCJN.

Aunado a ello, la exposición de los nombres de dominios de los servicios internos podría tener la intensión de revelar información sensible de servicios de la SCJN, con la finalidad de realizar ataques o intentos de acceso, los cuales en caso de concretarse tendrían acceso información (sic) *confidencial de la SCJN, tal y como se describe en la siguiente tabla:*

Servicio	*Repercusión en caso de concretar un ataque*
Servicios de videoconferencia.	*Espiar conversaciones del personal de la SCJN, así como su divulgación.*
Servicios de telefonía IP	*Espiar conversaciones del personal de la SCJN, así como su divulgación.*
Servicios de comunicación Lync (Skype Empresarial)	*Espiar conversaciones del personal de la SCJN, así como su divulgación.*
Servicios de correo electrónico	*Realizar ataques de phishing o de usurpación de identidad.*
Servicios de DNS	*Evitar el acceso a cualquier servicio publicado en internet.*
Servicios de continuidad de operación.	*Afectar a servicios de publicación web de la SCJN*
Servicios de conexión remota (VPN para conexión remota de la SCJN).	*Acceso a la red interna de la SCJN. Implicación robo de información, acceso a sistemas internos, modificación o eliminación de información.*

Conclusiones:

De acuerdo a lo antes descrito se reitera que la información solicitada por el usuario sea considerada como reservada 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 estos sistemas.

Cabe precisar, que este tipo de información evidentemente es solicitada por personal experto en la materia, situación que al no ser de uso cotidiano, se requiere de sensibilización en el tema de seguridad informática."

Al oficio transcrito se adjuntó la impresión de una nota periodística.

V. Acuerdo de turno. Mediante proveído de veinticuatro de septiembre de dos mil dieciocho, el Presidente del Comité de Transparencia de este Alto Tribunal, con fundamento en los artículos 44, fracción I de la Ley General de Transparencia y Acceso a la Información Pública, así como 23, fracción I y 27 del Acuerdo General de Administración 5/2015, ordenó integrar el expediente de cumplimiento **CT-CUM/A-37/2018** y remitirlo al Contralor del Alto Tribunal, por ser el ponente de la resolución precedente, a fin de que presentara la propuesta sobre el cumplimiento de lo ordenado por este Comité, lo que se hizo mediante oficio CT-1449-2018 en la misma fecha.

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

I. 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, fracción I de la Ley General de Transparencia y Acceso a la Información Pública, así como 23, fracción I del Acuerdo General de Administración 5/2015.

II. Análisis de cumplimiento. En la resolución emitida en la clasificación CT-CI/A-21-2018, se determinó requerir a la Dirección General de Tecnologías de la Información para que precisara y justificara, de forma suficiente, desde la especifica prueba de daño, la reserva de la información

requerida, conforme a las hipótesis previstas en el artículo 113 de la Ley General de Transparencia.

En cumplimiento a lo anterior, sin precisar una causa de reserva específica, el Director General de Tecnologías de la Información señala que la divulgación de los datos solicitados podría proporcionar información sensible de la operación y seguridad de los servicios publicados en Internet de este Alto Tribunal, por los motivos que se reseñan:

- Para acceder a un servicio publicado en Internet se hace uso de una dirección *"web"* que se encuentra asociada a un dominio o subdominio, precisando que el dominio es identificable fácilmente y las direcciones *"web"* no lo son, por tratarse de números o direcciones *"IP"*, para lo cual se indica como ejemplo que el portal web del Alto Tribunal se compone del dominio principal *"scjn.gob.mx"* y de un subdominio *"www"*.
- Para obtener la dirección *"IP"* del nombre de un dominio o subdominio del servicio *"web"* que se desea consultar, se hace uso de un sistema denominado *"DNS"* (*"Domain Name System"*), el cual interpreta el nombre del dominio y le indica al equipo de cómputo del que se accede, el valor número del dominio correspondiente.
- La Suprema Corte de Justicia de la Nación cuenta con un *"DNS"* propio con el que se atienden todas la consultas de los justiciables y de los servidores públicos que requieren acceder a los servicios internos y portales *"web"* internos, por lo que en caso de falla no se puede acceder a los mismos, originando repercusiones legales
- Los nombres de dominios de portales *"web"* son de uso público y pueden ser consultados desde cualquier navegador, pero los servicios internos son de uso exclusivo para los servidores públicos del Alto Tribunal, dentro de los cuales se encuentran aquéllos que son consultados entre sistemas y que únicamente compete al personal técnico de la Suprema Corte su uso y configuración.

