Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Expediente: RRA 6073/18
Sujeto obligado: Secretaría de Relaciones Exteriores
Folio de la solicitud: 0000500130518
Comisionado Ponente: Carlos Alberto Bonnin Erales

Visto el expediente del recurso de revisión citado al rubro, interpuesto ante este Instituto, se procede a dictar la presente resolución con base en los siguientes:

RESULTANDOS

1. Solicitud de información. El siete de agosto de dos mil dieciocho, mediante la Plataforma Nacional de Transparencia, una persona presentó una solicitud de acceso a la información pública ante la Secretaría de Relaciones Exteriores, requiriendo lo siguiente:

> **Modalidad preferente de entrega:** "Entrega por Internet en la PNT"
>
> **Descripción de la solicitud de información:** "Con fundamento en el artículo 6 constitucional, atentamente requiero que en función de los principios constitucionales de máxima publicidad, transparencia, rendición de cuentas y gratuidad, me entregue a través de un medio gratuito derivado de los avances tecnológicos y en formato de documento portátil (PDF) comprimido o en diverso de naturaleza similar, la siguiente información pública documentada en el ejercicio de las facultades, competencias y funciones previstas en las normas jurídicas aplicables. 1. Ordenado por Número de serie, de cada uno de los equipos de cómputo y de cada uno de los MODEMS, ROUTERS (rúters) o Puntos de acceso inalámbricos, en posesión del sujeto obligado. a. Nombre de aquellas personas físicas que cuentan con las contraseñas administrativas o su equivalente (permisos informáticos, credenciales administrativas, privilegios de superusuario "su", "root", etc.) para el manejo, administración y control de la configuración de cada equipo. b. Tipo de contratación, empleo, cargo o comisión que desempeñan las personas que resulten del inciso a. c. Forma en que cada equipo obtiene o asigna, según sea el caso, la dirección IP (por sus siglas en ingles Internet protocol) privada en la red (de forma manual o por medio del Protocolo de Configuración Dinámica de Host DHCP, por sus siglas en ingles Dynamic Host Configuration Protocol). d. Domicilio actual en donde se encuentra físicamente cada equipo." (sic)

2. Respuesta a la solicitud. El veintinueve de agosto del dos mil dieciocho, el sujeto obligado, a través de la Plataforma Nacional de Transparencia, notificó al particular la reserva de parte de la información que da respuesta a la solicitud de acceso a la información, en los términos siguientes:

"...

Con fundamento en la Ley General de Transparencia y Acceso a la Información Pública, la información no puede ser proporcionada debido a que es:

Reservada 5 años

Motivo del daño por divulgar la información:
Ver archivo anexo

Ley	**Artículo y fracción**
LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL	Artículo 110, fracción I de la LFTAIP.

..." (sic)

El sujeto obligado adjuntó copia digitalizada de los documentos siguientes:

a) Oficio número UDT-4459/2018, del veintinueve de agosto de dos mil dieciocho, emitido por la Titular de la Unidad de Transparencia del sujeto obligado, y dirigido al solicitante, en los siguientes términos:

"...
Como respuesta a su solicitud presentada a través de la Plataforma Nacional de Transparencia, me permito hacer de su conocimiento la resolución que el Comité de Transparencia de la Secretaría de Relaciones Exteriores pronunció con motivo de la solicitud de acceso a la información. Se acompaña copia del oficio CTA-21718.

Se reitera el interés de esta Unidad de Transparencia en atender su solicitud y se hace de su conocimiento el derecho de interponer recurso de revisión ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, de conformidad con los Artículos 147, 148 y 149 de la Ley Federal de Transparencia y Acceso a la Información Pública.
..." (sic)

b) Oficio número CTA-21718, del veintiocho de agosto de dos mil dieciocho, suscrita por los integrantes del Comité de Transparencia de la Secretaría de Relaciones Exteriores, emitida en los términos siguientes:

"...
Visto el expediente que contiene la solicitud de acceso a la información anotada al rubro, el Comité de Transparencia de la Secretaria de Relaciones Exteriores ha procedido a analizar

de forma exhaustiva el contenido de las misma y la respuesta emitida por la **DIRECCIÓN GENERAL DE TECNOLOGÍAS DE INFORMACIÓN E INNOVACIÓN** mediante correo electrónico TIN-3159 de fecha 27 de agosto de 2018, de la que se desprende la clasificación de parte la información solicitada como **RESERVADA**, atendiendo a las siguientes consideraciones:

[Se transcribe la solicitud de acceso a la información]

Respuesta de la Unidad Administrativa consultada: la **DIRECCIÓN GENERAL DE TECNOLOGÍAS DE INFORMACIÓN E INNOVACIÓN** mediante correo electrónico TIN-3159 de fecha 27 de agosto de 2018, emitió su pronunciamiento en los siguientes términos:

> ***"Para las preguntas: 1. Los números de serie de cada uno de los equipos de cómputo y de cada MODEMS, ROUTERS (rúters) o Puntos de acceso inalámbricos en posesión del sujeto obligado:***
>
> ***a. Nombre de aquellas personas físicas que cuentan con las contraseñas administrativas o su equivalente para el manejo, administración y control de la configuración de cada equipo.***
> ***b. Tipo de contratación, empleo, cargo o comisión que desempeñan las personas que resulten del inciso a***
> ***c. Forma en que cada equipo obtiene o asigna, según sea el caso, la dirección IP privada en la red de forma manual o por medio del Protocolo de Configuración Dinámica de Host DHCP.***

La información solicitada, en la pregunta 1 e inciso c) respecto al número de serie de los equipos de cómputo y la forma en que cada equipo obtiene o asigna la dirección IP, se manifiesta que dicha información compromete la seguridad nacional y revela especificaciones técnicas de equipos útiles a la generación de inteligencia, por lo que no se encuentran abiertos a toda persona, aunado a que si bien es cierto existe la información de los equipos en las páginas del fabricante, también lo es que están enumerados de conformidad con sus características, sin que se especifique quienes son sus compradores, la finalidad para la que fueron adquiridas; ni las ubicaciones de los equipos, por lo que al proporcionar la información solicitada el usuario conocerá específicamente los equipos que se encuentran en las unidades administrativas que integran de esta Secretaría y por lo tanto se podrían lanzar ataques cibernéticos desde alguno o algunos de los equipos de la red de computadoras, introducir algún tipo de malware a la red, infectar el portal web o incluso paralizar las actividades de la red de computadoras, entre otras.

En ese sentido, el conocer el número de serie y la forma de cómo se asignan las dirección IP, no es una vulnerabilidad en sí, pero si algún hacker tuviera conocimiento del mismo, le serviría para indagar con el fabricante lo siguiente:

- *El lote de equipos al que pertenece los números de serie*
- *Con esto podría investigar que componentes tenían los equipos de dicho lote que fueron entregados como son: Modelo de Tarjeta Madre, Memoria RAM, Versión de BIOS, tarjeta de red, etc.*
- *Una vez con el conocimiento anterior, podría dedicarse a investigar que vulnerabilidades tiene el tipo de tarjeta madre, las vulnerabilidades del BIOS y lanzar un ataque en específico.*
- *Como una alegoría, en una chapa de seguridad, al conocer el número de serie podría investigar qué tipo de cilindro y componentes internos tiene el modelo para así allegarse de elementos específicos para lograr abrirla sin la llave.*

Esta Dirección General llega a la conclusión de que si bien es cierto existe el derecho de acceso a la información, también lo es que dicho derecho debe tener una utilidad pública y en el caso que nos ocupa no se detecta que dicha información lo sea, ya que lejos de beneficiar a la colectividad, se estaría poniendo en riesgo la información de miles de ciudadanos bajo resguardo de esta Secretaría, ya que la obtención de la información beneficiaría a una persona o pequeño grupo. Lo cual refuerza lo ya mencionado, en virtud de que la información que se aloja en los equipos es la que generan las unidades administrativas de la Cancillería, dentro de las cuales existen algunas que cuentan con el carácter de Instancias de Seguridad Nacional, de conformidad con las Bases de Colaboración que en el marco de la Ley de Seguridad Nacional. Por ende, la información que se genera también se encuentra catalogada como de Seguridad Nacional, actualizándose el artículo 110 fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública en relación con el artículo 51, fracción I de la Ley de Seguridad Nacional.

Adicionalmente y en el ámbito de máxima transparencia, la Secretaría consultó al proveedor, el cual es dueño de los equipos, si encontraba algún inconveniente de que se otorgara la información requerida, argumentando lo siguiente:

> *"PRIMERO.- De conformidad con la cláusula décima octava del contrato plurianual de prestación del servicio de arrendamiento de bienes muebles propalado con la Secretaría de Relaciones Exteriores, la cual establece que las partes se obligan a guardar la información que conozcan con motivo del desarrollo y cumplimiento del contrato, en virtud de que la información que se genere derivada del objeto del mismo está protegida por la Ley de Seguridad Nacional y se encuentra clasificada como reservada y/o confidencial en los términos de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP).*
>
> *SEGUNDO. - De acuerdo al artículo 99 de la LFTAIP, que establece que la información clasificada como reservada, de acuerdo al artículo 110 de dicha ley, podrá permanecer con tal carácter hasta par 5 años a partir de la fecha en que se clasifica como tal.*

TERCERO. - El artículo 110 de la LFTAIP contempla la información que se puede considerar como reservada, y en el artículo 113 de la misma ley se establece lo que se clasifica como información confidencial. En virtud de lo anterior, y toda vez que la información que se nos requiere contempla información sensible como: contraseñas de acceso, números de serie, versión del BIOS de los equipos, Sistema Operativo, entre otra, el divulgar la misma provocaría, entre otros, los siguientes riesgos:

1. Cualquier persona en posesión de la misma podría acceder a la información de los equipos (PCs) en uso en la Secretaría.
2. Al tener acceso a los equipos se podría buscar alguna vulnerabilidad de seguridad en la red de computadoras de la Secretaría y acceder a la información contenida en los sistemas de procesamiento y almacenamiento de información de la dependencia.
3. Lanzar ataques cibernéticos desde alguno o algunos de los equipos de la red de computadoras de la Secretaría.
4. Introducir algún tipo de malware a la red de computadoras de la Secretaría.
5. Infectar el portal web de la Secretaría.
6. Paralizar las actividades de la red de computadoras de la Secretaría.

Así las cosas, si esta H. Secretaría insistiera en requerir dicha información de acuerdo a su solicitud, sería requisito previo el modificar el contrato en el clausulado correspondiente, y bajo su propio riesgo, insistiendo en que se podría vulnerar el equipo y comprometer la información contenida en los equipos propiedad de mi representada.

Basamos la contestación al presente oficio, en términos del artículo 3 de la LFTAIP, el cuál a continuación nos permitimos transcribir, así como en los artículos de la misma ley referidos en el cuerpo del presente memorial:

[Se transcribe el artículo 3 de la Ley Federal de Transparencia y Acceso a la Información Pública]

En conclusión, tanto esta Secretaría considera NO viable proporcionar la información a que hace alusión el solicitante, en virtud de que proporcionarla pondría en riesgo la seguridad de la información contenida en los equipos, ya que los equipos que se encuentran instalados y conectados a la Red de la Secretaría, por lo que es considerado de que se transgrede la seguridad de los equipos instalados y se estaría en posibilidad de transgredir la totalidad de los equipos con los que cuenta la Secretaría, aunado a que se está considerado el hecho de que la persona, compañía, grupo o conjunto de personas con el conocimiento al respecto, podrían lanzar ataques cibernéticos desde alguno o algunos de los equipos de la red de computadoras, introducir algún tipo de malware a la red, infectar el portal web o incluso paralizar las actividades de la red de computadoras de la Secretaría, entre otras.

Asimismo, esta unidad administrativa señala que los servicios contratados a través de los proveedores de servicios de Telecomunicaciones y de Seguridad Informática a grandes

rasgos son servicios múltiples de telefonía, red multiservicios nacional, servicio integral de voz y datos y servicios de seguridad informática que incluyen la implementación, administración, operación, mantenimiento y suministro de servicios de seguridad informática, servicios de red voz y datos, telefonía, acceso a internet y enlaces WAN en los diferentes inmuebles que ocupa "LA SECRETARÍA", y no el arrendamiento de Módems o routers y de cortafuegos (firewalls), ya que dichos componentes son utilizados por los proveedores para poder proporcionar los servicios contratados, de ahí que esta Secretaría no cuente con la información solicitada referente a "ordenado por número de serie".

Para robustecer lo arriba citado; se informa que existen diversos tipos de intentos de hackeo:

- *Los que corresponden a Antivirus son realizados par malware que se intenta infiltrar en el SO de los equipos personales y servidores.*
- *Los de Filtrado Web son troyanos que están dentro del código de páginas web y que el usuario no lo detecta al querer abrir y navegar por estos sitios. Estos ataques son contenidos por nuestra herramienta de filtrado de contenido.*
- *Los más severos son los de IPS y que si son lanzados directamente par hackers hacia las direcciones IP de la SRE.*

Antivirus SRE Nacional	*Antivirus Exterior*	*Filtrado WEB*	*IPS Firewall Alameda*	*IPS Firewall Triangular*
amenazas y detectadas y bloqueadas	*amenazas y detectadas y bloqueadas2*	*amenazas y detectadas y mitigadas*	*ataques y detectados y bloqueados*	*ataques y detectados y bloqueados*
235	*26,618*	*91,500*	*99*	*2,556*

En ese sentido, el conocimiento o posesión de la información requerida podría permitir que cualquier tercero contara con los elementos suficientes para encontrar vulnerabilidades y acceder remotamente a los equipos y a su contenido.

Ahora bien, atendiendo a lo dispuesto en el artículo 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, a continuación, se establece la prueba de daño:

I. La divulgación de la información que se reserva representa un riesgo real, demostrable e identificable de perjuicio significativo a los intereses del gobierno mexicano. -La información reservada consistente en los números de serie, si se cuenta con contraseña para acceder a la configuración u administración y la forma en como se le asigna la IP, los cuales se consideran sensibles en virtud de que dan cuenta de los equipos y tecnología empleadas por

las Unidades Administrativas de esta Secretaría, resaltando que algunas de ellas realizan actividades en el marco de la Seguridad Nacional, derivado de su reconocimiento como Instancia de Seguridad Nacional. En virtud de lo anterior, las ubicaciones, tecnologías utilizadas y demás elementos de carácter técnico, representan información reservada, ya que dan cuenta de las características técnicas de la infraestructura contratada, la cual soporta los sistemas centrales que contienen bases de datos e información, lo que podría ser aprovechada por terceros con conocimientos técnicos para detectar puntas de vulnerabilidad en la infraestructura informática de la Secretaría de Relaciones Exteriores, conocer su capacidad de reacción en materia de seguridad informática, cuestión que potenciaría actos de sabotaje, monitoreo y/o control de los equipos de cómputo, siendo así susceptible a ser atacada o vulnerada afectando la integridad y disponibilidad de la información teniendo como posibles consecuencias la interrupción del desarrollo de las atribuciones conferidas a esta Secretaría, incluidas aquellas que albergan información confidencial y/o sensible al tratarse de infraestructuras críticas, la información generada por las unidades administrativas de la Secretaría que son instancias de seguridad nacional, así como los servicios a la ciudadanía como es la emisión de documentación oficial por parte de la dependencia.

II. El riesgo de perjuicio supera el interés público general de que se difunda. - La divulgación de las características de los dispositivos solicitados permitiría conocer los mecanismos que sigue esta Secretaría para los servicios de red, a través de los cuales puede viajar información sensible y dan conectividad a equipos de cómputo. Adicionalmente, se protege el poder contar con una red y servicios de conectividad, que den continuidad operativa y permitan mejorar los sistemas y aplicativos con los que la Secretaría cuenta para funcionar internamente. En este sentido, es importante recalcar que los servicios brindados se realizan dentro del marco de seguridad nacional, por lo que el omitir la normatividad bajo la cual se rige, se traduciría en transgredir los sistemas en ambientes de desarrollo, calidad y producción que son utilizados para realizar la operación sustantiva; asimismo, se vulneraría los servicios los cuales requieren un alto nivel de disponibilidad, además del servicio de equipamiento para proporcionar servicios a la red interna de datos, entre otros.

III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio. - La limitación del derecho del solicitante a conocer la información que se reservan es proporcional. El derecho a buscar y recibir información, si bien es un derecho fundamental, no es absoluto y puede ser limitado siempre y cuando: i) el fin sea constitucionalmente válido (fin legítimo); ii) la medida sea idónea para alcanzar el fin constitucionalmente válido; iii) no exista un medio menos lesivo; y, iv) la limitación sea proporcional en sentido estricto. (véanse tesis 1a. CCLXV/2016 (10a.), 1a. CCLXVIII/2016 (10a.), 1a. CCLXX/2016 (10a.) y 1a. CCLXXII/2016 (10a.) de noviembre de 2016, derivadas del Amparo en Revisión 237/2014 Josefina Ricaño Bandala y otros, 4 de noviembre de 2015)."

Para los incisos a) y b) de la solicitud que nos ocupa, respecto a los nombres de aquellas personas físicas que cuentan con las contraseñas administrativas o su equivalente y el tipo de contratación, empleo, cargo o comisión que desempeñan las personas que resulten del inciso anterior; se informa que los equipos son arrendados por esta Secretaría, de ahí que se desconozca el nombre, cargo y comisión de las personas a que hace alusión el solicitante, ya que no existe una relación laboral entre esta Secretaría y el personal que contrata los proveedores que brindan el servicio.

> *En este sentido, el proveedor no tiene la obligación, ni la Secretaría de contar con un listado de características o descripciones adicionales a las necesarias para dar cuenta del cumplimiento a los requerimientos previamente señalados, ni la de elaborar dicho documento, en términos del criterio intitulado* ***No existe obligación de elaborar documentos ad hoc para atender las solicitudes de acceso a la información****, que a la letra dispone:*
>
> *"...Los artículos 129 de la Ley General de Transparencia y Acceso a la Información Pública y 130, párrafo cuarto, de la Ley Federal de Transparencia y Acceso a la Información Pública, señalan que los sujetos obligados deberán otorgar acceso a los documentos que se encuentren en sus archivos o que estén obligados a documentar, de acuerdo con sus facultades, competencias o funciones, conforme a las características físicas de la información o del lugar donde se encuentre. Por lo anterior, los sujetos obligados deben garantizar a la información del particular, proporcionando la información con la que cuentan en el formato en que la misma obre en sus archivos; sin necesidad de elaborar documentos ad hoc para atender las solicitudes de información ....".*

Lo anterior, se refuerza tomando en cuenta que la información que se aloja en los sistemas de procesamiento y que viaja a través de los dispositivos, es la que de conformidad con sus atribuciones generan o pueden ser un media de acceso a las unidades administrativas de la Cancillería que tienen el carácter de Instancias de Seguridad Nacional de conformidad con las Bases de Colaboración que en el marco de la Ley de Seguridad Nacional celebran el Titular de la Secretaría de Gobernación, en su carácter de Secretario Ejecutivo del Consejo de Seguridad Nacional, y la Titular de la Secretaría de Relaciones Exteriores, publicadas en el DOF de fecha 27 de mayo de 2008.

Dado lo anterior, se actualiza la reserva de la información por un periodo de 5 años, de conformidad con lo previsto en el artículo 110, fracción I de la Ley Federal de Transparencia y Acceso a la Información pública.

Adicionalmente y en el ámbito de máxima transparencia, la Secretaría consultó al proveedor, el cual es dueño de los dispositivos, si encontraba algún inconveniente de que se otorgara la información requerida, argumentando lo siguiente:

"Consideramos que la información solicitada no debe de ser proporcionada ya que resulta un riesgo por lo sensible de la información para la Secretaría, el tener expuestos estos datos puede representar una posible amenaza. Considerando lo establecido en la Cláusula Décima del contrato acerca de la confidencialidad, el proveedor es responsable de salvaguardar la información que entregue o que produzca, para lo cual anexo un fragmento relevante del contrato "se compromete a tomar las medidas necesarias para salvaguardar la información confidencial y a evitar que tengan acceso personas ajenas al presente contrato sin consentimiento previo por escrito de "LA SECRETARÍA". Para brindar mayor claridad enlisto algunos riesgos de esta información:

- *Al tener versiones y modelos se podría buscar alguna vulnerabilidad de seguridad en la red de la Secretaría y acceder a la información contenida en los sistemas de procesamiento y almacenamiento de información de la dependencia.*
- *El acotar especificaciones de la seguridad establecida en la red Inalámbrica puede ser más susceptible a ser vulnerada.*
- *La entrega de información puede facilitar diversos ataques (Spoofing, Backdoor, Ataque DMA, Eavesdropping, phising, escalonamiento de privilegios, Trashing, DoS, etc.)*
- *Brinda factibilidad de una posible intrusión a la red y recursos de la Secretaría.*
- *Lanzar ataques desde el interior a otras dependencias comprometiendo el nombre de la Secretaría.*
- *Atacar los sitios Web de la Secretaría (DDoS, ataques de inyección, ataques de fuerza bruta, Cross-Site Scripting, etc.)*
- *Introducir algún tipo de malware, spyware, spam, o pharming, etc a la red de la Secretaría.*
- *Afectar algún servicio crítico a raíz de una intrusión*
- *Provocar alguna interrupción en a operaci6ón de la red de la Secretaría*
- *Se puede considerar el simple hecho de solicitar este tipo de información como un ataque de Ingeniería social*

En base a lo mencionado anteriormente nuestra recomendación es que la información no sea proporcionada."

En conclusión esta Secretaría considera NO viable proporcionar la información a que hace alusión el solicitante, en virtud de que proporcionarla pondría en riesgo la seguridad de la información que viaja por los dispositivos y/o contenida en los dispositivos conectados a estos, ya que está considerado el hecho de que la persona, compañía, grupo a conjunto de personas con el conocimiento al respecto, podrían lanzar ataques cibernéticos a alguno o algunos de los equipos de la red, introducir algún tipo de malware a la red, utilizar alguna vulnerabilidad, pudiendo afectar la integridad, disponibilidad y confidencialidad de la red, entre otras.

Lo anterior se robustece con las resoluciones recaídas a los Recursos de Revisión números 2448/18, 2537/18 y 2577/18, en los cuales el Pleno del Instituto solicitó opinión a su Dirección General de Tecnologías de Información, misma que refirió a grandes rasgos que, a través de un equipo de cómputo conectado a una red, es posible que se le permita a algún potencial atacante cibernético dirigir algún ataque informático, como lo es suplantación de identidad con usos maliciosos, interceptar, modificar o incluso retener datos que están en tránsito o un ataque de fuerza bruta el cual consiste en recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso al equipo. Por lo que de manera acertada, en las 3 resoluciones ya citadas, se determinó de manera correcta reservar la información, en virtud de que es posible que se pueda ejecutar un potencial ataque al ponerse en riesgo la seguridad de la información perteneciente a la Secretaría que viaja por medio de estos dispositivos y misma que se encuentra contenida en los equipos conectados a estos.

Por último, se informa que los equipos se encuentran físicamente instalados conforme al organigrama institucional en los siguientes inmuebles:

- *Edificio Tlatelolco*
- *Edificio Triangular*
- *Instituto Matías Romero*
- *Ex Convento*

...

Clasificación de la información solicitada: RESERVADA, los números de serie, parte de módems y routers, si se cuenta con contraseña para acceder a la configuración, administración y la forma en como se le asigna la IP, de conformidad con lo señalado por el solicitante.

Motivación para clasificación de la información: La divulgación de la información que se reservada cuenta de los equipos y tecnología empleados por las Unidades Administrativas de esta Secretaría en el desarrollo de las actividades que les han sido conferidas, resaltando aquellas que realizan actividades en el marco de la Seguridad Nacional, derivado de su reconocimiento como Instancia de Seguridad Nacional, por lo que pondría en riesgo la infraestructura contratada, la cual soporta los sistemas centrales que contienen bases de datos e información, obtenida y/o generada por esta Secretaría, pues el conocimiento de normas, procedimientos, métodos, fuentes, especificaciones técnicas, tecnología o equipo que sean útiles para la generación de inteligencia para la seguridad nacional, podría ser aprovechado por terceros con conocimientos técnicos para detectar puntos de vulnerabilidad en la citada infraestructura informática, conocer su capacidad de reacción en materia de seguridad informática, potenciando así los riesgos de actos de sabotaje, monitoreo y/o control de los equipos de cómputo, siendo así susceptible a ser atacada o vulnerada afectando la integridad y disponibilidad de la información, teniendo como posibles consecuencias la

interrupción del desarrollo de las atribuciones conferidas a esta Secretaría, incluidas aquellas que albergan información confidencial y/o sensible al tratarse de infraestructuras críticas, vulnerando la información generada por las unidades administrativas de la Secretaría que son instancias de seguridad nacional, así como los servicios prestados a la ciudadanía, tales como la emisión de documentación oficial por parte de la dependencia.

Fundamentación Jurídica de la clasificación de información RESERVADA: Artículos 6, fracción I, de la Constitución Política de los Estados Unidos Mexicanos; 110, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública; numerales Cuarto, Quinto, Séptimo, fracción I, Octavo, Décimo Séptimo, fracción IV, Trigésimo Tercero y Trigésimo Cuarto de los Lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, publicados en el Diario Oficial de la Federación el15 de abril de 2016.

Periodo de reserva: 5 años.

Prueba de daño: La señalada por la Unidad Administrativa consultada.

Fundamentación jurídica de la resolución: Analizadas todas y cada una de las constancias que integran el expediente en comento, con fundamento en los artículos 6° de la Constitución Política de los Estados Unidos Mexicanos; 28, de la Ley Orgánica de la Administración Pública Federal; 36 del Reglamento Interior de la Secretaría de Relaciones Exteriores; Acuerdo por el que se adscriben orgánicamente las unidades administrativas a que se refiere el Reglamento Interior de la Secretaría de Relaciones Exteriores, publicado en el Diario Oficial de la Federación el 4 de octubre de 2011 última reforma publicada en el Diario Oficial de la Federación el 04 de mayo de 2016; Acuerdo por el que se crea la Unidad de Transparencia y se establece el Comité de Transparencia de la Secretaría de Relaciones Exteriores publicado en el Diario Oficial de la Federación el 30 de agosto de 2016; 1, 2, 3, fracción V, y 13, de la Ley Federal de Procedimiento Administrativo; 61, fracciones II y V, 64, 65, fracción II, 97, 98, fracción I, 100, 102, 103, 110, fracción I, 111,134, 135, 140, fracción I y Tercero Transitorio de la Ley Federal de Transparencia y Acceso a la Información Pública; numerales Cuarto, Quinto, Séptimo, fracción I, Octavo, Décimo Séptimo, fracción IV, Trigésimo Tercero y Trigésimo Cuarto de los Lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, publicados en el Diario Oficial de la Federación el 15 de abril de 2016; artículo 24 de la Convención de Viena sobre Relaciones Diplomáticas, el Comité de Transparencia de la Secretaría de Relaciones Exteriores:

RESUELVE

PRIMERO. Que el Comité de Transparencia de la Secretaría de Relaciones Exteriores es competente para resolver respecto del presente asunto de conformidad con los artículos 102,

140, fracción I y tercero transitorio, de la Ley Federal de Transparencia y Acceso a la Información Pública.

SEGUNDO. Se confirma la clasificación de parte de la información que pudiera encontrarse en los archivos de la Unidad Administrativa consultada como **RESERVADA**, de conformidad con la respuesta emitida por la **DIRECCIÓN GENERAL DE TECNOLOGÍAS DE INFORMACIÓN E INNOVACIÓN**, respecto de la solicitud de acceso a la información identificada con el número de folio 0000500130518, por encontrarse apegada a derecho, atendiendo a los razonamientos expresados en la presente resolución.

TERCERO. Notifíquese la presente resolución al interesado para su conocimiento y efectos legales, hágase del conocimiento del solicitante que le asiste el derecho a interponer recurso de revisión ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales de conformidad con los artículos 61, fracción V y 147, de la Ley Federal de Transparencia y Acceso a la Información Pública, y 3°, fracción XV, de la Ley Federal de Procedimiento Administrativo.
..." (sic)

3. Interposición del recurso de revisión. El cinco de septiembre de dos mil dieciocho, se recibió en este Instituto, por medio de la Plataforma Nacional de Transparencia, el recurso de revisión interpuesto por la parte peticionaria en contra de la respuesta emitida por el sujeto obligado, en los términos siguientes:

Acto que se Recurre y Puntos Petitorios: "INFORMACIÓN DETALLADA EN ARCHIVO ANEXO." (sic)

Otros Elementos a Someter: "INFORMACIÓN DETALLADA EN ARCHIVO ANEXO." (sic)

Archivo Adjunto del Recurso de Revisión: 2018003396.pdf."

El archivo adjunto contiene escrito libre sin fecha, emitido en los términos siguientes:

"...
Por medio del presente escrito, señalando de entre el domicilio físico y la dirección de correo electrónico: [...] única y exclusivamente este último, como medio para recibir notificaciones; con fundamento en el artículo 6°, apartado A fracción IV constitucional, artículos 146, 147, 148, 149, 151 párrafo 2° y demás relativos de la Ley Federal de Transparencia y Acceso a la Información Pública, interpongo el recurso de revisión en contra de la clasificación de información y la declaración de inexistencia, efectuadas por la Secretaría

de Relaciones Exteriores (SRE) en respuesta a la solicitud de información número de folio 0000500130518.

I.- RAZONES Y MOTIVOS DE INCONFORMIDAD

AGRAVIO PRIMERO.- Violación a la garantía de máxima publicidad de la información.

ARTÍCULOS TRANSGREDIDOS: 6° DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, **4°, 11 Y 12** DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA, 3° DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA.

Inicialmente es oportuno señalar que por disposición del artículo 6° constitucional, el derecho fundamental de acceso a la información deberá interpretarse en función del principio de máxima publicidad. Asimismo, en atención a lo establecido en el artículo 1° constitucional y en la Ley reglamentaria del artículo 6° del mismo ordenamiento, en todo momento debe prevalecer la protección más amplia para la persona.

El principio de máxima publicidad enunciado en los artículos 11 y 12 de la Ley General de Transparencia y Acceso a la Información Pública (en lo subsecuente referida como Ley General), vincula a todo sujeto obligado a efecto de que permita el acceso y entregue todo tipo información generada, obtenida, adquirida, transformada o en su defecto se encuentre en su posesión; con exclusión de aquella que por disposición de Ley actualiza algún supuesto de excepcionalidad.

LEY GENERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 04-05-2015

[Se transcriben los artículos 11 y 12 de la Ley General de Transparencia y Acceso a la Información Pública]

Ahora bien, como se evidenciará a priori en las subsecuentes líneas, la clasificación de información efectuada por el sujeto obligado en atención a la solicitud 0000500130518 transgrede el principio de máxima publicidad de la información. Sin embargo, es de advertirse antes que en función de lo dispuesto en el artículo 20 de la Ley General, la carga de la prueba recae directamente sobre el sujeto obligado.

LEY GENERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 04-05-2015

[Se transcribe el artículo 20 de la Ley General de Transparencia y Acceso a la Información Pública]

Como se mencionó, el principio de máxima publicidad únicamente puede verse limitado por la actualización de algún supuesto previsto en el régimen de excepciones, es decir, ante la presencia de información clasificada como confidencial o reservada.

Los artículos 113 de la Ley General y 110 de la Ley Federal de Transparencia y Acceso a la Información Pública (en lo subsecuente Ley Federal) establecen que información será considerada como reservada.

LEY GENERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 04-05-2015

[Se transcribe el artículo 113 de la Ley General de Transparencia y Acceso a la Información Pública]

LEY FEDERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 09-05-2016

[Se transcribe el artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública]

Ahora bien, la información precisada en la solicitud 0000500130518 no actualiza algún supuesto previsto en los artículos antes transcritos, tal y como lo hace aparentar la clasificación efectuada por el sujeto obligado.

Lo anterior, toda vez que lo peticionado en la solicitud 0000500130518 se trata de información que de ninguna forma compromete la seguridad nacional, la seguridad pública o la defensa nacional; y menos aún vulnerar o alterar el normal desarrollo de las funciones desempeñadas por el sujeto obligado. Sino por el contrario, lo único que permite es corroborar si realmente el sujeto obligado emplea adecuadamente mecanismos o técnicas tendientes a robustecer su seguridad informática, y en última instancia la nacional y la pública. Además de permitir conocer qué personas administran los equipos informáticos que almacenan una cantidad considerable de información pública y privada de gran relevancia e importancia para la sociedad.

Es importante se tenga en consideración que lo peticionado en los incisos a) y b) son datos públicos por disposición de los artículos 68 de la Ley Federal y 70 fracción VII de la Ley General.

LEY FEDERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 09-05-2016

[Se transcribe el artículo 68 de la Ley Federal de Transparencia y Acceso a la Información Pública]

LEY GENERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 04-05-2015

[Se transcribe el artículo 70 fracción VII de la Ley General de Transparencia y Acceso a la Información Pública]

En cuanto al inciso d) y los números de serie, de igual forma son datos públicos por disposición de la fracción XXXIV del artículo antes citado; ya que este debe formar parte de los inventarios de los bienes muebles en posesión o propiedad el sujeto obligado.

LEY GENERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 04-05-2015

[Se transcribe el artículo 70 fracción XXXIV de la Ley General de Transparencia y Acceso a la Información Pública]

Por último, respecto del inciso c), también es información pública toda vez que por disposición de la fracción XLVIII del artículo antes citado, el sujeto obligado debe hacer publica cualquier información que sea de utilidad o se considere relevante.

LEY GENERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 04-05-2015

[Se transcribe el artículo 70 fracción XLVIII de la Ley General de Transparencia y Acceso a la Información Pública]

La información peticionada en el inciso c) de la solicitud 0000500130518 es suma relevancia y utilidad, puesto que esta permite conocer si emplean adecuadamente mecanismos o técnicas tendientes a robustecer la seguridad informática del sujeto obligado; lo cual a su vez da a conocer que tan protegida se encuentra la información que circula por la red del sujeto obligado.

Inclusive, si alguno de los datos requeridos en la solicitud 0000500130518 pusieran en riesgo la seguridad informática implementada por el sujeto obligado; el Servicio de Administración Tributaria (SAT), el Instituto Federal de Telecomunicaciones (IFT), la Auditoria Superior de la Federación (ASF), la Secretaria de Comunicaciones y Transportes (SCT), la Consejería Jurídica del Ejecutivo Federal, el Instituto Mexicano del Seguro Social (IMSS) y este Instituto (INAI); no hubiesen entregado datos equivalentes en respuesta a las solicitudes de información pública: 0610100124118, 0912100054218, 0110000049118, 0000900168418, 0220000006018, 0064101346818 y 0673800128118, respectivamente; mismas que con fundamento en el penúltimo párrafo del artículo 149 de la Ley Federal, someto a consideración de este Instituto.

En suma, la clasificación efectuada por el sujeto obligado resulta violatoria del principio de máxima publicidad, y en última instancia del derecho fundamental de acceso a la información

reconocido constitucional y convencionalmente en beneficio del hoy recurrente; ya que como se argumentó en líneas anteriores, lo requerido en la solicitud 0000500130518 no actualiza algún supuesto de reserva previsto en la Ley Federal o en la Ley General.

AGRAVIO SEGUNDO. - Falta de notificación de la Resolución del Comité de Transparencia, por la cual se clasificó la información requerida.

ARTÍCULOS TRANSGREDIDOS: 137, EN RELACIÓN CON EL **132** DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA, **140** EN RELACIÓN CON EL **135** DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA.

Por disposición del artículo 140 de la Ley Federal y 137 de la Ley General, los sujetos obligados deben seguir el siguiente procedimiento cuando consideren que los Documentos o la información requerida deban ser clasificados.

LEY FEDERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 09-05-2016

[Se transcribe el artículo 140 de la Ley Federal de Transparencia y Acceso a la Información Pública]

LEY GENERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 04-05-2015

[Se transcribe el artículo 137 de la Ley General de Transparencia y Acceso a la Información Pública]

Ahora bien, en contravención a los preceptos jurídicos antes citados, el sujeto obligado omite notificarme la resolución signada por los integrantes del Comité de Transparencia, a través de la cual se clasifico la información requerida en la solicitud 0000500130518.

AGRAVIO TERCERO. - Violación a las garantías de documentación de la acción gubernamental y presunción de existencia de la información.

ARTÍCULOS TRANSGREDIDOS: 18, 19 Y 20 DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA, **12 Y 13** DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA.

Para comenzar el presente agravio es necesario evocar que por disposición de los artículos 1° de la CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS y 7° de la Ley Reglamentaria del artículo 6° constitucional, en todo momento se debe favorecer la protección más amplia para la persona.

Bajo este principio constitucional, es menester que este Instituto valore como garantías del derecho fundamental de acceso a la información pública, a los principios de documentación de la acción gubernamental y presunción de existencia de la información.

Conforme a los artículos 18 y 19 de la Ley General de Transparencia y Acceso a la Información Pública (en lo subsecuente referida como Ley General), las garantías antes mencionadas consisten respectivamente, en que todo sujeto obligado deberá documentar todo acto que derive del ejercicio de sus facultades, competencias o funciones; y que se presume la existencia de la información si se refiere a las facultades, competencias y funciones que las normas otorgan a los sujetos obligados.

LEY GENERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 04-05-2015

[Se transcriben los artículos 18 y 19 de la Ley General de Transparencia y Acceso a la Información Pública]

En los mismos términos los artículos 12 y 13 de la Ley Federal de Transparencia y Acceso a la Información Pública (en lo subsecuente referida como Ley Federal) disponen el alcance jurídico de las garantías de documentación de la acción gubernamental y presunción de existencia de la información.

LEY FEDERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 09-05-2016

[Se transcriben los artículos 12 y 13 de la Ley Federal de Transparencia y Acceso a la Información Pública]

Ahora bien, en la solicitud 0000500130518 precisa información pública que debió haberse documentado por el sujeto obligado, en el ejercicio de las facultades, competencias o funciones, previstas en Ley Federal y la Ley General; ordenamientos de orden público y observancia general.

LEY GENERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 04-05-2015

[Se transcribe el artículo 1 de la Ley General de Transparencia y Acceso a la Información Pública]

LEY FEDERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 09-05-2016

[Se transcribe el artículo 1 de la Ley Federal de Transparencia y Acceso a la Información Pública]

Sin embargo, en la respuesta 0000500130518 el sujeto obligado declara sin formalidad alguna la inexistencia parcial de la misma.

Es oportuno hacer un paréntesis para indicar que ante esta declaración de inexistencia, conforme a lo dispuesto en el artículo 20 de la Ley General, la carga de la prueba recae directamente sobre el sujeto obligado, es decir, deberá demostrar que la información en cuestión no se refiere a alguna de sus facultades, competencias o funciones.

LEY GENERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 04-05-2015

[Se transcribe el artículo 20 de la Ley General de Transparencia y Acceso a la Información Pública]

Aunque no obstante la carga de la prueba recaiga sobre el sujeto obligado, a continuación se indicaran los preceptos específicos que hacen presumir la existencia de la información.

Como se hace alusión en el agravio primero del presente, al ser lo peticionado en los incisos a) y b) datos públicos, ello conlleva a que en atención a lo dispuesto en dichos artículos 68 de la Ley Federal y 70 fracción VII de la Ley General, aplicable en términos del ACUERDO ACTPUB/ 14/09/2016.05, el sujeto obligado previamente debió de haberlos documentado.

LEY FEDERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 09-05-2016

[Se transcribe el artículo 68 de la Ley Federal de Transparencia y Acceso a la Información Pública]

LEY GENERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 04-05-2015

[Se transcribe el artículo 70 fracción VII de la Ley General de Transparencia y Acceso a la Información Pública]

Es importante destacar que aunque si fuese cierto como indica el sujeto obligado en la respuesta 0000500130518, que los bienes muebles en cuestión derivan de un contrato de arrendamiento; ello no implica que el sujeto obligado no pueda manipular de acuerdo a sus necesidades y lo convenido con la contraparte, dichos equipos, debido a que como se indica en el artículo del Código Civil Federal el sujeto obligado al ser arrendatario tiene el uso y el goce temporal de los equipos.

CÓDIGO CIVIL FEDERAL

[Se transcribe el artículo 2398 del Código Civil Federal]

Luego entonces, al contar con dicho uso y goce temporal, deben existir determinadas personas (servidores públicos) que materialicen dichas potestades.

En resumen, al declarar inexistente la información requerida en la solicitud 0000500130518, el sujeto obligado transgrede las garantías de documentación de la acción gubernamental y presunción de existencia de la información, protectoras del derecho fundamental de acceso a la información reconocido constitucional y convencionalmente en favor de mi persona; puesto que la Ley Federal y la Ley General le atribuyen facultades, competencias y funciones que debieron ser forzosamente documentadas.

AGRAVIO SEGUNDO. - Falta de notificación de la Resolución del Comité de Transparencia, por la cual se confirma la inexistencia de la información requerida.

ARTÍCULOS TRANSGREDIDOS: 139, EN RELACIÓN CON EL 138 DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA, **143 EN RELACIÓN CON EL 141** DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA.

Por disposición del artículo 141 de la Ley Federal en relación con el numeral 138 de la Ley General, el Comité de Transparencia de los sujetos obligados debe seguir el siguiente el procedimiento cuando no se encuentre la información solicitada en sus archivos.

LEY FEDERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 09-05-2016

[Se transcribe el artículo 141 de la Ley Federal de Transparencia y Acceso a la Información Pública]

LEY GENERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 04-05-2015

[Se transcribe el artículo 138 de la Ley General de Transparencia y Acceso a la Información Pública]

La resolución del Comité de Transparencia a que se hace referencia en los artículos antes transcritos, es decir, aquella a través de la cual se confirme la inexistencia de la información requerida, debe ser notificada al solicitante. Esto debido a que es la única forma por la cual dicha persona puede cerciorarse de que el sujeto obligado utilizo un criterio de búsqueda exhaustivo, además de permitirle conocer las circunstancias de tiempo, modo y lugar que generaron la declaratoria de inexistencia, y por último ser sabedor del servidor público responsable de contar con dicha información.