- En Internet se hace uso de técnicas, herramientas, *“malware”* y ataques para obtener información sensible de usuarios, empresas e instituciones y, con ello, extorsionar, robar información, divulgarla o solicitar remuneraciones.
- Entre las técnicas referidas se encuentra la denominada *“Phishing”* que consiste en suplantar la identidad de una persona, empresa o institución para obtener información sensible de su víctima y dicha técnica puede ser utilizada vía Internet, correo electrónico, mensajes de teléfono o llamadas telefónicas, lo cual se ejemplifica con una nota periodística en la que, mediante un correo electrónico de la Comisión Federal de Electricidad se solicitaba ingresar a una liga para obtener un descuento de una deuda del consumidor.
- Dar a conocer los dominios del Alto Tribunal podría generar que la ciberdelincuencia realice ataques de *“Phishing”*, como pudiera ser al Sistema de la Firma Electrónica (FIREL), accediendo a expedientes electrónicos de los justiciables, así como a los procesos jurídicos de la Suprema Corte.
- La exposición de los nombres de dominio de los servicios internos podría revelar información sensible de servicios del Alto Tribunal, lo que permitiría realizar ataques o intentos de acceso a tales servicios (servicios de videoconferencia, servicios de telefonía *“IP”*, servicios de comunicación Lync, servicios de correo electrónico, servicios *“DNS”*, servicios de continuidad de operación, servicios de conexión remota *“VPN”*).
- La información requerida por el peticionario debe ser considerada como reservada, porque su divulgación puede originar que se acceda a información sensible de la operación y seguridad de los servicios en Internet de la Suprema Corte de Justicia de la Nación, derivando en ataques informáticos, afectación y degradación de estos sistemas.

No obstante lo expuesto por la instancia requerida, este Comité de Transparencia advierte que, contrario a lo que sostiene, algunos dominios son públicos y, a través de ellos, se permite el acceso a la información que tiene publicada en medios electrónicos este Alto Tribunal, destacando, por ejemplo, el dominio relativo al portal de Internet http://www.scjn.gob.mx, el cual se menciona en el propio informe que se analiza como un dominio público, o bien, el correspondiente al Canal Judicial, http://canaljudicial.mx

Derivado de lo expuesto, se estima que a pesar de la exposición que se realiza en el oficio de la Dirección General de Tecnologías de la Información, este Comité no cuenta con los elementos suficientes que le permitan confirmar o no la reserva que hace respecto de la información solicitada, pues a partir de la afirmación de que todo lo relativo a los dominios es reservado, se pretender dar respuesta a la totalidad de los planteamientos formulados en la solicitud de origen; sin embargo, como ya se hizo notar, se tiene conocimiento de nombres de dominio que son públicos.

Por lo anterior, tomando en cuenta que este órgano colegiado es la instancia competente para dictar las medidas necesarias para garantizar el ejercicio del derecho de acceso a la información de los peticionarios, atendiendo al principio de máxima publicidad, con apoyo en los artículos 44, fracción I de la Ley General de Transparencia y Acceso a la Información Pública, 23, fracción I y 37 del Acuerdo General de Administración 5/2015, se requiere al titular de la Dirección General de Tecnologías de la Información, por conducto de la Secretaría Técnica de este Comité, para que en un plazo de dos días hábiles posteriores a la notificación de la presente resolución, emita un informe en el que considerando lo expuesto en esta resolución, y sólo en la medida en que no comprometa la seguridad, dé respuesta puntual a la solicitud de origen, en los siguientes términos:

1. Nombre de los dominios de los que la Suprema Corte de Justicia de la Nación es titular, señalando la disposición, clasificación y, en su caso, modalidad de acceso al contrato o documentos relativos a su adquisición o renovaciones posteriores.
2. *De haber sufrido ciberocupación, ocupación ilegítima o realizaran alguna reclamación sobre un nombre de dominio, solicito la demanda ante el proveedor de servicios de disputa de nombres de dominio en formato electrónico, correos electrónicos de comunicación y notificaciones, así como la resolución recaída, así como los comprobantes de cualquier erogación realizada por ese concepto*.
3. Listado de nombres de dominio adquiridos de 1990 a la fecha de la solicitud, señalando el nombre de dominio, la fecha de adquisición, si el dominio sigue activo o se perdió, la evidencia de su adquisición, así como las razones por las que aún se conservan esos dominios o por las que se han perdido.

Por lo expuesto y fundado; se,

R E S U E L V E:

ÚNICO. Se requiere a la Dirección General de Tecnologías de la Información, en los términos señalados en la presente 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 Alejandro Manuel González García, Secretario Jurídico de la Presidencia y Presidente del Comité, y el licenciado Juan Claudio Delgado Ortiz Mena, Contralor del Alto Tribunal. Ausente el Magistrado Constancio Carrasco Daza, titular de la Unidad

General de Enlace con los Poderes Federales. Firma el secretario del Comité que autoriza.

LICENCIADO ALEJANDRO MANUEL GONZÁLEZ GARCÍA
PRESIDENTE DEL COMITÉ

LICENCIADO JUAN CLAUDIO DELGADO ORTIZ MENA
INTEGRANTE DEL COMITÉ

LICENCIADO LUIS RAMÓN FUENTES MUÑOZ
SECRETARIO DEL COMITÉ