LEY GENERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 04-05-2015

[Se transcribe el artículo 139 de la Ley General de Transparencia y Acceso a la Información Pública]

LEY FEDERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 09-05-2016

[Se transcribe el artículo 143 de la Ley Federal de Transparencia y Acceso a la Información Pública]

Ahora bien, en contravención a los preceptos jurídicos citados en el presente agravio, el sujeto obligado omite notificarme la resolución signada por cada uno de los integrantes del Comité de Transparencia a través de la cual se confirmó la inexistencia de lo peticionado en la solicitud 0000500130518.

Generando con esta omisión, que no se me permite tener la certeza respecto de si el sujeto obligado utilizo un criterio de búsqueda exhaustivo, además de impedirme saber las circunstancias de tiempo, modo y lugar que generaron la declaratoria de inexistencia, así como también no permitirme conocer al servidor público responsable de contar con la información que requiero.

PRUEBAS

A. Con fundamento en el artículo 20 de la Ley General, de aplicación supletoria a la Ley Federal, atentamente solicito se aplique la reversión de la carga de la prueba al sujeto obligado, es decir, se le requiera para que pruebe la reserva de la información precisada en la solicitud de información pública número 0000500130518.

LEY FEDERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 09-05- 2016

[Se transcribe el artículo 7 de la Ley Federal de Transparencia y Acceso a la Información Pública]

LEY GENERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 04-05-2015

[Se transcribe el artículo 20 de la Ley General de Transparencia y Acceso a la Información Pública]

B. La instrumental de actuaciones y la presuncional en su doble aspecto, en todo lo que me favorezca.

PUNTOS PETITORIOS

Por lo antes expuesto y fundado atentamente solicito:

I. Tenerme por interpuesto en tiempo y forma el presente recurso.
II. Tenerme por señalado como único y exclusivo medio para recibir notificaciones el correo electrónico indicado.
III. Aplicar la suplencia de la queja al presente recurso.
IV. Revocar o en su caso modificar la respuesta del sujeto obligado, con la finalidad de que se me entregue la información pública solicitada, conforme a los términos y criterios precisados originalmente; y en el supuesto de no poderse entregar bajo la modalidad de entrega elegida, manifiesto conformidad para que se realice vía correo electrónico señalado en la presente." (sic)

4. Turno del recurso de revisión. El cinco de septiembre de dos mil dieciocho, el Comisionado Presidente de este Instituto asignó el número de expediente **RRA 6073/18** al recurso de revisión y, con base en el sistema aprobado por el Pleno de este Instituto, lo turnó al Comisionado Ponente, para los efectos del artículo 156, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública.

5. Admisión del recurso de revisión. El diez de septiembre de dos mil dieciocho, se dictó acuerdo por medio del cual se admitió a trámite el recurso de revisión.

6. Notificación de la admisión a la parte recurrente: El once de septiembre de dos mil dieciocho, mediante correo electrónico, se notificó a la parte solicitante la admisión del recurso.
7. Notificación de la admisión al sujeto obligado: El once de septiembre de dos mil dieciocho, se notificó al sujeto obligado, a través de la Plataforma Nacional de Transparencia, la admisión del recurso de revisión.

8. Alegatos del sujeto obligado. El veinte de septiembre de dos mil dieciocho, se recibió, a través de la Plataforma Nacional de Transparencia de este Instituto, el oficio número CTA-26318, sin fecha, suscrito por el Comité de Transparencia de la Secretaría de Relaciones Exteriores, y dirigido al Comisionado Ponente, a través del cual manifestó los siguientes:

"...

ALEGATOS

I. Respecto al tratamiento a las solicitudes de acceso a la información, cabe recordar que se tienen cuatro supuestos, atendiendo a la naturaleza de lo que requerido por el particular, mismos que pueden actualizarse de manera simultánea:

1.- Se hace entrega de la información por ser de carácter público;
2.- Se declara la inexistencia de la información derivado de que ciertas facultades, competencias p funciones no se hayan ejercido;
3.- Se hace del conocimiento del solicitante que el sujeto obligado al cual requirió información, no es el competente para conocer y/o generar la misma, de conformidad con las atribuciones que le han sido conferidas por la ley, por lo que se procede a orientarlo para que dirija su solicitud al sujeto obligado que podría conocer de la información (incompetencia); y
4.- Se clasifica la información por actualizarse los supuestos de Reserva y/o Confidencialidad contenidos en la ley de la materia, negándose así su entrega o bien, poniendo a disposición del solicitante versión pública de lo requerido; según corresponda.

En ese sentido, se procedió a hacer del conocimiento del entonces solicitante, que la naturaleza de la información requerida actualizaba el supuesto de reserva contemplados en el articulo 110, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP) y en el numeral Décimo Séptimo, fracción IV de los lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas (Lineamientos).

Ahora bien, el recurrente en su escrito de inconformidad manifiesta una supuesta violación al principio de máxima publicidad; arguyendo que la información requerida es de carácter público por el simple hecho de encontrarse en posesión de este sujeto obligado.

Dichas consideraciones resultan equívocas, ya que el derecho de acceso a la información no es absoluto y se encuentra supeditado al interés público y a la seguridad nacional, siendo obligación de esta Secretaría su resguardo y clasificación temporal como reservada, en caso de actualizarse estos últimos, atendiendo en todo momento a las formalidades establecidas en la LFTAIP.

II. En consideración a las particularidades que rodean al presente caso, más allá de lo que puede deducirse de la información requerida por sí sola, resulta pertinente señalar a ese Instituto, la necesidad de emprender un análisis muy apartado de cualquier estimación genérica y, que a su vez, contemple las circunstancias de hecho presentes en el Recurso de Revisión de mérito.

En ese sentido, resulta prudente retomar el criterio emitido por la Suprema Corte de Justicia de la Nación en Sesión Pública Ordinaria de su Pleno, de fecha lunes 05 de diciembre de 2016, en la cual se resolvió el Recurso de Revisión en materia de seguridad nacional previsto en la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) 1/2016, promovido por el Consejero Jurídico del Ejecutivo Federal en contra de la resolución dictada en el expediente del recurso de revisión RDA-2149/16, emitida por el Pleno del INAI (Anexo I).

En la página 16 de dicho documento, se destaca lo expresado por el Ministro Zaldívar Lelo de Larrea, puntualizando que en temas de Seguridad Nacional, no es factible realizar un análisis aislado de los elementos integrantes del tema en cuestión, sino que se debe adoptar una perspectiva bajo las premisas de la llamada "Teoría del mosaico", la cual estima que determinada información aparentemente inocua, unida a otra clase de información podría representar un componente significativo para comprometer la Seguridad Nacional.

Ahora bien, dicha tesitura ha sido también adoptada por el Pleno del INAI en la resolución que emitió el Recurso de Revisión RRA-7151/17 (*Anexo II*), estimando que el análisis respecto a información relacionada con Seguridad Nacional, debe realizarse de manera casuística, considerando además de los elementos componentes de la misma, el contexto que lo rodea, permitiendo así una visión integral. Lo anterior da pauta a la identificación de los posibles resultados que se obtendrían al relacionar la información en pugna, con otros elementos.

Dicho cuanto, se presentan para consideración de ese Instituto, los siguientes puntos:

a) Además de la solicitud de acceso a la información pública origen de este procedimiento, fueron presentadas diversas, la primera ante la Agencia Mexicana de Cooperación Internacional para el Desarrollo, órgano desconcentrado dependiente de esta Secretaría de Relaciones Exteriores, la cual fue tramitada bajo el número de folio 0510000001918, y recurrida ante ese Instituto, correspondiéndole el número de expediente RRA-2577/18:

"Con fundamento en el artículo 6 constitucional, atentamente requiero que en función de los principios constitucionales de máxima publicidad, transparencia, rendición de cuentas y gratuidad, me entregue a través de un medio gratuito derivado de los avances tecnológicos y en formato de documento portátil (PDF) comprimido o en diverso de naturaleza similar, la siguiente información pública documentada en el ejercicio de las facultades, competencias y funciones previstas en las normas jurídicas aplicables. 1. De cada uno de los equipos de cómputo en posesión del sujeto obligado: a. Numero de serie y de parte. b. Versión de la BIOS (siglas en Ingles de Basic Input/Output System). c. Marca. d. Si se cuenta con contraseña para acceder a la configuración de la BIOS (siglas en inglés de Basic Input/Output

System). e. Procesador. f. Capacidad de almacenamiento. g. Conforme al organigrama estructural, unidad, área u órgano que hace uso del equipo de cómputo."

La segunda, presentada ante la Secretaría de Relaciones Exteriores, con número de folio 0000500059218, también recurrida, cuyo Recurso de Revisión se tramitó bajo el expediente RRA-2537/18:

"Con fundamento en el artículo 6 constitucional, atentamente requiero que en función de los principios constitucionales de máxima publicidad, transparencia, rendición de cuentas y gratuidad, me entregue a través de un medio gratuito derivado de los avances tecnológicos y en formato de documento portátil (PDF) comprimido o en diverso de naturaleza similar, la siguiente información pública documentada en el ejercicio de las facultades, competencias y funciones previstas en las normas jurídicas aplicables desglosado por número de serie o número de parte de cada uno de los equipos de cómputo en posesión del sujeto obligado, nombre de los navegadores de Internet que se encuentran instalados en dichos equipos de cómputo. 2. Motivos por los cuales son utilizados únicamente los navegadores de Internet a los que se haga referencia en relación al punto anterior. 3.Número de serie o número de parte de cada equipo de cómputo en posesión del sujeto obligado que tenga instalado el navegador de Internet denominado YANDEX BROWSER. 4. NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DE TODOS LOS "PROVEEDORES DE SERVICIOS DE TELECOMUNICACIONES. ESPECIFICANDO AQUELLOS QUE PROVEAN ACCESO A INTERNET. 5. SERVIDORES DNS (Domain Name System) UTILIZADOS PARA EL ACCESO A INTERNET. 6. Cuáles son las redes sociales oficiales utilizadas como medios de comunicación. 7. Motivos por los cuales son utilizados únicamente las redes sociales a las que se haga referencia en el punto anterior. 8. Cuenta oficial en la red social de VK (Vkontakte). 9. Por número de serie o número de parte de cada uno de los equipos de cómputo en posesión del sujeto obligado, la dirección MAC (por sus siglas en ingles Media Access Control) de cada tarjeta o adaptador de red (WIFI, BLUETOOTH, ETHERNET) de la que disponga cada equipo de cómputo."

Una tercera, también presentada ante la Secretaría de Relaciones Exteriores, con número de folio 0000500043718, también recurrida, cuyo Recurso de Revisión se tramitó bajo el expediente RRA-2448/18:

"Con fundamento en el artículo 6 constitucional, atentamente requiero que en función de los principios constitucionales de máxima publicidad, transparencia, rendición de cuentas y gratuidad, me entregue a través de un medio gratuito derivado de los avances tecnológicos y en formato de documento portátil (PDF) comprimido o en diverso de naturaleza similar, la siguiente información pública documentada en el ejercicio de las facultades, competencias y funciones previstas en las normas jurídicas aplicables. 1. De cada uno de los equipos utilizados en el Secretaría: a. Número de serie y de parte. b. Versión de la BIOS (siglas en ingles de Basic Input/Output System). c. Marca. d. Si se cuenta con contraseña para acceder a la configuración de la BIOS (siglas en inglés de Basic Input/Output System). e. Procesador.

F. Capacidad de almacenamiento en el Disco Duro. g. Conforme al organigrama estructural, unidad administrativa que hace uso del equipo de cómputo."

Una cuarta, también presentada ante la Secretaría de Relaciones Exteriores, con número de folio 0000500062518, también recurrida, cuyo Recurso de Revisión se tramitó bajo el expediente RRA-3661/18:

Con fundamento en el artículo 6 constitucional, atentamente requiero que en función de los principios constitucionales de máxima publicidad, transparencia, rendición de cuentas y gratuidad, me entregue a través de un medio gratuito derivado de los avances tecnológicos y en formato de documento portátil (PDF) comprimido o en diverso de naturaleza similar, la siguiente información pública documentada en el ejercicio de las facultades, competencias y funciones previstas en las normas jurídicas aplicables 1. De cada uno de los MODEMS, ROUTERS (rúters) o Puntos de acceso inalámbricos en posesión del sujeto obligado: a. Número de serie, de parte y de modelo. b. Marca. c· Si se cuenta con contraseña para acceder a la configuración u administración del MÓDEM, ROUTER (rúter) o punto de acceso inalámbrico. d. Si se encuentra activada la tecnología WPS (por sus siglas en Ingles Wi-Fi Protected Setup). e. Si se encuentra activada la tecnología WIFI. f. Seguridad o cifrado implementado en la conexión WIFI (WEP-Wired Equivalence Privacy, WPA – Wi-Fi Protected Access, WPA2 -Wi,-Fi Protected Access 2, etc). g. Conforme al organigrama estructural, unidades, áreas u órganos que hacen uso del MODEM, ROUTER (rúter) o punto de acceso inalámbrico."

En todos los medios de impugnación citados, el Pleno del INAI estimó que la naturaleza de la información requerida, actualizaba la causal de Reserva señalada en el artículo 110, fracción I de la LFTAIP, en virtud de que esta revelaría normas, procedimientos, métodos, fuentes, especificaciones técnicas, tecnología o equipo que sean útiles para la generación de inteligencia para la seguridad nacional, de conformidad con las atribuciones que ejercen algunas de las Unidades Administrativas de la Secretaría de Relaciones Exteriores en el marco de su reconocimiento como Instancia de Seguridad Nacional.

b) Con fecha 11 de abril, fue recibida la solicitud de acceso a la información número 0000500061418, a través de la cual se requirió:

"Se pide lo siguiente respecto al sistema de nómina que actualmente usa:
1.Nombre (del sistema).
2.Si es desarrollo propio o de un tercero.
2a. En caso de ser desarrollo de un tercero, el nombre del proveedor y de su representante legal, así como un número telefónico del proveedor.
3. Los costos anuales de la licencia de uso y de la de mantenimiento y/o soporte técnico. Cada uno por separado.

4. La cantidad de trabajadores de la institución.
5. El nombre del sistema operativo con el que opera.
6. Los nombres de los informes y/o reportes que genera.
7. Cantidad de usuarios del sistema.
8. Nombres de los responsables del sistema (dentro de la institución).
9. La fecha desde cuándo se usa ese sistema.
10. Indicar los nombres de otros sistemas con los que se interrelaciona (si fuese el caso).
11. Una breve y clara descripción de cómo opera el sistema (considérese cuales son las entradas y salidas del sistema).
12. Los tipos de problemas más comunes (3 de estos)."

Dado que el desarrollo del sistema es propio y su operación no se encuentra interrelacionado con otros sistemas, se consideró factible proporcionar algunos de los elementos requeridos por el particular, sin embargo, se procedió a notificarle la declaratoria de Reserva de la información por un periodo de 5 años, por 10 que hace al punto 8, por actualizarse la causal contenida en artículo 110, fracción V de la LFTAIP.

Cabe señalar que para determinar la clasificación de la información, se tomaron en consideración elementos del contexto actual, **específicamente los ataques informáticos perpetrados en contra de la Secretaría de Cultura de la Ciudad de México el pasado 14 de noviembre de 2017, mismos que causaron un daño al erario público cercano a los cinco millones de pesos.**

c) Como bien lo expresó el recurrente, este ha ingresado solicitudes de acceso a la información muy similares, inclusive sustancialmente idénticas ante diversos sujetos obligados.

Por lo que hace a solicitudes de acceso a la información atendidas por otros sujetos obligados, se aclara que de conformidad con lo establecido en la LFTAIP, esta Secretaría tiene la obligación de llevar a cabo un análisis de la naturaleza de la información requerida, atendiendo a las particularidades caso por caso, por lo que no hay cabida a una sustanciación generalizada a todas las solicitudes que recibe, máxime a las atendidas por otros sujetos obligados extraños a esta Secretaría de Relaciones Exteriores, los cuales son jurídica, financiera y operativamente ajenos, de conformidad con la Ley Orgánica de la Administración Pública Federal.

[Se transcriben los artículos 98 fracción I, 102 primer y segundo párrafo, y 105 de la Ley Federal de Transparencia y Acceso a la Información Pública]

Con independencia de lo anterior, se procedió a consultar en la Plataforma Nacional de Transparencia (PNT) la respuesta que otorgaron los sujetos obligados a las solicitudes listadas por el recurrente, de entre las cuales destaca la emitida por el Comité de

Transparencia del INAI, en la cual se procedió a declarar la clasificación de la información como Reservada por un periodo de 5 años, por actualizarse las causales contempladas en los artículos 113, fracción VII de la LGTAIP y 110, fracción VII de la LFTAIP, bajo la premisa de potenciación de un riesgo de hackeo a sus equipos de cómputo, lo que permitiría la comisión de delitos relacionados con la suplantación de identidad, así como con el acceso ilícito a sistemas, equipos e información propiedad del estado mexicano (*Anexo III*).

Más allá del trámite y la respuesta otorgada a cada una de las solicitudes en cita, resulta pertinente tomar en consideración que la información requerida no muestra objetivamente utilidad alguna para la consecución de las finalidades en el marco de la rendición de cuentas por parte de una institución pública, sino que desde el punto de vista técnico implica posibles usos muy específicos, encaminados a la intervención, sabotaje, intrusión, a la toma de control de equipos vía remota, así como a la libre disposición (alteración, difusión y/o eliminación) de la información generada y resguardada por la Cancillería en cumplimiento a las atribuciones que le han sido conferidas a sus Unidades Administrativas, enfatizando aquellas llevadas a cabo en su calidad de Instancias de Seguridad Nacional.

d) En años recientes, se ha presentado un incremento en los ataques informáticos, tanto a instituciones del sector privado, como a las de carácter público, lo cual es un tema relevante para las autoridades estatales, y de fácil consulta para cualquier persona, tal como se puede apreciar a continuación:

El Centro Criptológico Nacional (CCN) del Estado español, es el Organismo responsable de coordinar las acciones de las diferentes entidades de la Administración Pública que utilizan medios o procedimientos de cifra, de garantizar la seguridad de las Tecnologías de la Información y de formar al personal especialista en este campo.

Dicho organismo se encuentra adscrito al Centro Nacional de Inteligencia (CNI), siendo este último el encargado del ejercicio de las funciones relativas a la seguridad de las Tecnologías de la Información y de protección de la información clasificada del gobierno español.

El CCN mediante un comunicado publicado el pasado 07 de abril de 2016 pronosticó un alza de 40% en los ciberataques a la Administración y a empresas de interés estratégico; con base en los ciberincidentes que ha gestionado, el cual puede ser empleado como referencia para contextualizar el riesgo que supone la divulgación de la información de la solicitud de mérito.

"...

- *Así lo recoge el Informe CCN-CERT IA-09/16 de Ciberamenazas 2015/Tendencias 2016 que hace balance de los principales ciberincidentes registrados el pasada año (18.232), las herramientas empleadas y las vulnerabilidades encontradas.*

- *El informe aborda las principales tendencias para este 2016 y tres grandes anexos que completan una visión general del panorama de la ciberseguridad: actividad más destacada del CCN; Dispositivas y Comunicaciones Móviles y Hacktivismo en 2015.*

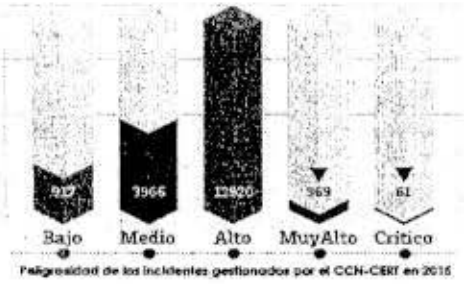
- *Los ataques al hardware y las dificultades de su detección principal tendencia de este año según el CCN-CERT*

Al igual que en años anteriores, 2015 vio incrementar el número, tipología y de los ataques contra los sistemas de información de las Administraciones Públicas y Gobiernos, de las empresas e instituciones de interés estratégico o aquellas poseedoras de importantes activos de propiedad intelectual e industrial y, en general, contra todo tipo de entidades y ciudadanos.

Así lo ha constatado, un año más, el Centro Criptológico Nacional al elaborar su ya tradicional informe de Ciberamenazas y Tendencias (CCN-CERT-IA-09/16) en el que señala que fueron 18.232 los ciberincidentes gestionados par su Capacidad de Respuesta (CERT), un 41% más que en 2014, de los cuales 430 tuvieron una peligrosidad de "muy alta" o "Crítica".

El documento examina el impacto, en España y fuera de sus fronteras, de las amenazas y los ciberincidentes más significativos ocurridos en 2015: ciberespionaje (por estados y empresas), ciberdelincuencia, hacktivismo y, como singularidad, el que hemos denominado ciberyihadismo (acciones atribuibles a grupos de tendencia violenta y radical dentro del islam político), los actores internos a los ciberinvestigadores.

El documento aborda además las herramientas empleadas por los atacantes (con especial relevancia de los exploits, exploit-kits y código dañino) y la resiliencia (la forma en que los sistemas de información han sabido afrontar los ciberataques y sus vulnerabilidades y las medidas adoptadas para fortalecerlos).



Tendencias 2016.

Para este 2016, el CCN-CERT pronostica un incremento en la capacidad de los atacantes para sortear los sistemas de seguridad y evitar ser detectados al tiempo que experimentarán con infecciones que no requieren del uso de un archivo. De este modo; se aprovecharán de las vulnerabilidades del hardware o del firmware (como la BIOS), al tiempo que se eludirán las defensas inyectando comandos en la memoria o manipulando funciones para introducir una infección o filtrar datos.

Ahora bien, la situación actual se encuentra signada por una serie de ataques de esa clase, a escala global involucrando a instituciones de más de 50 países, llegando al punto en el que la Oficina Federal de Investigación de EE.UU. (FBI por sus siglas en inglés) ha emitido una alerta del hackeo mundial a cientos de miles de rúters:

- Diario "El financiero" (México):

"El FBI, alertó que piratas informáticos rusos comprometieron cientos de miles de routers domésticos y de oficinas y podrían recopilar información de usuarios o dar de baja el tráfico de la red.

La agencia estadounidense pidió a los dueños de varias marcas de enrutadores los apaguen y vuelvan a encender y que descarguen actualizaciones de los fabricantes para protegerse.

La advertencia tuvo lugar después de una orden emitida la semana pasada por una corte que autorizó al FBI a intervenir un sitio web que los hackers planeaban para utilizar instrucciones a los routers. A pesar de esto, los routers aún seguían infectados y la advertencia tenía el objetivo de limpiar esas máquinas.

Las infecciones fueron detectadas en más de 50 países, aunque el objetivo principal para futuras acciones era probablemente Ucrania, sino de muchas infecciones recientes y campo de batalla de la guerra cibernética desde hace tiempo.

Al obtener la orden Judicial, el Departamento de Justicia dijo que los piratas informáticos involucrados estaban en un grupo llamado Sofacy que respondía al Gobierno ruso.

Sofacy, también conocido como APT28 y 'Fancy Bear', ha sido culpado de muchos de los hackeos rusos más dramáticos, incluido el del Comité Nacional Demócrata durante la campaña presidencial de 2016 en Estados Unidos.

Cisco Systems dijo que el ataque informático tenía como objetivo dispositivos de Linksys de Belkin International, MikroTik, Netgear, TP-Link y QNAP.

Cisco compartió los detalles técnicos de su investigación con los gobiernos de Estados Unidos y Ucrania. Expertos occidentales dicen que Rusia ha realizado una serie de ataques contra compañías en Ucrania durante más de un año, en medio de hostilidades armadas entre los dos países, provocando cientos de millones de dólares en daños y al menos un apagón energético".

- Periódico "El País" (España):

"Una alerta sin precedentes y con un alcance que puede considerarse masivo: el FBI ha detectado un ataque de hackers proveniente de Rusia mediante el cual se introduciría un malware que se apropiaría del router doméstico. Las autoridades estadounidenses han identificado este malware como VPNFilter, que tomaría el control de nuestro router para propagar ataques mundiales coordinados, y por descontado, registrar toda la actividad en la red de los dispositivos conectados. La gravedad de este ataque es tal, que los hackers podrían anular por completo la conexión a internet en zonas enteras y lo que resulta más preocupante, llevar a cabo ataques masivos a objetivos determinados.

Todavía no se conoce el alcance de este ataque, pero se estima que estarían afectados más de medio millón de routers domésticos en todo el planeta, y dada la configuración en red de este tipo de ataques, es de suponer que ese número se dispare exponencialmente por minutos. El funcionamiento es el siguiente: un router afectado por VPNFilter se queda en modo aletargado a la espera de recibir instrucciones de cara a llevar a cabo un ataque coordinado contra un objetivo determinado por los hackers. Entre tanto, registraría toda la información proveniente de nuestra actividad en la red (sí, contraseñas también), y los investigadores que han identificado el hack han comprobado la existencia de un 'botón letal' mediante el cual los atacantes podrían inutilizar definitivamente el dispositivo.

En una acción coordinada a gran escala, VPNFilter podría inutilizar la conexión a internet en barrios o ciudades enteras, dada la gran cantidad de marcas afectadas. El FBI ha enumerado en un listado los equipos afectados, pero ha avanzado que ello no quiere decir que aquellos que no aparezcan en la lista no estén afectados o sean susceptibles de ello. En este listado

encontramos fabricantes como Netgear, TP-Link o Linksys, aunque como apuntamos, los fabricantes afectados podrían ser muchos más. ¿Qué hacer en cualquier caso? Las autoridades recomiendan llevar a cabo algo muy simple: reiniciar el router (desenchufar y volverlo a enchufar); con este paso se inutilizaría el malware en la mayoría de los casos, aunque tampoco hay garantías de ello.

Los expertos de Cisco, la firma que habría detectado en primera instancia el ataque, van más allá en sus recomendaciones: restablecer el dispositivo a la configuración de fábrica para asegurarse de que no queda rastro del malware. Esta medida es más definitiva, pero es poco recomendable para todos aquellos que no cuenten con un elevado conocimiento en este tipo de equipos, ya que nos obligará después de volver a configurar el router internamente (la gran mayoría de los routers los entrega el proveedor de internet y vienen configurados de fábrica). Una medida adicional y que siempre resulta recomendable: cambiar la contraseña del panel de control que da acceso al router. Los expertos recomiendan, asimismo, asegurarse de que el router lleva ya la última versión del firmware (cabe esperar que los fabricantes se han puesto manos a la obra para atajar el problema).

Expertos consultados por EL PAÍS califican la recomendación de reiniciar el router como "desesperada" pero la medida no soluciona el problema de fondo: "reiniciar un router puede hacer que se vuelva a un estado previo al de su infección, pero no lo protege contra una nueva", explica Fernando Suárez, vicepresidente del Consejo General de Colegios de Ingeniería Informática. El router es siempre un dispositivo "más vulnerable", según este experto, ya que suele comercializarse con la configuración de fábrica "y en entornos pequeños no están protegidos con herramientas como antivirus".

- Periódico "The New York Times" (Estados Unidos de América):

"Con la esperanza de frustrar un sofisticado Sistema de malware vinculado a Rusia que ha infectado cientos de miles de enrutadores de Internet, el FBI ha hecho una solicitud urgente a cualquiera con uno de los dispositivos: apáguelo y vuelva a encenderlo.

El malware es capaz de bloquear el tráfico web, recolectar información que pasa a través de los enrutadores domésticos y de oficina, y deshabilitar por completo los dispositivos, anunció la oficina el viernes.

Una red global de cientos de miles de enrutadores ya está bajo el control del Grupo Sofacy, dijo el Departamento de Justicia la semana pasada. Ese grupo, que también es conocido como APT 28 y Fancy Bear y se cree que es dirigido por la agencia de inteligencia militar de Rusia, hackeó el Comité Nacional Demócrata antes de las elecciones presidenciales de 2016, según agencias de inteligencia estadounidenses y europeas.

El FBI tiene varias recomendaciones para cualquier propietario de una pequeña oficina o enrutador de oficina doméstica. Lo más simple es reiniciar el dispositivo, que interrumpirá temporalmente el malware si está presente. También se recomienda a los usuarios actualizar el firmware del dispositivo y seleccionar una nueva contraseña segura. Si hay alguna configuración de administración remota en funcionamiento, el FBI sugiere desactivarla.

Un análisis de Talos, la división de inteligencia de amenazas para el gigante tecnológico Cisco, calculó que al menos 500,000 enrutadores en al menos 54 países habían sido infectados por el malware, que el FBI y los investigadores de ciberseguridad llaman VPNFilter. Entre los equipos de red afectados se encontró durante su investigación dispositivos de fabricantes como Linksys, MikroTik, Netgear y TP-Link.

Para desbaratar la red Sofacy, el Departamento de Justicia buscó y recibió permiso para apoderarse del dominio web toknowall.com, que según dijo era una parte fundamental de la "infraestructura de comando y control" del malware. Ahora que el dominio está bajo el control del FBI, cualquier intento del malware de reinfectar un enrutador comprometido se devolverá a un servidor del FBI que puede registrar la dirección IP del dispositivo afectado.

'Esta incautación ordenada por la corte ayudará a identificar los dispositivos de la víctima e interrumpirá la capacidad de estos piratas informáticos de robar información personal y otra información delicada y llevar a cabo ataques cibernéticos disruptivos', Scott W. Brady, abogado de los Estados Unidos para el Distrito Oeste de Pensilvania, dijo en la declaración del Departamento de Justicia.
El análisis de Talos señala importantes similitudes entre el código de computadora de VPNFilter y 'versiones del malware BlackEnergy, que fue responsable de múltiples ataques a gran escala contra dispositivos en Ucrania'.

En la evaluación de Talos, las amenazas planteadas por VPNFilter van más allá de los problemas personales creados por las contraseñas robadas: bajo las circunstancias correctas, un ataque podría tener un alcance global."

Dicho cuanto, se informa a ese Instituto que tanto la solicitud de acceso a la información de mérito, como las citadas en el inciso "a)", fueron ingresadas mediante el uso de cuentas de correo electrónico originarias de Rusia.

e) De igual forma, se reitera que esta Secretaría ha sido blanco de múltiples intentos de hackeo, tanto de manera directa, como a través de correos electrónicos con direcciones web o archivos electrónicos maliciosos, mismos que a la fecha de respuesta a la solicitud por parte de la Dirección General de Tecnologías de Información e Innovación, se reportaron las siguientes amenazas detectadas y bloqueadas:

- **26,618** Correspondientes a Antivirus Exterior, así como **235** Antivirus SER Nacional, que son realizados por malware que se intenta infiltrar en el SO de los equipos personales y servidores;

- **91,500** de Filtrado Web, que son troyanos que están dentro del código de páginas web y que el usuario no lo detecta al querer abrir y navegar por estos sitios. Estos ataques son contenidos por nuestra herramienta de filtrado de contenido; y

- **2,556** correspondientes al Edificio Triangular y **99** al Edificio Tlatelolco, los cuales son de los IPS, resultando los más severos, ya que son lanzados directamente, por hackers hacía las direcciones Ip de la SRE.

En ese tenor, los números de serie o de parte, modelo de módems y routers, si se cuenta con contraseña para acceder a la configuración, administración y la forma en que se le asigna la IP, así como empleados, resultan información sensible, cuyo conocimiento podría permitir o facilitar el eventual sabotaje, monitoreo y/o control remoto de los equipos de las Unidades Administrativas integrantes de esta Secretaría, incluyendo aquellas reconocidas como instancias de seguridad nacional, de conformidad con las Bases de Colaboración en el marco de la Ley de Seguridad Nacional, celebradas par el Titular de la Secretaría de Gobernación, en su carácter de Secretario Ejecutivo del Consejo de Seguridad Nacional, y la Titular de la Secretaría de Relaciones Exteriores, publicadas en el DOF de fecha 27 de mayo de 2008.

Es así que la Ley de Seguridad Nacional señala:

[Se transcribe el artículo 51 de la Ley de Seguridad Nacional]

La publicidad de las normas, procedimientos, métodos, fuentes, especificaciones técnicas, tecnología o equipo útiles para la consecución de las atribuciones a cargo de este sujeto obligado, no sólo implica la actualización o potenciación de múltiples amenazas a las bases de datos y las operaciones de las Instancias de Seguridad Nacional de esta Secretaría, sino de todas sus Unidades Administrativas, lo que podría implicar afectaciones en los diversos trámites y servicios que se prestan a la ciudadanía en general.

f) Ahora bien, contrario a lo expresado por el recurrente, la información requerida no forma parte de las obligaciones de transparencia contenidas de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), como se puede apreciar a continuación.

[Se transcribe el artículo 70 fracción XXXIV de la Ley General de Transparencia y Acceso a la Información Pública]

De los formatos que el INAI ha determinado para dar cumplimiento a esta obligación, particularizándose a bienes muebles, resaltan los siguientes rubros:

34-A Inventario de bienes muebles.

- *Descripción del bien; Código de identificación, en su caso;*
- *Institución a cargo del bien mueble, en su caso;*
- *Número de inventario; Monto unitario del bien;*
- *Área(s) responsable(s) que genera(n), posee(n), publica(n) y actualizan la información*

34-B Inventario de altas practicadas a bienes muebles.

- *Descripción del bien;*
- *Número de inventario;*
- *Causa de alta;*
- *Valor del bien a la fecha de la alta;*
- *Área(s) responsable(s) que genera(n), posee(n), publica(n) y actualizan la información*

34-C Inventario de bajas practicadas a bienes muebles.

- *Descripción del bien;*
- *Número de inventario;*
- *Causa de baja;*
- *Fecha de baja;*
- *Valor del bien a la fecha de la baja;*
- *Área(s) responsable(s) que genera(n), posee(n), publica(n) y actualizan la información*

34-G Inventario de bienes muebles e inmuebles donados.

- *Descripción del bien;*
- *Actividades a que se destinará el bien (catálogo);*
- *Valor de adquisición o de inventario del bien donado;*
- *Área(s) responsable(s) que genera(n), posee(n), publica(n) y actualizan la información*

Es por todo lo anterior; que dada la existencia del riesgo, su probabilidad y especificidad; la Secretaría de Relaciones Exteriores se encuentra constreñida a tomar acciones preventivas a fin de salvaguardar la información sensible que obra en su poder, siendo la clasificación de la información como Reservada por un periodo de 5 años, el acto jurídico idóneo para tales efectos.

III. Con el fin de contar con los elementos necesarios para dar correcta atención al presente recurso de revisión, este sujeto obligado procedió a consultar de nueva cuenta a las áreas administrativas que originalmente dieron respuesta a la solicitud de acceso a la información.

Respuesta de la Unidad Administrativa consultada: la **DIRECCIÓN GENERAL DE TECNOLOGÍAS DE INFORMACIÓN E INNOVACIÓN** mediante correo electrónico TIN **3524**/2018 de fecha 18 de septiembre de 2018, respondió lo siguiente:

"Antes de entrar a estudio de los agravios hechos valer por el peticionario, se informa que esta Cancillería brindó la respuesta en su totalidad, cubriendo cada una de las preguntas formuladas por el peticionario, como se acreditara en las líneas siguientes.

***En el agravio primero**, el peticionario argumenta que se transgredió el principio de máxima Publicidad y que la respuesta brindada no recaía en el supuesto de información reservada, ya que de ninguna forma compromete la seguridad nacional, la seguridad pública o la defensa nacional y menos aún vulnerar o altera el normal desarrollo de las funciones desempeñadas por el sujeto obligado.*

*Al respecto, para la pregunta número **1. Los números de serie de cada uno de los equipos de cómputo y de cada MODEMS, ROUTERS (rúters) o Puntos de acceso inalámbricos en posesión del sujeto obligado**, así como para el inciso c) **Forma en que cada equipo obtiene o asigna, según sea el caso, la dirección IP privada en la red de forma manual o por media del Protocolo de Configuración Dinámica de Host DHCP**, ésta Secretaría informó que dicha información compromete la seguridad nacional y revela especificaciones técnicas de equipos útiles a la generación de inteligencia, por lo que no se encuentran abiertos a toda persona, aunado a que si bien es cierto existe la información de los equipos en las páginas del fabricante, también lo es que están enumerados de conformidad con sus características, sin que se especifique quienes son sus compradores, la finalidad para la que fueron adquiridas; ni las ubicaciones de los equipos, por lo que al proporcionar la información solicitada el usuario conocerá especificamente los equipos que se encuentran en las unidades administrativas que integran de esta Secretaría y por lo tanto se podrían lanzar ataques cibernéticos desde alguno o algunos de los equipos de la red de computadoras, introducir algún tipo de malware a la red, infectar el portal web o incluso paralizar las actividades de la res de computadoras, entre otras.*

En ese sentido, el conocer el número de serie y la forma de cómo se asignan las dirección IP, no es una vulnerabilidad en sí, pero si algún hacker tuviera conocimiento del mismo, le serviría para indagar con el fabricante lo siguiente:

- *El lote de equipos al que pertenece los números de serie*

- *Con esto podría investigar que componentes tenían los equipos de dicho lote que fueron entregados como son: Modelo de Tarjeta Madre, Memoria RAM, Versión de BIOS, tarjeta de red, etc.*
- *Una vez con el conocimiento anterior, podría dedicarse a investigar que vulnerabilidades tiene el tipo de tarjeta madre, las vulnerabilidades del BIOS y lanzar un ataque en específico.*
- *Como una alegoría, en una chapa de seguridad, al conocer el número de serie podría investigar qué tipo de cilindro y componentes internos tiene el modelo para así allegarse de elementos específicos para lograr abrirla sin la llave.*

Esta Dirección General llega a la conclusión de que si bien es cierto existe el derecho de acceso a la información, también lo es que dicho derecho debe tener una utilidad pública y en el caso que nos ocupa no se detecta que dicha información lo sea, ya que lejos de beneficiar a la colectividad, se estaría poniendo en riesgo la información de miles de ciudadanos bajo resguardo de esta Secretaría, ya que la obtención de la información beneficiaría a una persona o pequeño grupo. Lo cual refuerza lo ya mencionado, en virtud de que la información que se aloja en los equipos es la que generan las unidades administrativas de la Cancillería, dentro de las cuales existen algunas que cuentan con el carácter de Instancias de Seguridad Nacional, de conformidad con las Bases de Colaboración que en el marco de la Ley de Seguridad Nacional. Por ende, la información que se genera también se encuentra catalogada como de Seguridad Nacional, actualizándose la causal de reserva contenida en el artículo 110, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación el artículo 51, fracción I de la Ley de Seguridad Nacional.

Adicionalmente y en el ámbito de máxima transparencia, la Secretaría consultó al proveedor, el cual es dueño de los equipos, si encontraba algún inconveniente de que se otorgara la información requerida, argumentando lo siguiente:

"PRIMERO.- De conformidad con la cláusula décima octava del contrato plurianual de prestación del servicio de arrendamiento de bienes muebles propalado con la Secretaría de Relaciones Exteriores, la cual establece que las partes se obligan a guardar la información que conozcan con motivo del desarrollo y cumplimiento del contrato, en virtud de que la información que se genere derivada del objeto del mismo está protegida por la Ley de Seguridad Nacional y se encuentra clasificada como reservada y/o confidencial en los términos de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP).

SEGUNDO.- De acuerdo al artículo 99 de la LFTAIP, que establece que la información clasificada como reservada; de acuerdo al artículo 110 de dicha ley, podría permanecer con tal carácter hasta por 5 años a partir de la fecha en que se clasifica como tal.

TERCERO.- El artículo 110 de la LFTAIP contempla la información que se puede considerar como reservada, y en el artículo 113 de La misma ley se establece lo que se clasifica como información confidencial.

En virtud de lo anterior, y toda vez que la información que se nos requiere contempla información sensible, como contraseñas de acceso, números de serie, versión del BIOS de los equipos, sistema operativo, entre otra, el divulgar la misma provocaría, entre otros, los siguientes riesgos:

1. Cualquier persona en posesión de la misma podría acceder a la información de los equipos (PCs) en uso en la Secretaría.
2. Al tener acceso a los equipos se podría buscar alguna vulnerabilidad de seguridad en la red de computadoras de la Secretaría y acceder a la información contenida en los sistemas de procesamiento y almacenamiento de información de la dependencia.
3. Lanzar ataques cibernéticos desde alguno o algunos de los equipos de la red de computadoras de la Secretaría.
4. Introducir algún tipo de malware a la red de computadoras de la Secretaría.
5. Infectar el portal web de la Secretaría.
6. Paralizar las actividades de la red de computadoras de la Secretaría.

Así las cosas, sí esta H. Secretaría insistiera en requerir dicha información de acuerdo a su solicitud, sería requisito previo el modificar el contrato en el clausulado correspondiente, y bajo su propio riesgo, insistiendo en que se podría vulnerar el equipo y comprometer la información contenida en los equipos propiedad de mi representada.

Basamos la contestación al presente oficio, en términos del artículo 3 de la LFTAIP, el cuál a continuación nos permitimos transcribir, así como en los artículos de la misma ley referidos en el cuerpo del presente memorial:

[Se transcribe el artículo 3 de la Ley Federal de Transparencia y Acceso a la Información Pública]

En conclusión, tanto esta Secretaría considera NO, viable proporcionar la información a que hace alusión el solicitante, en virtud de que proporcionarla pondría en riesgo la seguridad de la información contenida en los equipos, ya que los equipos que se encuentran instalados y conectados a la Red de la Secretaria, por lo que es considerado de que se transgrede la seguridad de los equipos instalados y se estaría en posibilidad de transgredir la totalidad de los equipos con los que cuenta la Secretaría, aunado a que se está considerado el hecho de que la persona, compañía, grupo o conjunto de personas con el conocimiento al respecto, podrían lanzar ataques cibernéticos desde alguno o algunos de los equipos de la red de

computadoras, introducir algún tipo de malware a la red, infectar el portal web o incluso paralizar las actividades de la red de computadoras de la Secretaría, entre otras.

Asimismo, esta unidad administrativa señala que los servicios contratados a través de los proveedores de servicios de Telecomunicaciones y de Seguridad Informática a grandes rasgos son servicios múltiples de telefonía, red multiservicios nacional, servicio integral de voz y datos y, servicios de seguridad informática que incluyen la implementación, administración, operación, mantenimiento y suministro de servicios de seguridad informática, servicios de red voz y datos, telefonía, acceso a internet y enlaces WAN en los diferentes inmuebles que ocupa "LA SECRETARÍA", y no el arrendamiento de Módems o routers y de cortafuegos (firewalls), ya que dichos componentes son utilizados por los proveedores para poder proporcionar los servicios contratados, de ahí que esta Secretaría no cuente con la información solicitada referente a "ordenado por número de serie".

Para robustecer lo arriba citado, se informa que existen diversos tipos de intentos de hackeo:

- *Los que corresponden a Antivirus son realizados por malware que se intenta infiltrar en el SO de los equipos personales y servidores.*
- *Los de Filtrado Web son troyanos que están dentro del código de páginas web y que el usuario no lo detecta al querer abrir y navegar por estos sitios. Estos ataques son contenidos por nuestra herramienta de filtrado de contenido.*
- *Los más severos son los de IPS y que si son lanzados directamente por hackers hacia las direcciones Ip de la SRE.*

Antivirus SRE Nacional	***Antivirus Exterior***	***Filtrado WEB***	***IPS Firewall Alameda***	***IPS Firewall Triangular***
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

En ese sentido, el conocimiento o posesión de la información requerida podría permitir que cualquier tercero contara con los elementos suficientes para encontrar vulnerabilidades y acceder remotamente a los equipos y a su contenido.

Ahora bien, atendiendo a lo dispuesto en el artículo 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, a continuación, se establece la prueba de daño:

I. La divulgación de la información que se reserva representa un riesgo real, demostrable e identificable de perjuicio significativo a los intereses del gobierno mexicano. –La información reservada consistente en los números de serie, si se cuenta con contraseña para acceder a la configuración u administración y la forma en como se le asigna la IP, los cuales se consideran sensibles en virtud de que dan cuenta de los equipos y tecnología empleadas por las Unidades Administrativas de esta Secretaría, resaltando que algunas de ellas realizan actividades en el marco de la Seguridad Nacional, derivado de su reconocimiento como Instancia de Seguridad Nacional. En virtud de lo anterior, las ubicaciones, tecnologías utilizadas y demás elementos de carácter técnico, representan información reservada, ya que dan cuenta de las características técnicas de la infraestructura contratada, la cual soporta los sistemas centrales que contienen bases de datos e información, lo que podría ser aprovechada por terceros con conocimientos técnicos para detectar puntos de vulnerabilidad en la infraestructura informática de la Secretaría de Relaciones Exteriores, conocer su capacidad de reacción en materia de seguridad informática, cuestión que potenciaría actos de sabotaje, monitoreo y/o control de los equipos de cómputo, siendo así susceptible a ser atacada a vulnerada afectando la integridad y disponibilidad de la información, teniendo como posibles consecuencias la interrupción del desarrollo de las atribuciones conferidas a esta Secretaría, incluidas aquellas que albergan información confidencial y/o sensible al tratarse de infraestructuras críticas, la cual es generada por las unidades administrativas de la Secretaría que son instancias de seguridad nacional, así como los servicios a la ciudadanía como es la emisión de documentación oficial por parte de la dependencia.

II. El riesgo de perjuicio supera el interés público general de que se difunda. - La divulgación de las características de los dispositivos solicitados permitiría conocer los mecanismos que sigue esta Secretaría para los servicios de red, a través de los cuales puede viajar información sensible y dan conectividad a equipos de cómputo. Adicionalmente, se protege el poder contar con una red y servicios de conectividad, que den continuidad operativa y permitan mejorar los sistemas y aplicativos con los que la Secretaría cuenta para funcionar internamente. En este sentido, es importante recalcar que los servicios brindados se realizan dentro del marco de seguridad nacional, por lo que el omitir la normatividad bajo la cual se rige, se traduciría en transgredir los sistemas en ambientes de desarrollo, calidad y producción que son utilizados para realizar la operación sustantiva; asimismo, se vulneraría los servicios los cuales requieren un alto nivel de disponibilidad, además del servicio de equipamiento para proporcionar servicios a la red interna de datos, entre otros.

III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio. - La limitación del derecho del solicitante a

conocer la información que se reservan es proporcional. El derecho a buscar y recibir información, si bien es un derecho fundamental, no es absoluto y puede ser limitado siempre y cuando: i) el fin sea constitucionalmente válido (fin legítimo); ii) la medida sea idónea para alcanzar el fin constitucionalmente válido; iii) no exista un medio menos lesivo; y, iv) la limitación sea proporcional en sentido estricto. (véanse tesis 1a. CCLXV/20l6 (10a.), 1a. CCLXVIII/20l6 (10a.), 1a. CCLXX/2016 (10a.) y la CCLXXII/2016 (10a.) de noviembre de 2016, derivadas del Amparo en Revisión 237/2014 Josefina Ricaño Bandala y otros, 4 de noviembre de 2015).

Por lo anterior, no le asiste la razón al peticionario de argumentar que de ninguna forma se compromete la seguridad nacional, pública o la defensa nacional y menos aún vulnera o altera el normal desarrollo de las funciones desempeñadas por el sujeto obligado, aunado a que dicha información ya había sido requerida con anterioridad e incluso al igual que el peticionario interponían recurso de revisión. Ahora bien, las resoluciones recaídas a los Recursos de Revisión números 2448/18, 2537/18, 2577/18 y 3661/18, en los cuales el Pleno del Instituto solicitó opinión a su Dirección General de Tecnologías de Información, robustece la respuesta brindada por esta Secretaría, ya que se determinó a grandes rasgos que, a través de un equipo de cómputo conectado a una red, es posible que se le permita a algún potencial atacante cibernético dirigir algún ataque informático, como lo es suplantación de identidad con usos maliciosos, interceptar, modificar o incluso retener datos que están en tránsito o un ataque de fuerza bruta el cual consiste en recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso al equipo.

De manera acertada en las 4 resoluciones ya citadas, se determinó de manera correcta reservar la información, en virtud de que es posible que se pueda ejecutar un potencial ataque al ponerse en riesgo la seguridad de la información perteneciente a la Secretaría que viaja por medio de estos dispositivos y misma que se encuentra contenida en los equipos conectados a estos, de ahí que contrario a lo argumentado por el peticionario, el dar a conocer los mecanismos o técnicas tendientes a robustecer la seguridad informática, pondría en vulnerabilidad a esta Secretaría ante posibles ataques.

Asimismo, el peticionario manifiesta que tanto el inciso d) Domicilio actual en donde se encuentra físicamente cada equipo y los números de serie, son datos públicos por disposición de la fracción XXXIV del artículo 70 de la Ley General, ya que esta debe formar parte de los inventarios de los bienes muebles en posesión o propiedad el sujeto obligado.

Al respecto, no le asiste la razón al peticionario, ya que para el inciso d), si se brindó la respuesta, informando los inmuebles en donde se encontraban físicamente instalados, siendo los siguientes:

- *Edificio Tlatelolco*

- *Edificio Triangular*
- *Instituto Matías Romero*
- *Ex Convento*

Ahora bien, el peticionario de manera incorrecta argumenta que el número de serie se encuentran abiertos al público, de conformidad con lo señalado en el artículo 70 fracción XXXIV de la Ley General (sic) lo anterior no es así, ya que confunde el número de inventario con un número de serie, lo cual son conceptos completamente distintos, el número de inventario es el que se asigna en una relación detallada, ordenada y valorada de los elementos que componen los objetos o bienes de la Dependencia y el cual no se está vinculado con algún detalle que pueda poner en riesgo la seguridad de esta Institución, de ahí que esta Secretaría haya reservado lo solicitado en primera instancia por el peticionario, como ya se informó el otorgar el número de serie, se permitiría dirigir algún ataque informático, como lo es suplantación de identidad con usos maliciosos, interceptar, modificar o incluso retener datos que están en tránsito o un ataque de fuerza bruta el cual consiste en recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso al equipo, reiterando que el Pleno del Institutor confirmó la respuesta brindada.

Por último, respecto a lo argumentado en el sentido de que el Servicio de Administración Tributaria, Instituto Federal de Telecomunicaciones, la Auditoría Superior de la Federación, Secretaría de Comunicaciones y Transportes, la Consejería Jurídica del Ejecutivo Federal, el Instituto Mexicano del Seguro Social y ese Instituto Nacional de Transparencia, sí entregaron la información requerida, se manifiesta que se desconoce las políticas de seguridad o la infraestructura con la que se cuenten en dichas dependencias, sin embargo, esta Secretaría reitera su postura de mantener reservada la información solicitada a través de la petición número 0000500130518.

***Respecto al Agravio Segundo**, el peticionario argumenta la falta de notificación de la Resolución del Comité de Transparencia, por la cual se clasifico la información requerida.*

El agravio que nos ocupa no es competencia de esta Dirección General, por lo que deberá ser contestado por el Comité de Transparencia.

Por lo que hace al Tercer Agravio**, el peticionario manifiesta que se deberá demostrar que la información en cuestión no se refiere a alguna de las facultades, competencias o funciones de esta Secretaría, además presume la existencia de la información respecto al inciso **a) Nombre de aquellas personas físicas que cuentan con las contraseñas administrativas o su equivalente para el manejo, administración y control de la configuración de cada equipo, y del inciso b) Tipo de contratación, empleo, cargo o comisión que desempeñan las personas que resulten del inciso a.

Por lo que hace a los nombres de aquellas personas físicas que cuentan con las contraseñas administrativas o su equivalente y el tipo de contratación, empiezo, cargo o comisión que desempeñan las personas que resulten del inciso anterior; se informa que los equipos son arrendados por esta Secretaría, de ahí que se desconozca el nombre, cargo y comisión de las personas a que hace alusión el solicitante, ya que no existe una relación laboral entre esta Secretaría y el personal que contrata los proveedores que brindan el servicio.

En este sentido, el proveedor no tiene la obligación, ni la Secretaría de contar con un listado de características o descripciones adicionales a las necesarias para dar cuenta del cumplimiento a los requerimientos previamente señalados en el contrato, ni la de elaborar dicho documento, en términos del criterio intitulado ***No existe obligación de elaborar documentos ad hoc para atender las solicitudes de acceso a la información,*** *que a la letra dispone:*

[Se transcribe el criterio emitido por el INAI, bajo el rubro "No existe obligación de elaborar documentos ad hoc para atender las solicitudes de acceso a la información"]

Se concluye que el peticionario de manera errónea, argumenta que esta Secretaría debe elaborar documentación exclusivamente para atender su solicitud, no obstante que existe un contrato en el cual quedaron asentadas derechos y obligaciones para ambas partes, no encontrándose el tener una relación del personal que laborara para la empresa, la que se acredita con la cláusula denominada "Responsabilidad Laboral" en la que el prestador de servicio reconoce y acepta ser el único patrón de todos y cada uno de los trabajadores que intervienen en el desarrollo y ejecución del arrendamiento y servicios pactados en el contrato, de forma tal, que deslinda de toda responsabilidad a la Secretaría, por lo que por ningún motivo se le considerará patrón solidario o sustituto.

En conclusión, no le asiste la razón al peticionario respecto al agravio que nos ocupa y contrario a lo manifestado por este, la Secretaría cumple con la obligación de transparencia, ya que pone a disposición del público la documentación que de acuerdo a las facultades conferidas se genera.

En otro orden de ideas y sin ser parte de la solicitud primigenia, el peticionario argumenta que la Secretaría transgrede el artículo 70 fracción VII de la Ley General (sic); de nueva cuenta es incorrecta la manifestación realizada, en virtud de que el directorio de esta Secretaría está actualizado, encontrándose todos los Servidores públicos pertenecientes a esta Dependencia, lo cual puede corroborar en la siguiente liga https://directorio.sre.gob.mx/

En virtud de lo anterior, este sujeto obligado dio cabal cumplimiento a lo dispuesto en la LFTAIP y demás disposiciones aplicables a la materia, al proporcionar la información requerida en punto g, de la solicitud de acceso a la información pública y, a su vez, haciendo del conocimiento del hoy recurrente, que por lo que respecta a lo señalado en resto de su solicitud, se actualiza el supuesto de Reserva contemplado en el artículo 110, fracción I de la misma ley y en el numeral Décimo Séptimo, fracción IV de los Lineamientos, notificándole la resolución administrativa CTA-2117 de fecha 28 de agosto de 2018, emitida por el Comité de Transparencia de la Secretaría de Relaciones Exteriores, en la cual se confirma la declaratoria de Reserva de la información atendiendo a la prueba de daño, así como a las debidas fundamentación y motivación de la Unidad Administrativa que de conformidad con las atribuciones que le han sido conferidas, resulta la facultada para dar cuenta de la información requerida; cumpliendo con todas las formalidades del procedimiento, por lo que en ningún momento se causó agravio alguno al particular.

En esa tesitura, se solicita atentamente a ese Instituto, tome en consideración todos los elementos descritos, bajo una perspectiva amplia, a manera de que su análisis incluya los factores de hecho, es decir, el contexto actual en cuanto a la seguridad informática mundial y los retos que está presentando, a efecto de determinar cómo factores de derecho y de hecho podrían interactuar entre sí, y los resultados que propiciarían de hacer pública la información requerida en la solicitud de acceso a la información origen del presente procedimiento.

Asimismo, de conformidad con lo anteriormente vertido, a juicio de este sujeto obligado, la divulgación de la información y los posibles usos que un tercero o terceros pudieran darle, representan alto riesgo para la seguridad de su estructura informática, por lo que se solicita respetuosamente a esa H. Ponencia someta a la consideración del Pleno de ese Instituto su proyecto de resolución en el cual se proceda a **CONFIRMAR** la respuesta emitida por la Secretaría de Relaciones Exteriores a la solicitud de acceso a la información con número de folio 0000500130518.

Atendiendo a los Alegatos expresados, se ofrecen las siguientes:

PRUEBAS

I. LA DOCUMENTAL PÚBLICA. - Consistente en la respuesta que a través del Sistema de Solicitudes de Información (SISI) se dio a la solicitud con folio 0000500130518, de cuya lectura se desprende que la Secretaría de Relaciones Exteriores, en todo momento ha cumplido con lo establecido en la normativa aplicable, relacionando esta prueba con todos y cada uno de los alegatos referidos en el presente ocurso.

II. LA DOCUMENTAL PÚBLICA. - Consistente en todos y cada uno de los oficios que han emitido el Comité de Transparencia y la Unidad de Transparencia, y que se agregan al

presente, de cuya lectura se desprende que la Secretaría de Relaciones Exteriores, ha cumplido con las obligaciones que le impone la Ley Federal de Transparencia y Acceso a la Información Pública, relacionando esta prueba con todos y cada uno de los alegatos referidos en el presente ocurso.

III. LA INSTRUMENTAL DE ACTUACIONES. - Consistente en todas y cada una de las actuaciones única y exclusivamente en tanto favorezcan los intereses de esta Dependencia, relacionando esta prueba con todos y cada uno de los alegatos referidos en el presente ocurso.

DERECHO

Fundan los presentes alegatos los artículos en los artículos 6°, de la Constitución Política de los Estados Unidos Mexicanos; 28 de la Ley Orgánica de la Administración Pública Federal; 2, 3, 61, 64, 65, 121, 123, 127, 133, 140, 147, 148 y 149, y Tercero Transitorio de la Ley Federal de Transparencia y Acceso a la Información Pública; 3°, fracción VII, 5, 6, 8 y 15 de la Ley Federal de Procedimiento Administrativo.

Por lo antes expuesto, a usted C. Comisionado Ponente, respetuosamente solicitamos:

PRIMERO. - Tener por presentado en tiempo y forma el presente escrito, expresándose alegatos y ofreciéndose los elementos de prueba que este Comité consideró favorables a los intereses de esta Secretaría.

SEGUNDO. - Desahogada la secuela procesal, proceder a **CONFIRMAR** la respuesta emitida por este sujeto obligado a la solicitud de acceso a la información presentada bajo el número de folio 0000500130518, atendiendo a los argumentos, pruebas y fundamentos de derecho expuestos en el presente escrito de alegatos

TERCERO. - En su oportunidad, y previos los trámites de ley, resolver presente asunto como total y definitivamente concluido y ordenar su archivo.
..." (sic)

El sujeto obligado adjuntó la digitalización de los documentos siguientes:

a) Formato emitido por el Sistema de Solicitudes de Información, expedido por este Instituto, el cual contiene el registro de la solicitud de acceso a la información con número de folio 0000500130518.

b) Oficio número UDT-3867/2018, del ocho de agosto del dos mil dieciocho emitido por el Titular de la Unidad de Transparencia, y dirigido al Director General del Servicio Exterior y de Recursos Humanos, a través del cual le comunica los plazos para dar atención a la solicitud de información.

c) Correo electrónico del ocho de agosto de dos mil dieciocho, emitido por la Unidad de Transparencia, y dirigido al Director General de Tecnologías de Información e Innovación y al Director General del Servicio Exterior y de Recursos Humanos, mediante el cual remite la solicitud de acceso a la información con número de folio 0000500130518.

d) Correo electrónico del veintisiete de agosto de dos mil dieciocho, emitido por el Director General de Tecnologías de Información e Innovación, y dirigido al Titular de Transparencia, mediante el cual remite oficio número TIN 3159/2018, emitido en la misma fecha de su envió, mediante el cual remite respuesta a la solicitud de acceso a la información con número de folio 0000500130518, cuyo contenido ha sido desarrollado en el resultando 8 de la presente resolución.

e) Oficio número CTA-21718, el cual contiene Acta del Comité de Transparencia de la Secretaría de Relaciones Exteriores, del veintiocho de agosto de dos mil dieciocho, cuyo contenido ha sido desarrollado en el resultando 2 inciso b) de la presente resolución.

f) Oficio número UDT-4459/2018, del veintinueve de agosto de dos mil dieciocho, suscrito por el Titular de la Unidad de Transparencia, y dirigido al solicitante, cuyo contenido ha sido desarrollado en el resultando 2 inciso a) de la presente resolución.

g) Copia del Formato emitido por el Sistema de Solicitudes de Información, a través del cual se registró la respuesta a la solicitud de acceso a la información con número de folio 0000500130518.

h) Acta de la Sesión Pública Ordinaria Núm. 113, del cinco de diciembre del dos mil dieciséis, emitido por el Pleno de la Suprema Corte de Justicia de la Nación, relacionada con el Centro de Investigación y Seguridad Nacional.

i) Resolución RRA 7151/17, del siete de febrero de dos mil dieciocho, emitida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

j) Resolución de la Sesión Extraordinaria 18/2018, del veinticinco de mayo de dos mil dieciocho, emitida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

18. Cierre de instrucción. El veintitrés de octubre de dos mil dieciocho, al no existir diligencias pendientes por desahogar, se declaró cerrada la instrucción, mismo que fue notificado a las partes el mismo día.

CONSIDERANDOS

PRIMERO. Competencia. El Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales es competente para conocer respecto del asunto, con fundamento en el artículo 6o, apartado A, fracción VIII, de la Constitución Política de los Estados Unidos Mexicanos; artículo 41 fracciones I, II y XI de la Ley General de Transparencia y Acceso a la Información Pública; artículos 21, fracciones I, II y XXIV, 29, fracciones I, VIII y X, 151 y 156 de la Ley Federal de Transparencia y Acceso a la Información Pública y artículos 12, fracciones I, V y XXXV, y 18, fracciones V, XV, XVI, XXVI y XXIX del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

SEGUNDO. Estudio de causales de improcedencia y sobreseimiento. Este Instituto procederá al estudio oficioso de las causales de improcedencia y sobreseimiento previstas en los artículos 161 y 162 de la Ley Federal de Transparencia y Acceso a la Información Pública, por tratarse de una cuestión de orden público y de estudio preferente.

Causales de improcedencia

En el artículo 161 de la Ley Federal de Transparencia y Acceso a la Información Pública, se dispone lo siguiente:

> "**Artículo 161.** El recurso será desechado por improcedente cuando:
> I. Sea extemporáneo por haber transcurrido el plazo establecido en el artículo 147 de la presente Ley;
> II. Se esté tramitando ante el Poder Judicial algún recurso o medio de defensa interpuesto por el recurrente;
> III. No actualice alguno de los supuestos previstos en el artículo 148 de la presente Ley;
> IV. No se haya desahogado la prevención en los términos establecidos en el artículo 150 de la presente Ley;
> V. Se impugne la veracidad de la información proporcionada;
> VI. Se trate de una consulta, o
> VII. El recurrente amplíe su solicitud en el recurso de revisión, únicamente respecto de los nuevos contenidos."

De las constancias que obran en autos, se desprende que en el caso concreto **no se actualiza alguna de las causales de improcedencia referidas**, en virtud de los siguientes argumentos:

I. Oportunidad del recurso de revisión. El recurso de revisión fue interpuesto en tiempo y forma, ya que el sujeto obligado notificó la respuesta impugnada, el veintinueve de agosto del dos mil dieciocho y el recurso de revisión fue interpuesto el cinco de septiembre del mismo año, es decir, dentro del plazo de quince días hábiles siguientes a la fecha en que fue notificada la respuesta al solicitante, previsto en el artículo 147 de la Ley Federal de Transparencia y Acceso a la Información Pública; lo anterior, tomando en consideración que el plazo comenzó a computarse, el treinta de agosto de dos mil dieciocho y feneció el diecinueve de septiembre del mismo año por lo que a la fecha de la presentación del medio de impugnación, transcurrieron cinco días hábiles.

II. Litispendencia. Este Instituto no tiene conocimiento de que se encuentre en trámite algún medio de impugnación ante el Poder Judicial de la Federación interpuesto por la parte recurrente, en contra del mismo acto que impugna a través del presente recurso de revisión.

III. Procedencia del recurso de revisión. Los supuestos de procedencia del recurso de revisión, se encuentran establecidos en el artículo 148 de la Ley Federal de Transparencia y Acceso a la Información Pública y en el caso concreto, resulta aplicable

el previsto en la fracción I y II, toda vez que la parte recurrente se inconformó con la clasificación e inexistencia aludida por el sujeto obligado.

IV. Falta de desahogo a una prevención. Este Instituto no realizó prevención alguna al particular derivado de la presentación de su recurso de revisión, ya que cumplió con lo dispuesto en el artículo 149 de la Ley Federal de Transparencia y Acceso a la Información Pública.

V. Veracidad. La veracidad de la respuesta no forma parte del agravio.

VI. Consulta. No se realizó una consulta en el presente caso.

VII. Ampliación. No se ampliaron los alcances de la solicitud a través del presente recurso de revisión.

Causales de sobreseimiento

En el artículo 162 de la Ley Federal de Transparencia y Acceso a la Información Pública, se establece lo siguiente:

> "**Artículo 162.** El recurso será sobreseído, en todo o en parte, cuando, una vez admitido, se actualicen alguno de los siguientes supuestos:
> **I.** El recurrente se desista expresamente del recurso;
> **II.** El recurrente fallezca o tratándose de personas morales que se disuelvan;
> **III.** El sujeto obligado responsable del acto lo modifique o revoque de tal manera que el recurso de revisión quede sin materia, o
> **IV.** Admitido el recurso de revisión, aparezca alguna causal de improcedencia en los términos del presente Capítulo."

En el caso concreto no hay constancia de que la parte peticionaria haya fallecido, se desistiera expresamente del recurso de revisión, que el sujeto obligado hubiere modificado o revocado el acto reclamado de tal manera que el recurso de revisión quedara sin materia o, que una vez admitido, apareciere alguna de las causales de improcedencia previstas en el artículo 161 de la Ley Federal de Transparencia y Acceso a la Información Pública; por consiguiente, ninguno de los supuestos establecidos en el artículo 162 del citado ordenamiento jurídico, se actualiza.

En consecuencia, este Órgano Colegiado se avocará al estudio de fondo del presente asunto.

TERCERO. Síntesis del caso y fijación de la Litis. El particular solicitó a la Secretaría de Relaciones Exteriores, le proporcionara, mediante la Plataforma Nacional de Transparencia, respecto de cada uno de los equipos de cómputo y de cada uno de los MODEMS, ROUTERS (rúters) o puntos de acceso inalámbricos en posesión del sujeto obligado, y ordenado por número de serie, lo siguiente:

a) Nombre de las personas físicas que cuentan con las contraseñas administrativas o su equivalente -permisos informáticos, credenciales administrativas, privilegios de súper usuario o su "root" para el manejo, administración y control de la configuración de cada equipo.

b) Tipo de contratación, empleo, cargo o comisión que desempeñan las personas que resulten del inciso anterior.

c) La forma en que cada equipo obtiene o asigna, según sea el caso, la dirección IP, es decir, si es forma manual o por medio del Protocolo de Configuración Dinámica Host DHCP

d) Domicilio actual en donde se encuentran físicamente cada equipo.

En respuesta, el sujeto obligado, a través de la **Dirección General de Tecnologías de Información e Innovación**, indicó respecto al **inciso "c"**, que la información es reservada ya que compromete la seguridad nacional ya que revela especificaciones técnicas de quipos útiles a la generación de inteligencia, por lo que no se encuentran abiertos a toda persona, ya que se podrían lanzar ataques cibernéticos desde alguno (s) de los equipos de la red de computadoras e introducir algún tipo de malware a la red e infectar el portal web o incluso paralizar las actividades de la red de computadoras. Por tanto, conocer el número de serie y la forma en cómo se asignan las direcciones IP, podría ser información para que un hacker pudiera indagar con el fabricante lo siguiente:

- El lote de equipos al que pertenecen los números de serie, con ello podría investigar qué componentes tenías lo equipos en dicho lote tales como modelo de tarjeta madre, memoria RAM; versión de BIOS, tarjeta de red, entre otros.

- Con ello, se podría indagar en las vulnerabilidades que tiene el tipo de tarjeta madre, el BIOS y lanzar un ataque específico.

En este sentido, se indicó que dar a conocer la información se estaría poniendo en riesgo la información de miles de ciudadanos bajo el resguardo de la Secretaría, ya que la información que se localiza en los equipos es la que generan las unidades administrativas de la Cancillería entre las que se encuentran las de carácter de instancias de Seguridad Nacional, de conformidad con las bases de colaboración en el marco de la Ley de Seguridad Nacional, por tanto, la información es reservada con fundamento en la fracción I del artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el artículo 51, fracción I de la Ley de Seguridad Nacional.

Adicionalmente, indicó se consultó con el proveedor dueño de los equipos, si consideraba algún inconveniente para la entrega de la información, sin embrago, indicó que de conformidad con la cláusula décima octava del contrato plurianual de prestación del servicio de arrendamiento de bienes muebles se establece que las partes se obligan a guardar la información que conozcan con motivo del desarrollo y cumplimiento del contrato ya que la información que se genere derivada del objeto del mismo está protegida por la Ley de Seguridad Nacional y se encuentra clasificada como reservada y/o confidencial en los términos de la Ley Federal de Transparencia y Acceso a la Información Pública.

En este sentido indicó que, al tratarse de información sensible como contraseñas de acceso, números de serie, versión BIOS de los equipos, Sistema operativo, entre otra, podría provocar riesgos como que cualquier persona pueda acceder a la información de los equipos, y vulnerar la seguridad en la red de computadoras y almacenamiento de información. En consecuencia, podría lanzar ataques, introducir algún tipo de malware, infectar el portal web y paralizar las actividades de la red de computadoras.

Asimismo, indicó que la Secretaría cuenta con servicios contratados a través de los proveedores de servicios de Telecomunicaciones y de Seguridad Informática, y no del

arrendamiento de Modems o routers y de cortafuegos, ya que dichos componentes son utilizados por los proveedores para poder proporcionar los servicios contratados, de ahí que esta Secretaría no cuente con la información solicitada en lo referente a "ordenado por número de serie".

En este sentido, el sujeto obligado emitió su prueba de daño, lo siguiente:

- La **divulgación de la información que se reserva representa un riesgo real, demostrable e identificable de perjuicio significativo a los intereses del gobierno mexicano**. -La información reservada consistente en los números de serie, si se cuenta con contraseña para acceder a la configuración u administración y la forma en como se le asigna la IP, los cuales se consideran sensibles en virtud de que dan cuenta de los equipos y tecnología empleadas por las Unidades Administrativas de esta Secretaría. En consecuencia, información reservada, ya que dan cuenta de las características técnicas de la infraestructura contratada, la cual soporta los sistemas centrales que contienen bases de datos e información, lo que podría ser aprovechada por terceros con conocimientos técnicos para detectar puntas de vulnerabilidad en la infraestructura informática de la Secretaría de Relaciones Exteriores, conocer su capacidad de reacción en materia de seguridad informática, cuestión que potenciaría actos de sabotaje, monitoreo y/o control de los equipos de cómputo.

- El **riesgo de perjuicio supera el interés público general de que se difunda**. - La divulgación de las características de los dispositivos solicitados permitiría conocer los mecanismos que sigue esta Secretaría para los servicios de red, a través de los cuales puede viajar información sensible y dan conectividad a equipos de cómputo.

- La **limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio**. - La limitación del derecho del solicitante a conocer la información que se reservan es proporcional.

En relación con los **incisos a y b**, indicó que se informa que los equipos son arrendados por esta Secretaría, de ahí que se desconozca el nombre, cargo y comisión de las personas a que hace alusión el solicitante, ya que no existe una relación laboral entre

esta Secretaría y el personal que contrata los proveedores que brindan el servicio. En este sentido, el proveedor no tiene obligación, ni la Secretaría de contar con un listado de características o descripciones adicionales a las necesarias para dar cuenta del cumplimiento a los requerimientos previamente señalados, ni la de elaborar dicho documento, en términos del Criterio 03/17, emitido por el Pleno de este Instituto.

Por otra parte, indicó que los equipos se encuentran físicamente instalados conforme al organigrama institucional en el edificio Tlatelolco, Triangular, Matías Romero y Ex convento.

Inconforme con la respuesta, el particular se inconformó ante este Instituto manifestando lo siguiente:

- Se inconformó con la clasificación invocada por el sujeto obligado, ello en virtud, de que manifestó respecto al **inciso c**, es información pública ya que la fracción XLVIII del artículo 70 de la Ley General de Transparencia y Acceso a la Información Pública señala que el sujeto obligado debe hacer pública cualquier información que sea de utilidad o se considere relevante. Asimismo, refirió que los **números de serie** es información pública ya que debe formar parte de los inventarios de los bienes inmuebles o en posesión del sujeto obligado, además de que no compromete la seguridad nacional, la seguridad pública o la defensa nacional; y menos aún vulnerar o alterar el normal desarrollo de las funciones desempeñadas por el sujeto obligado.

- Así también, refirió que la información solicitada en el inciso c, permite conocer si emplea adecuadamente mecanismos o técnicas tendientes a robustecer la seguridad informática del sujeto obligado, lo cual a su vez da a conocer que tan protegida se encuentra la información que circula por la red del sujeto obligado.

- Respecto a la inexistencia de la información de los **incisos a y b**, indicó que, si bien se celebró un contrato de arrendamiento, lo cierto es que el sujeto obligado tiene el uso y goce temporal de los equipos. En este sentido, debe existir determinadas personas que ocupen los equipos. Además, es información pública

por disposición de los artículos 68 de la Ley Federal de Transparencia y Acceso a la Información Pública y 70, fracción VII de la Ley General.

- Que el sujeto obligado omitió notificarle la resolución emitida por el Comité de Transparencia de la Secretaría de Relaciones Exteriores, a través de la cual clasificó la información requerida.

- Que el sujeto obligado omitió notificar la resolución a través de la cual se confirmó la inexistencia de la información.

En relación con lo anterior, es preciso señalar que el particular no manifestó inconformidad respecto del **inciso "d"**, lo que permite válidamente colegir que esos extremos de la respuesta fueron consentidos tácitamente por el peticionario.

En este sentido, cabe recordar que el artículo 93 de la Ley Federal de Procedimiento Administrativo,[1] establece que no se podrán revocar o modificar los actos administrativos en la parte no impugnada por los recurrentes.

Asimismo, se hace del conocimiento a la parte solicitante que este recurso de revisión, era el instrumento idóneo para inconformarse en parte o en todo de la respuesta inicial si le hubiera causado agravio alguno.

Por tanto, las partes de la respuesta inicial del sujeto obligado que no fueron combatidas por la parte recurrente se entienden consentidas y no serán materia de estudio en el análisis de la presente resolución.

Al respecto, resultan aplicables los criterios sostenidos por el Poder Judicial de la Federación, en las siguientes tesis:

"No. Registro: 204,707
Jurisprudencia
Materia(s): Común
Novena Época
Instancia: Tribunales Colegiados de Circuito

[1] De aplicación supletoria a la Ley Federal de Transparencia y Acceso a la Información Pública de conformidad a su artículo 7°.

Fuente: Semanario Judicial de la Federación y su Gaceta
II, Agosto de 1995
Tesis: VI.2o. J/21
Página: 291

ACTOS CONSENTIDOS TÁCITAMENTE. Se presumen así, para los efectos del amparo, los **actos del orden civil y administrativo, que no hubieren sido reclamados en esa vía dentro de los plazos que la ley señala**."

"Época: novena época.
Registro: 176608.
Instancia: Tribunales Colegiados de Circuito.
Tipo de tesis: jurisprudencia.
Fuente: Semanario Judicial de la Federación y su Gaceta.
Tomo xxii, diciembre de 2005,
Materia(s): común.
Tesis: vi.3o.c. j/60.
Página: 2365.

ACTOS CONSENTIDOS. SON LOS QUE NO SE IMPUGNAN MEDIANTE EL RECURSO IDÓNEO. Debe reputarse como consentido el acto que no se impugnó por el medio establecido por la ley, ya que si se hizo uso de otro no previsto por ella o si se hace una simple manifestación de inconformidad, tales actuaciones no producen efectos jurídicos tendientes a revocar, confirmar o modificar el acto reclamado en amparo, lo que significa consentimiento del mismo por falta de impugnación eficaz."

En su oficio de alegatos, el sujeto obligado reitero su respuesta inicial e indicó que en diversas resoluciones relacionadas con la materia de la solicitud de acceso a la información que nos ocupa, el Pleno de este Instituto actualizaba la causal de resera prevista en la fracción I del artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública.

Asimismo, indicó que la Secretaría ha sido blanco de múltiples intentos de hackeo, tanto de manera directa, como a través de correos electrónicos con direcciones web o archivos electrónicos maliciosos, mismos que a la fecha de respuesta a la solicitud por parte de la Dirección General de Tecnologías de Información e Innovación, se reportaron diversas amenazas detectadas y bloqueadas.

En este sentido, indicó que los números de serie o de parte, modelo de módems y routers, si se cuenta con contraseña para acceder a la configuración, administración y la forma en que se le asigna la IP, así como empleados, resultan información sensible, cuyo conocimiento podría permitir o facilitar el eventual sabotaje, monitoreo y/o control remoto de los equipos de las Unidades Administrativas integrantes de esta Secretaría, incluyendo aquellas reconocidas como instancias de seguridad nacional, de conformidad con las Bases de Colaboración en el marco de la Ley de Seguridad Nacional.

Por otra parte, indicó que para el inciso d, si se brindó respuesta informando los inmuebles en donde se encontraba físicamente instalados.

Así también, refirió que la información no forma parte de las obligaciones de transparencia contenidas de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), toda vez que el número de inventario con un número de serie, lo cual son conceptos distintos, ya que primero se refiere a una relación detallada, ordenada y valorada de los elementos que componen los objetos o bienes de la dependencia y el cual no se está vinculando con algún detalle que pueda poner que pueda poner en riesgo la seguridad de la institución.

Finalmente, en relación con el contenido "a", reiteró que los equipos son arrendados, por tanto, se desconoce el nombre, cargo y comisión de las personas a que hace alusión el solicitante, ya que no existe una relación laboral entre la Secretaría y el personal que contrata los proveedores que brindan el servicio.

Finalmente, el sujeto obligado ofreció como pruebas la Instrumental de Actuaciones y la Presuncional Legal y Humana.

Al respecto, se señala que la mismas se desahogan por su propia y especial naturaleza, tal y como se señala en el criterio intitulado **PRUEBAS INSTRUMENTAL DE ACTUACIONES Y PRESUNCIONAL LEGAL Y HUMANA. NO TIENEN VIDA PROPIA LAS** que refiere que la prueba instrumental de actuaciones y la presuncional legal y humana, no tienen desahogo, es decir, que no tienen vida propia, pues no es más que el nombre que en la práctica se ha dado a la totalidad de las pruebas recabadas en el

juicio, por lo que respecta a la primera; y por lo que corresponde a la segunda, ésta se deriva de las mismas pruebas que existen en las constancias de autos.

Por lo tanto, en el caso concreto, las pruebas descritas se tienen por desahogadas por su propia y especial naturaleza, toda vez que se trata de documentales públicas, operando a su favor la instrumental de actuaciones y la presuncional legal y humana, toda vez que el artículo 130 del Código Federal de Procedimientos Civiles, dispone que los documentos públicos harán fe en juicio. Lo anterior, aplicado a la sustanciación de los recursos de revisión como el que se resuelve, se traduce en que cualquier documento emitido por las partes, en atención a las solicitudes de información, en principio y salvo que exista un elemento probatorio que lo controvierta, debe **hacer prueba plena**.

En tales circunstancias, conviene traer a colación, por analogía, la Tesis P. XLVII/96, visible en la página 125 del Semanario Judicial de la Federación y su Gaceta, Tomo III, abril de 1996, Novena Época, de rubro y texto siguientes:

> "**PRUEBAS. SU VALORACIÓN CONFORME A LAS REGLAS DE LA LÓGICA Y DE LA EXPERIENCIA, NO ES VIOLATORIA DEL ARTÍCULO 14 CONSTITUCIONAL (ARTÍCULO 402 DEL CÓDIGO DE PROCEDIMIENTOS CIVILES PARA EL DISTRITO FEDERAL).** El Código de Procedimientos Civiles del Distrito Federal, al hablar de la valoración de pruebas, sigue un sistema de libre apreciación en materia de valoración probatoria estableciendo, de manera expresa, en su artículo 402, que **los medios de prueba aportados y admitidos serán valorados en su conjunto por el juzgador, atendiendo a las reglas de la lógica y de la experiencia**; y si bien es cierto que la garantía de legalidad prevista en el artículo 14 constitucional, preceptúa que las sentencias deben dictarse conforme a la letra de la ley o a su interpretación jurídica, y a falta de ésta se fundarán en los principios generales del derecho, **no se viola esta garantía porque el juzgador valore las pruebas que le sean aportadas atendiendo a las reglas de la lógica y de la experiencia, pues el propio precepto procesal le obliga a exponer los fundamentos de la valoración jurídica realizada y de su decisión.**"

Así también, el sujeto obligado ofreció como pruebas, diversas documentales públicas, mismas que serán analizadas en términos del siguiente criterio emitido por el Poder Judicial Federal, obligatorio para ésta autoridad en términos del artículo 217, de la Ley de amparo, que a continuación se inserta:

"Época: Décima Época
Registro: 160064
Instancia: Tribunales Colegiados de Circuito
Tipo de Tesis: Jurisprudencia
Fuente: Semanario Judicial de la Federación y su Gaceta
Libro IX, Junio de 2012, Tomo 2
Materia(s): Civil
Tesis: I.5o.C. J/36 (9a.)
Página: 744

PRUEBAS. SU VALORACIÓN EN TÉRMINOS DEL ARTÍCULO 402 DEL CÓDIGO DE PROCEDIMIENTOS CIVILES PARA EL DISTRITO FEDERAL.

El artículo 402 del Código de Procedimientos Civiles para el Distrito Federal establece que los Jueces, al valorar en su conjunto los medios de prueba que se aporten y se admitan en una controversia judicial, deben exponer cuidadosamente los fundamentos de la valoración jurídica realizada y de su decisión, lo que significa que la valoración de las probanzas debe estar delimitada por la lógica y la experiencia, así como por la conjunción de ambas, con las que se conforma la sana crítica, como producto dialéctico, a fin de que la argumentación y decisión del juzgador sean una verdadera expresión de justicia, es decir, lo suficientemente contundentes para justificar la determinación judicial y así rechazar la duda y el margen de subjetividad del juzgador, con lo cual es evidente que se deben aprovechar "las máximas de la experiencia", que constituyen las reglas de vida o verdades de sentido común."

Con base en lo anterior, la presente resolución verificará la legalidad de la respuesta otorgada por el sujeto obligado en relación con el agravio sostenido por los particulares, en términos de la Ley Federal de Transparencia y Acceso a la Información Pública, su Reglamento y demás disposiciones aplicables.

CUARTO. Estudio de Fondo. De las constancias que integran el recurso de revisión, se advierte que el agravio del recurrente **resulta parcialmente fundado**, lo que conlleva a **MODIFICAR** la respuesta de Secretaría de Relaciones Exteriores, con base en las siguientes consideraciones:

En el caso en concreto, se tiene que la particular se inconformó ante este Instituto, respecto de lo siguiente.

a) La **inexistencia** de **los incisos a y b**, esto es, el nombre da las personas que cuentan con las contraseñas administrativas o su equivalente -permisos

informáticos, credenciales administrativas, privilegios de súper usuario o su "root" para el manejo, administración y control de la configuración de cada equipo; y el tipo de contratación, empleo, cargo o comisión que desempeñan. Así como, que no le fue notificada el acta emitida por su Comité de Transparencia.

b) La **clasificación** de la información relacionada con la forma en que cada equipo obtiene o asigna, según sea el caso, la dirección IP, es decir, si es forma manual o por medio del Protocolo de Configuración Dinámica Host DHCP; **inciso c**, y el **número de serie**. Asimismo, que no le fue notificada el acta de inexistencia respectiva.

Una vez señalado lo anterior, se procederá a realizar el análisis respectivo.

- **Análisis de inexistencia.**

Al respecto, el procedimiento de búsqueda previsto en la Ley Federal de Transparencia y Acceso a la Información Pública, establece lo siguiente:

> "**Artículo 124**. Tratándose de solicitudes de acceso a información formuladas mediante la Plataforma Nacional, se asignará automáticamente un número de folio, con el que los solicitantes podrán dar seguimiento a sus requerimientos. En los demás casos, la Unidad de Transparencia tendrá que registrar y capturar la solicitud de acceso en la Plataforma Nacional y deberá enviar el acuse de recibo al solicitante, en el que se indique la fecha de recepción, el folio que corresponda y los plazos de respuesta aplicables.
> [...]
>
> **Artículo 133.** Las Unidades de Transparencia deberán garantizar que las solicitudes se turnen a todas las Áreas competentes que cuenten con la información o deban tenerla de acuerdo a sus facultades, competencias y funciones, con el objeto de que realicen una búsqueda exhaustiva y razonable de la información solicitada.
>
> **Artículo 134.** La Unidad de Transparencia será el vínculo entre el sujeto obligado y el solicitante, ya que es la responsable de hacer las notificaciones a que se refiere esta Ley. Además, deberá llevar a cabo todas las gestiones necesarias con el sujeto obligado a fin de facilitar el acceso a la información.

> **Artículo 135.** La respuesta a la solicitud deberá ser notificada al interesado en el menor tiempo posible, que no podrá exceder de veinte días, contados a partir del día siguiente a la presentación de aquélla.
>
> **Artículo 136**. El acceso se dará en la modalidad de entrega y, en su caso, de envío elegidos por el solicitante. Cuando la información no pueda entregarse o enviarse en la modalidad elegida, el sujeto obligado deberá ofrecer otra u otras modalidades de entrega.
> [...]"

De conformidad con la normativa en cita, se tiene que la **Unidad de Transparencia garantizará que las solicitudes se turnen a todas las áreas competentes que cuenten con la información o deban tenerla de acuerdo a sus facultades, competencias y funciones, para que realicen una búsqueda exhaustiva de la información solicitada**.

El acceso se dará en la modalidad de entrega y en su caso, de envío elegido por el solicitante, en caso de que no pueda entregarse en dicha modalidad, el sujeto obligado deberá ofrecer otras.

La Unidad de Transparencia es la responsable de hacer las notificaciones correspondientes, **además de llevar a cabo todas las gestiones necesarias con el sujeto obligado para facilitar el acceso a la información**. Así, la respuesta a las solicitudes deberá ser notificada al interesado en el menor tiempo posible, que no podrá exceder veinte días, contados a partir de la presentación de ésta.

Asimismo, la citada norma establece lo siguiente:

> "**Artículo 141.** Cuando la información no se encuentre en los archivos del sujeto obligado, será aplicable para el Comité de Transparencia el procedimiento previsto en el Capítulo I del Título Séptimo de la Ley General, y lo establecido en este artículo:
>
> I. Analizará el caso y tomará las medidas necesarias para localizar la información;
>
> II. Expedirá una resolución que confirme la inexistencia del Documento;
>
> III. Ordenará, siempre que sea materialmente posible, que se genere o se reponga la información en caso de que ésta tuviera que existir en la medida que deriva del ejercicio de

sus facultades, competencias o funciones, o que previa acreditación de la imposibilidad de su generación, exponga de forma fundada y motivada, las razones por las cuales en el caso particular no ejerció dichas facultades, competencias o funciones o que la documentación de que se trate haya sido objeto de baja documental en términos de las disposiciones aplicables en materia de archivos, lo cual notificará al solicitante a través de la Unidad de Transparencia, y

IV. Notificará al Órgano Interno de Control o equivalente del sujeto obligado quien, en su caso, deberá iniciar el procedimiento de responsabilidad administrativa que corresponda.
[...]

Artículo 143. La resolución del Comité de Transparencia que confirme la inexistencia de la información solicitada contendrá los elementos mínimos que permitan al solicitante tener la certeza de que se utilizó un criterio de búsqueda exhaustivo, además de señalar las circunstancias de tiempo, modo y lugar que generaron la inexistencia en cuestión, y señalará al servidor público responsable de contar con la misma.
[...]"

De conformidad con los ordenamientos en cita, se tiene que cuando la información no se localice en los archivos del sujeto obligado, el Comité de Transparencia realizará lo siguiente:

- Analizará el caso y tomará las medidas necesarias para localizar la información.

- Expedirá una resolución en que confirme la inexistencia del documento, la cual contendrá los elementos mínimos que permitan al solicitante tener certeza de que **se utilizó un criterio de búsqueda exhaustivo, además de señalar las circunstancias de tiempo, modo y lugar que generaron la inexistencia en** comento, y señalará al servidor público responsable de contar con la misma.

- En su caso, ordenará –siempre que sea materialmente posible- **(i)** que se genere o reponga la información en caso de que ésta tuviera que existir -derivado del ejercicio de sus facultades-; **(ii)** que previa acreditación de la imposibilidad de su generación, se exponga de manera fundada y motivada las razones por las cuales en el caso en particular, no ejerció sus facultades; y **(iii)** en caso, de que la

documentación haya sido objeto de baja documental, esto deberá ser notificado al solicitante.

Una vez señalado lo anterior, resulta necesario citar lo que al respecto establece el Reglamento Interior de la Secretaría de Relaciones Exteriores, dispone lo siguiente:

Artículo 2. Corresponde a la Secretaría:

I. Ejecutar la política exterior de México;

II. Promover, propiciar y coordinar las acciones en el exterior de las dependencias y entidades de la Administración Pública Federal, de conformidad con las atribuciones que a cada una de ellas corresponda;

III. Dirigir el Servicio Exterior Mexicano;

IV. Intervenir en toda clase de tratados, acuerdos y convenciones de los que el país sea parte,

V. Supervisar el cumplimiento de los objetivos consignados en el Programa de Cooperación Internacional para el Desarrollo.
[...]

Artículo 5.- Al frente de la Secretaría de la Secretaría de Relaciones Exteriores habrá un Secretario del Despacho, titular de la misma quien, para el desahogo de los asuntos de su competencia, se auxiliará de las unidades administrativas siguientes:
[...]

E) Oficialía Mayor;
[...]

H) Direcciones Generales:
[...]

XXII. De Tecnologías de Información e Innovación;
[...]

Artículo 11. Al frente de la Oficialía Mayor habrá un Oficial Mayor, quien tendrá las atribuciones siguientes:

I. Dirigir las políticas, normas, sistemas y procedimientos administrativos para la organización y funcionamiento de la Secretaría y para la gestión de los recursos humanos, financieros, materiales, informáticos, así como las que correspondan a las unidades administrativas que tenga adscritas y darle seguimiento a su observancia;
[...]

XXI. Dirigir las relaciones laborales de la Secretaría, así como promover la capacitación y actualización de la estructura ocupacional de la Secretaría;
[...]

XXIV. Expedir los nombramientos del personal de la Secretaría;

Artículo 36. Corresponde a la **Dirección General de Tecnologías de Información e Innovación**:

I. Proponer las medidas para apoyar el proceso de modernización mediante el uso de herramientas tecnológicas, simplificación y desconcentración de las funciones a cargo de la Secretaría, coadyuvando a incrementar la productividad y eficiencia en el trabajo;

II. Proponer, autorizar, emitir e instrumentar los planes, programas, estrategias, políticas y normas necesarias para encauzar la actividad de las áreas a su cargo, dentro de un margen de seguridad acorde con los estándares internacionales en el manejo de la información;

III. Vigilar los recursos de infraestructura de informática y telecomunicaciones en la Secretaría, así como supervisar y, en su caso, regular el uso adecuado y responsable de estos recursos por parte de los servidores públicos de la misma;

IV. Vigilar los recursos de informática y telecomunicaciones en las representaciones de México en el exterior, **así como regular el uso adecuado y responsable de estos recursos por parte del personal de las mismas;**

V. Desarrollar y, en su caso, coordinar y **apoyar técnicamente las tareas de diseño, construcción, implantación y operación de los sistemas y aplicaciones de informática y telecomunicaciones que requieran las áreas de la Secretaría;**

VI. Desarrollar, promover y coordinar los programas de capacitación necesarios para el mejor uso y aprovechamiento de los recursos informáticos y de telecomunicaciones, así como brindar la asistencia técnica y asesoría necesarias a las áreas usuarias;

VII. Representar y promover a la Secretaría en los eventos relacionados con la informática y las telecomunicaciones en el país y en el extranjero;

VIII. Realizar la investigación continua del avance tecnológico en materia de informática y telecomunicaciones;

IX. Coordinar los servicios de seguridad y de vigilancia de los bienes muebles e inmuebles, de las personas en éstos, del control del flujo de individuos y de bienes, informáticos y de telecomunicaciones, de la Secretaría;
[...]

XV. Coordinar y emitir la comunicación con las diversas instituciones de **seguridad nacional** y aquellas internacionales que soliciten información **sobre las bases de datos de los distintos sistemas informáticos de la Secretaría;**

> XVI. Coordinar con las unidades administrativas competentes **la celebración de contratos, convenios y demás instrumentos jurídicos en materia de su competencia, con organismos y entidades tanto públicos como privados, nacionales o internacionales**, y [...]

De conformidad con la normativa analizada se advierte que la Secretaría de Relaciones Exteriores tiene como misión **conducir la política exterior de México** mediante el diálogo, la cooperación, la promoción del país y la atención a los mexicanos en el extranjero, así como coordinar la actuación internacional del Gobierno de la República.

En ese sentido, al frente de la Secretaría de Relaciones Exteriores habrá un Secretario del Despacho, titular de la misma quien, para el desahogo de los asuntos de su competencia, se auxiliará de diversas unidades administrativas de entre las que se encuentran la **Oficialía Mayor** y la **Dirección General de Tecnologías de Información e Innovación**, mismas que cuentan con las atribuciones siguientes, de conformidad con la materia de la solicitud de información que nos ocupa:

- La **Oficialía Mayor**, se encarga, entre otras cosas de dirigir las políticas, normas, sistemas y procedimientos administrativos para la organización y funcionamiento de la Secretaría y para la gestión de los recursos humanos, financieros, materiales, informáticos y que correspondan a las unidades administrativas; dirigir las relaciones laborales, así como promover la capacitación y actualización y darle seguimiento a su observancia; y expedir los nombramientos del personal de la Secretaria.

- La **Dirección General de Tecnologías de Información e Innovación**, se encarga de proponer las para apoyar el proceso de modernización mediante el uso de herramientas tecnológicas, simplificación y desconcentración de las funciones a cargo de la Secretaría, coadyuvando a incrementar la productividad y eficiencia en el trabajo; proponer, autorizar, emitir e instrumentar los planes, programas, estrategias, políticas y normas necesarias para encauzar la actividad de las áreas a su cargo; vigilar los recursos de infraestructura de informática y telecomunicaciones en la Secretaría, así como supervisar, y en su caso, regular el uso adecuado y responsable de estos recursos por parte de los servidores

> públicos; vigilar los recursos de informática y telecomunicaciones en las representaciones de México en el exterior, así como regular el uso adecuado y responsable de estos recursos por parte del personal; apoyar técnicamente las tareas de diseño, construcción, implantación y operación de los sistemas y aplicaciones de informática y telecomunicaciones que requieran las áreas de la Secretaría, desarrollar, promover y coordinar los programas de capacitación necesarios para el mejor uso y aprovechamiento de los recursos informáticos y de telecomunicaciones, así como brindar asistencia técnica y asesoría necesarias; representar y promover a la Secretaría en los eventos relacionados con la informática y las telecomunicaciones; coordinar los servicios de seguridad y de vigilancia de los bienes muebles e inmuebles de las personas en éstos, de control de flujo de individuos y de bienes informáticos y de telecomunicaciones; coordinar con diversas instituciones de seguridad nacional que soliciten información sobre bases de datos de los distintos sistemas informáticos de la Secretaría; coordinar la celebración de contratos, convenios y demás instrumentos jurídicos en materia de su competencia con organismos tanto públicos como privados, nacionales o internacionales entre otras.

Con base en la normativa analizada, se tiene que el sujeto obligado **no** cumplió con el procedimiento de búsqueda previsto en la Ley Federal de Transparencia y Acceso a la Información Pública, toda vez que **no turnó** el requerimiento de información a la totalidad de las unidades administrativas competentes, quienes, de conformidad con lo señalado previamente, cuentan con atribuciones para conocer de lo requerido.

Lo anterior, en virtud de que el sujeto obligado turnó el requerimiento de información únicamente a la **Dirección General de Tecnologías de Información e Innovación,** área competente para conocer de lo requerido, quien entre sus atribuciones se encuentran las siguientes:

- Apoyar el proceso de modernización mediante el uso de herramientas tecnológicas, simplificación y desconcentración de las funciones a cargo de la Secretaría.

- Vigilar los recursos de infraestructura de informática y telecomunicaciones en la Secretaría, así como supervisar, y en su caso, regular el uso adecuado y responsable de estos recursos por parte de los servidores públicos.
- Vigilar los recursos de informática y telecomunicaciones en las representaciones de México en el exterior.
- Apoyar técnicamente las tareas de diseño, construcción, implantación y operación de los sistemas y aplicaciones de informática y telecomunicaciones que requieran las áreas de la Secretaría.
- Coordinar la celebración de contratos, convenios y demás instrumentos jurídicos en materia de su competencia con organismos tanto públicos como privados, nacionales o internacionales.

No obstante lo anterior, y en virtud de que el requerimiento de información **se relaciona con la identificación de personal y el tipo de contratación, cargo, comisión o servicio**, se advierte que la Secretaria de Relaciones Exteriores cuenta con un área específica encargada de conocer sobre la materia de la solicitud, sin embargo, no se turnó el requerimiento de información, siendo esta la **Oficialía Mayor**, ya que entre sus atribuciones se encuentran las siguientes:

- Dirigir las políticas, normas, sistemas y procedimientos administrativos para la organización y funcionamiento de la Secretaría y para la gestión de los recursos humanos
- Dirigir las relaciones laborales
- Expedir los nombramientos del personal de la Secretaría.

Ahora bien, en el caso en concreto, es necesario recordar que el particular requirió conocer lo siguiente:

a) Nombre de las personas físicas que cuentan con las contraseñas administrativas o su equivalente -permisos informáticos, credenciales administrativas, privilegios de súper usuario o su "root" para el manejo, administración y control de la configuración de cada equipo.

b) Tipo de contratación, empleo, cargo o comisión que desempeñan las personas que resulten del inciso anterior.

En respuesta, el sujeto obligado que los equipos de uso de la Secretaría son arrendados de ahí que se desconozca el nombre, cargo y comisión de las personas de interés del particular, ya que no existe una relación laboral con el personal que contratan los proveedores, situación que originó el medio de impugnación que nos ocupa, en virtud de que el particular manifestó que, si bien los equipos son arrendados, lo cierto es que el sujeto obligado tiene el uso y goce temporal de los equipos.

De esta manera, es preciso señalar que a partir de una lectura integral tanto a la solicitud de información como al recurso de revisión se advierte que la pretensión del particular va encaminada a conocer el nombre de las personas que cuentan con privilegios de administrador en los sistemas o con permisos informáticos en los equipos de la dependencia, así como el tipo de cargo o contratación que desempeñan.

En este sentido, resulta necesario citar lo que establecen las Normas para el otorgamiento y uso de servicios que proporciona la Dirección General de Tecnologías de la Información y la Innovación.

> "**VIII.7 SEGURIDAD INFORMÁTICA**
>
> El servicio de seguridad informática, es de gran relevancia, ya que es la suma de acciones de quienes utilizan cualquier herramienta de tecnologías de información y comunicación, y el personal especializado de la DGTII, para vigilar los mecanismos que permitan la administración de la Seguridad de la Información de la institución, esto es, minimizar el impacto de eventos adversos, así como implantar y operar los controles de seguridad.
>
> Por cuestiones de seguridad, para estar en posibilidades de conocer las normas que regularán este servicio, deberá remitirse al documento denominado "Lineamientos para la Seguridad Tecnológica y el S.G.S.I (Sistema de Gestión de Seguridad de la Información)"
> [...]

Por su parte, los Lineamientos en materia de Seguridad Informática, establecen lo siguiente:

> **I.- INTRODUCCIÓN.**
> Con el propósito de mejorar los niveles de seguridad tanto del personal de la DGTII y de los recursos informáticos de la Secretaría de Relaciones Exteriores, se establecen los presentes Lineamientos en Materia de Seguridad Informática, que se detallan en el presente documento.
> [...]

III.- SUJETOS DE LINEAMIENTO.

Los presentes lineamientos son de observancia general y obligatoria para todas las áreas de la Dirección General de Tecnologías de Información e Innovación (DGTII) y el personal adscrito a las mismas. La inobservancia, en lo conducente, de los presentes lineamientos será causal de las responsabilidades administrativas, civiles o penales que correspondan
[...]

A. ACCESO FISICO

1. El centro de Datos de la SRE es considerada un área de acceso restringido exclusivo a personal que por sus funciones requiera acceso al mismo. Será responsabilidad de la Dirección Adjunta de Operación de Tecnologías de la Información (DGAOTI), a través de la Dirección de Infraestructura y Telecomunicaciones (DIT) establecer un control de acceso físico al interior del centro de Datos de la SRE, así como llevar el registro de visitas como evidencia del cumplimiento del lineamiento.

2. Las áreas donde se localizan las plantas eléctricas, equipamiento de telecomunicaciones, UPS's y tableros eléctricos son también consideradas áreas de acceso restringido. Será responsabilidad de la Dirección Adjunta de Operación de Tecnologías de la Información (DGAOTI), a través de la Dirección de Infraestructura y Telecomunicaciones (DIT) establecer un control de acceso físico al interior de las mismas.
[...]

B. ACCESO LÓGICO

1. Para hacer uso de los recursos informáticos disponibles en la SRE, un sujeto deberá realizar el acceso a los sistemas a través de una cuenta única de usuario, existiendo una relación única entre el sujeto y su cuenta, esto a fin de autenticar al sujeto, la DGAOTI será la responsable de administrar el sistema de control de accesos lógico.

2. Se debe establecer los mecanismos para la protección y los derechos de acceso a los recursos (sistemas informáticos y Datos) con el fin de controlar el acceso de sujetos (Programas, procesos o usuarios), así como la utilización de los mismos, garantizando la confidencialidad e integridad de dichos recursos.

3. No deberán existir cuentas de usuarios genéricas (usuarios agrupados bajo una sola contraseña compartida) para el uso de recursos.

4. Para los recursos informáticos como servicio de internet, su uso es exclusivo para temas laborales o de índole diplomático quedando prohibido por seguridad su uso para accesos de temas que fomenten la discriminación, pornografía y sitios catalogados con contenido de tipo malicioso (malware).

5. El resguardo de la contraseña ligada a una cuenta de usuario, es responsabilidad de la persona asignada a la misma, por lo cual, no se podrá revelar ni compartir la contraseña a un tercero.

6. Las contraseñas no podrán exhibirse en forma alguna, ni resguardarles en archivos sin encriptar, a fin de evitar que un sujeto externo o ajeno pueda acceder a ella.
[...]

9. El resguardo de contraseñas vinculadas a cuentas especiales será responsabilidad de la Dirección General Adjunta de Seguridad Tecnológica (DGAST) y proporcionará dicha contraseña en función a criterios establecidos a los usuarios de la misma (sujetos).

10. Los accesos lógicos serán realizados a través de los equipos que la Dirección de Servicios Informáticos (DSI) asigne para este fin, así mismo, la DSI establecerá los lineamientos necesarios para regular el uso de los equipos, el soporte que se preste a todos los recursos informáticos y que garantice la integridad de la información contenida en los mismos.
[...]

c. AUTENTICACIÓN
[...]

2. La Dirección General Adjunta de Arquitectura y Diseño de Tecnologías de Información (DGAADTI) a través de sus Direcciones de Arquitectura Aplicativa (DAA) y Arquitectura de Sistemas (DAS) garantizarán que todo el software desarrollado tenga control de acceso lógico a través de un método de autenticación

3. El proceso de validación deberá minimizar las falsas aceptaciones o entradas no autorizadas a los sistemas, así como los falsos rechazos, esto mediante la utilización de mecanismos autenticación (contraseña, credenciales, etc.) para lograr el acceso a los sistemas.

4. Para verificar la identidad del sujeto y por lo tanto ganar el acceso a los recursos como sujeto autorizada, deberá existir una cuenta única de usuario vinculada al sujeto, es decir, existirá una relación única entre la persona y su cuenta.
[...]

d. AUTORIZACIÓN E INTEGRIDAD
1. Para la utilización de los recursos por parte de los usuarios, se debe establecer diferentes niveles de autorización (privilegio) con el objeto de poder realizar operaciones sobre los recursos con derecho de acceso.

2. Cada usuario deberá tener el mínimo de privilegios requeridos a fin de realizar sus funciones de acuerdo a su perfil establecido, bajo los siguientes lineamientos:

- Para poder realizar las funciones asignadas se procurará satisfacer las propiedades del perfil de acuerdo a los derechos de acceso requeridas para la misma.

- La opción por omisión o no expresar el acceso a algo, significa todo está restringido, a menos que este expresamente permitido el acceso al recurso.

- Minimizar el uso de recursos compartidos.

D. CONFIDENCIALIDAD

1. Todos los funcionarios, personal de honorarios, becarios o proveedores adscritos a la DGTII deberán firmar una responsiva de confidencialidad donde se comprometan a mantener de manera confidencial la información que tienen a su cargo.

2. No está permitido hacer referencia a temas o información oficial y confidenciales de la SRE en público o la distribución de mismos por medio de cualquier dispositivo o canal de comunicación no controlados por la DGTII
[...]

F. PROVEEDORES EXTERNOS
[...]

2. Todos los contratos con proveedores externos deberán contener cláusulas de confidencialidad que obliguen al personal en sitio el mantener la confidencialidad, integridad y disponibilidad de la información al interior de la SRE.

3. Todos los contratos con proveedores externos deberán contener una cláusula que garantice que el personal asignado a la Secretaría ha sido sometido a análisis de confianza que indiquen que dicho personal no tiene antecedentes penales o que su perfil psicométrico lo vuelve apto para desempeñar las funciones conferidas.
[...]

H. DESARROLLO DE SOFTWARE

1. La Dirección General Adjunta de Arquitectura y Diseño de Tecnologías de Información (DGAADTI) a través de sus Direcciones de Arquitectura Aplicativa (DAA) y Arquitectura de Sistemas (DAS) será las únicas áreas al interior de la Secretaría que podrán desarrollar software.

2. El desarrollo de software deberá llevarse a cabo en apego a mejores prácticas de programación que garanticen que la codificación se hace bajo estándares de seguridad adecuados.

3. La DGAADTI será la responsable de garantizar que los programas que son puestos en producción en equipos a cargo de la DGTII, hayan sido revisado en búsqueda de vulnerabilidades de código que pudieran ser explotadas de manera maliciosa y pudiesen afectar la integridad o confidencialidad de la información.
[...]"

De conformidad con la normativa analizada, se tiene que la seguridad informática es de gran relevancia ya que es la suma de acciones de quienes utilizan cualquier herramienta tecnológica de información y comunicación para vigilar los mecanismos que permitan la administración de la seguridad de la información de la institución.

Asimismo, se indica que **para hacer uso de los recursos informáticos disponibles en la Secretaría, un sujeto deberá realizar el acceso a los sistemas a través de una cuenta única de usuario, existiendo una relación única entre sujeto y su cuenta**, esto a fin de autenticar al sujeto, la Dirección Adjunta de Operación de Tecnologías de la Información (DGAOTI), será la responsable de administrar el sistema de control de acceso lógico.

Al respecto, **se precisa que no deberán existir cuentas de usuarios genéricas**, para los recursos informáticos como servicios de internet, su uso es exclusivo para temas laborales o de índole diplomáticos quedando prohibido por seguridad el uso para acceso de temas que fomentes la discriminación, pornografía y sitios catalogados con contenidos de tipo maliciosos (malweare). Así, **el resguardo de la contraseña es responsabilidad de la persona asignada a la misma**, las contraseñas no podrán exhibirse en forma alguna, en resguardarse en archivos sin encriptar.

Así, para la utilización de los recursos por parte de los usuarios, se debe establecer **diferentes niveles de autorización (privilegio) con el objeto de poder realizar operaciones sobre los recursos con derecho de acceso**. Cada usuario deberá tener el mínimo de privilegios requeridos **a fin de realizar sus funciones de acuerdo a su perfil establecido**.

Asimismo, se indica que las cuentas especiales será responsabilidad de la Dirección General Adjunta de Seguridad Tecnológica (DGAST) y proporcionará dicha contraseña en función de criterios establecidos a los usuarios. Los accesos lógicos serán realizados a través de los equipos que la Dirección de Servicios Informáticos (DSI) asigne para este fin, de la misma manera, la DSI establecerá los lineamientos necesarios para regular el uso de los equipos, el soporte que se preste a todos los recursos informáticos y que garantice la integridad de la información contenida en los mismos.

La **Dirección General Adjunta de Arquitectura y Diseño de Tecnologías de Información (DGAADTI) a través de sus Direcciones de Arquitectura Aplicativa (DAA) y Arquitectura de Sistemas (DAS)** garantizarán que todo el software desarrollado tenga control de acceso lógico a través de un método de autenticación, y **serán las únicas áreas al interior de la Secretaría que podrán desarrollar software.** Particularmente, la Dirección General Adjunta de Arquitectura y Diseño de Tecnologías de Información **será la responsable de garantizar que los programas que son puestos en producción en equipos hayan sido revisados en búsqueda de vulnerabilidad e código que pudieran ser explotadas de manera maliciosa y pudiesen afectar la integridad o confidencialidad de la información.**

Con base en la normativa analizada, es posible señalar que **el sujeto obligado cuenta con personal al cual se le otorga una cuenta de usuario para hacer uso de los recursos informáticos de los que dispone la Secretaría**, para ello, **se establecen niveles de autorización (privilegio) con el objeto de poder realizar operaciones sobre los recursos con derecho de acceso** de cada usuario, se otorgará privilegios a fin de garantizar sus funciones de acuerdo al perfil establecido.

De la misma manera, se hace referencia a **cuentas especiales**, las cuales serán responsabilidad de la **Dirección General Adjunta de Seguridad Tecnológica (DGAST)**, quien proporcionará la contraseña en función de criterios establecidos a los usuarios.

Por otra parte, también se hace mención a que Dirección General Adjunta de Arquitectura y Diseño de Tecnologías de Información (DGAADTI) a través de sus Direcciones de Arquitectura Aplicativa (DAA) y Arquitectura de Sistemas (DAS) garantizarán que todo el software desarrollado tenga control de acceso lógico a través de un método de autenticación, y **serán las únicas áreas al interior de la Secretaría que podrán desarrollar software**, es decir, se puede entender que dichas áreas se les otorga privilegios para acceder y crear software específico.

Con base en lo anterior, es posible señalar que no atendió adecuadamente el requerimiento de información, toda vez que señaló que la información del nombre del personal con contraseñas asignadas y el tipo de contratación es inexistente, en virtud de

que los equipos son arrendados y es el proveedor quien cuenta con privilegios para acceder a ellos. No obstante, como se analizó **la Secretaría cuenta con personal a quien se le asignan contraseñan para el uso y resguardo de la información contenida en los equipos de cómputo del sujeto obligado, así como para la generación de software.**

Por otra parte, no se omite señalar que el particular manifestó que el sujeto obligado omitió notificarle el acta a través de la cual el sujeto obligado confirmó la inexistencia de la información solicitada. Al respecto, es de señalarse que con base en el análisis efectuado en el presente apartado, se advierte que no resulta procedente la inexistencia aludida por el sujeto obligado.

Asimismo, no se omite señalar que en el acta número CTA-21718, remitida en la respuesta inicial el Comité de Transparencia del sujeto obligado, manifestó respecto a los incisos a y b, que no cuenta con la información, en virtud de que los equipos de cómputo son arrendados. Es decir, en el acta señalada de manera inicial se analiza la inexistencia impugnada por el ahora recurrente, por tanto, no resulta procedente el señalamiento del particular.

Finalmente, es preciso recordar que el particular manifestó que la información debía existir porque corresponde a obligaciones de transparencia, previstas en la fracción VII del artículo 70 de la Ley General de Transparencia y Acceso a la Información Pública, la cual corresponde a la publicación del directorio de los servidores públicos a partir de jefe de departamento o su equivalente.

Al respecto, es de señalarse que **el particular no solicitó la información del registro de servidores públicos, sino requirió conocer de manera precisa el nombre de los servidores públicos de ese sujeto obligado que cuentan con las contraseñas administrativas o su equivalente** (permisos informáticos, credenciales administrativas, privilegios de superusuario "su", "root", etc.) para el manejo, administración y control de la configuración de cada equipo, el tipo de contratación, empleo, cargo o comisión que desempeñan las personas que sean señaladas.

Es decir, **contrario a lo manifestado por el particular en su recurso de revisión, éste no solicitó conocer de manera genérica el directorio de los servidores públicos con los que cuenta el sujeto obligado, pues requirió información específica y precisa para conocer información en relación a cada servidor público con actividades específicas en materia de seguridad informática dentro del sujeto obligado,** información que no se encuentra señalada como una obligación de transparencia en el artículo 70 de la Ley General de Transparencia y Acceso a la Información Pública.

- **Análisis de clasificación.**

Al respecto, la Ley Federal de Transparencia y Acceso a la Información Pública establece lo siguiente:

> "**Artículo 110.** Conforme a lo dispuesto por el artículo 113 de la Ley General, como información reservada podrá clasificarse aquella cuya publicación:
>
> I. **Comprometa la seguridad nacional**, la seguridad pública o la defensa nacional y **cuente con un propósito genuino y un efecto demostrable**;
> [...]
>
> XIII. **Las que por disposición expresa de una ley tengan tal carácter**, siempre que **sean acordes con las bases, principios y disposiciones establecidos en la Ley General** y **esta Ley** y **no las contravengan**; así como las previstas en tratados internacionales."

De los preceptos normativos referidos, es posible desprender que:

- Podrá clasificarse como reservada aquella información cuya divulgación comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino o un efecto demostrable.

- Podrá clasificarse como información reservada, aquella que por disposición expresa de una ley tenga ese carácter, siempre que sea acorde con las bases, principios y disposiciones establecidos en la ley General y Federal de transparencia, así como las previstas en tratados internacionales, sin contravenirlas.

Así, debe ser considerado el último párrafo del Décimo Séptimo de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, en adelante Lineamientos Generales, que a la letra dice:

> "**Décimo séptimo.** De conformidad con el artículo 113, fracción I de la Ley General, podrá considerarse como información reservada, aquella que de difundirse actualice o potencialice un riesgo o amenaza a la seguridad nacional cuando:
> [...]
>
> Asimismo, podrá considerarse como reservada aquella que revele datos que pudieran ser aprovechados para conocer la capacidad de reacción de las instituciones encargadas de la seguridad nacional; sus normas, procedimientos, métodos, fuentes, especificaciones técnicas, tecnología o equipo útiles a la generación de inteligencia para la Seguridad Nacional, sin importar la naturaleza o el origen de los documentos que la consignen."

Como se observa, en el Lineamiento de referencia se dispone que podrá reservarse aquella información que de difundirse actualice o potencialice un riesgo o amenaza a la seguridad nacional cuando se revelen datos que pueden ser aprovechados para conocer la capacidad de reacción de las instituciones encargadas de la seguridad nacional.

Ahora bien, con el fin de acreditar o verificar si se actualizan las dos causales invocadas por la autoridad recurrida, es necesario, en primer lugar, determinar la naturaleza de la información que se requiere, de conformidad con la normatividad aplicable a la autoridad recurrida.

En el caso concreto, resulta necesario recordar que la Secretaría de Relaciones Exteriores tiene como misión **conducir la política exterior de México** mediante el diálogo, la cooperación, la promoción del país y la atención a los mexicanos en el extranjero, así como coordinar la actuación internacional del Gobierno de la República.

En este sentido, es preciso señalar que que el artículo 3, fracciones I y III de la Ley de Seguridad Nacional, dispone que se entienden como acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano, entre otras, las siguientes:

a) La protección de la nación mexicana frente a las **amenazas** y riesgos que enfrente nuestro país, y

b) El mantenimiento del orden constitucional y el fortalecimiento de las instituciones democráticas de gobierno.

Asimismo, el artículo 5, fracciones I y XII de la Ley en comento, señala que se considera como **amenaza a la seguridad nacional** aquellos actos tendentes a consumar espionaje, **sabotaje,** terrorismo, rebelión, traición a la patria, genocidio, en contra de los Estados Unidos Mexicanos dentro del territorio nacional; así como a destruir o **inhabilitar la infraestructura** de carácter estratégico o indispensable para la provisión de bienes o servicios públicos.

En concatenación con lo anterior, es preciso recordar que el artículo 12, fracción VIII, de la Ley de Seguridad Nacional establece que el **Secretario de Relaciones Exteriores forma parte del Consejo de Seguridad Nacional**. Además, es importante retomar lo establecido en la Primera de las Bases de Colaboración que, en el marco de la Ley de Seguridad Nacional, celebran el Titular de la Secretaría de Gobernación, en su carácter de Secretario Ejecutivo del Consejo de Seguridad Nacional, y la Titular de la Secretaría de Relaciones Exteriores -en lo sucesivo Bases de Colaboración- publicadas en el Diario Oficial de la Federación el veintisiete de mayo de dos mil ocho, a saber:

> "**PRIMERA.** -A fin de consolidar la acción del Estado en materia de Seguridad Nacional, las partes se comprometen a:
>
> **IV.** Establecer los mecanismos que permitan el **intercambio de información** contenida en las bases de datos que en razón de sus atribuciones administren las partes, a fin de apoyar el desarrollo de las actividades de inteligencia y contrainteligencia que las instancias integrantes del Consejo de Seguridad Nacional realicen para investigar las siguientes amenazas a la Seguridad Nacional:
> [...]
>
> **VI. Contar con la infraestructura y mecanismos que se requieran para que la transmisión y flujo de información salvaguarde las condiciones de reserva y confidencialidad que demandan** los temas de Seguridad Nacional, y de conformidad con lo establecido en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, y
> [...]"

Como se observa, la Secretaria de Relaciones Exteriores, **al formar parte del Consejo de Seguridad Nacional**, cuenta **con mecanismos de intercambio de información con el resto de integrantes de tal Consejo**, con la finalidad de apoyar y desarrollar actividades de inteligencia y contrainteligencia; además, dicha dependencia está comprometida a contar con infraestructura y mecanismos necesarios para salvaguardar la información intercambiada en materia de seguridad nacional.

Adicionalmente, conforme a lo establecido en los puntos III.3 y III.4 de las multicitadas Bases de Colaboración, **se consideran como instancias de seguridad nacional de la Secretaría de Relaciones Exteriores las siguientes**: **la Dirección General de Delegaciones**, **Dirección General de Protección y Asuntos Consulares**, y **la Dirección General de Asuntos Jurídicos** y, en esa calidad, tienen la obligación de establecer en conjunto con el Secretario Ejecutivo, una Red Nacional de Información de Seguridad Nacional, mediante la aportación de las bases de datos que en función de sus atribuciones tengan a su cargo.

En este entendido, si bien no todas las Unidades Administrativas que forman parte de la Secretaría de Relaciones Exteriores revisten la calidad de Instancia de Seguridad Nacional, lo cierto es que tiene la obligación de resguardar la información intercambiada en materia de seguridad nacional.

En relación con lo anterior, es necesario recodar que el particular solicitó respecto de cada uno de los equipos de cómputo y de cada uno de los MODEMS, ROUTERS (rúters) o puntos de acceso inalámbricos en posesión del sujeto obligado, y ordenado por **número de serie,** entre otra información, la **forma en que cada equipo obtiene o asigna, según sea el caso, la dirección IP**, es decir, si es forma manual o por medio del Protocolo de Configuración Dinámica Host DHCP.

Al respecto, el sujeto obligado señaló como prueba de daño lo siguiente:

- La **divulgación de la información que se reserva representa un riesgo real, demostrable e identificable de perjuicio significativo a los intereses del gobierno mexicano**. -La información reservada consistente en los números de serie y la forma en como se le asigna la IP, información que se considera sensible

en virtud de que dan cuenta de los equipos y tecnología empleadas por las Unidades Administrativas de esta Secretaría. En consecuencia, es información reservada, ya que da cuenta de las características técnicas de la infraestructura contratada, la cual soporta los sistemas centrales que contienen bases de datos e información, lo que podría ser aprovechada por terceros con conocimientos técnicos para detectar puntas de vulnerabilidad en la infraestructura informática de la Secretaría de Relaciones Exteriores, conocer su capacidad de reacción en materia de seguridad informática, cuestión que potenciaría actos de sabotaje, monitoreo y/o control de los equipos de cómputo.

- El **riesgo de perjuicio supera el interés público general de que se difunda**. - La divulgación de las características de los dispositivos solicitados permitiría conocer los mecanismos que sigue esta Secretaría para los servicios de red, a través de los cuales puede viajar información sensible y dan conectividad a equipos de cómputo.

- La **limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio**. - La limitación del derecho del solicitante a conocer la información que se reservan es proporcional al bien jurídico que se tutela como lo es la seguridad nacional; además, dicha reserva constituye una medida de restricción temporal de la información, la cual no es excesiva, máxime que, el derecho a buscar y recibir información, si bien es un derecho fundamental, no es absoluto y puede ser limitado siempre y cuando: i) el fin sea constitucionalmente válido (fin legítimo); ii) la medida sea idónea para alcanzar el fin constitucionalmente válido; iii) no exista un medio menos lesivo; y, iv) la limitación sea proporcional en sentido estricto; como en este caso ocurre.

En este sentido, se comparte la idea de que los números de serie o de parte, así como la forma en que cada equipo obtiene o se le designa la dirección IP, privada, es información que compromete la seguridad nacional y revela especificaciones técnicas de equipos utilizados para la generación de información sensible, la cual al ser divulgada permitiría el **sabotaje, monitoreo y/o control** de los equipos de las unidades administrativas integrantes de la Secretaria de Relaciones Exteriores.

Además, la publicidad de la información no sólo pondría en riesgo las bases de datos y las operaciones de esa Secretaría, sino que también implicaría afectaciones en los diversos trámites y servicios que presta a la ciudadanía general.

En este sentido, se comparte el posicionamiento de la autoridad recurrida en relación a que existen elementos suficientes para considerar que, si se difunden la información solicitada se puede actualizar o potencializar un riesgo o amenaza de seguridad nacional porque la revelación de los datos pueden ser aprovechados por terceros con conocimientos técnicos para detectar puntos de vulnerabilidad en su infraestructura informática, conocer su capacidad de reacción en materia de seguridad informática y, en su caso, potenciar un ataque a tales equipos que ponga en riesgo las bases de datos contenidas en tales equipos, incluida aquella que se intercambia en el marco del Consejo de Seguridad Nacional y de las propias unidades administrativas de la dependencia catalogadas como instancias de seguridad nacional.

Además, es evidente que las características solicitadas por el particular de los equipos de cómputo de interés, forman parte de un conjunto de medidas de seguridad en materia informática de la Secretaría de Relaciones Exteriores, pues como se ha señalado, existen personas con los conocimientos necesarios que, a partir de la obtención de estos elementos, podrían desarrollar algún malware por sí o a través de terceros, que lo vincule con todos o la mayoría de sus equipos de cómputo, en el que se vería afectado el desempeño de sus funciones, ocasionar pérdida de la información, o inclusive, podría paralizarlas mediante ataques cibernéticos, lo cual comprometería sus atribuciones en el apoyo del desarrollo de las actividades de inteligencia y contrainteligencia que las instancias integrantes del Consejo de Seguridad Nacional realicen para investigar las amenazas a la Seguridad Nacional.

Robustece nuestro dicho, **las opiniones emitidas por el Titular de la Dirección General de Tecnologías de Información de este Instituto**, al cual se le requirió opinión mediante el oficio **número INAI/JSS/047/18** y el diverso **INAI/MPKV/242/2018**, quien, con los conocimientos precisos en la materia refirió que, a través de un equipo de cómputo conectado a una red, **es posible que se le permita a algún potencial atacante cibernético dirigir algún ataque informático, como lo es suplantación de identidad con usos maliciosos (Spoofing), interceptar, modificar o incluso retener datos que**

están en tránsito (ARP Spoofing), o un "ataque de fuerza bruta" el cual consiste en recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso al equipo. Asimismo, manifestó lo siguiente:

> "Por otro lado, se debe tomar en cuenta los siguientes aspectos en la gestión del riesgo y la toma de medidas preventivas en materia de seguridad de la información:
>
> • Los elementos que integran la plataforma tecnológica de una organización y que son los que soportan a los activos de información no son entes aislados, poseen una interrelación con el resto de equipos y dispositivos dentro de la red de datos y la información que por esta se transmite o almacena.
>
> • **Brindar información no necesaria a posibles atacantes que pudieran aprovecharse de posibles vulnerabilidades**, incluso aquellas desconocidas por el propio fabricante (vulnerabilidades de día O) de los dispositivos informáticos a nivel granular o periférico (tarjetas de red, procesadores, etc.) o vistos como componentes (equipos de cómputo, servidores, bases de datos, aplicaciones, módulos de almacenamiento, etc.).
>
> **Mediante un equipo de cómputo conectado en red y a través de la dirección IP, es un dato que permite identificar el equipo del usuario cuando accede a Internet o bien dentro de una red de datos de área local**, información con la cual podrían conocerse las decisiones que adopta en su navegación en Internet o de acceso a servicios informáticos internos, la publicidad de ésta podría ser información que vulnere la seguridad y de esta manera afectar la infraestructura de cómputo.
>
> Por lo anterior, podemos afirmar que, si un equipo de cómputo ha sido vulnerado por un atacante, la seguridad de otros equipos conectados a la misma red pudiese verse comprometida.
> [...]"

Es decir, la información que se requiere, contempla información sensible como: **números de serie, identificación de la IP**, dirección MAC, Sistema Operativo, entre otra, cuya divulgación provocaría, entre otros, los siguientes riesgos:

- Cualquier persona en posesión de la misma podría acceder a la información de los equipos (PCs) en uso en la Secretaría.
- Acceder a los equipos se podría buscar alguna vulnerabilidad de seguridad en la red de computadoras de la Secretaría y acceder a la información contenida en los sistemas de procesamiento y almacenamiento de información de la dependencia.

- Lanzar ataques cibernéticos desde alguno o algunos de los equipos de la red de computadoras de la Secretaría.
- Introducir algún tipo de malware a la red de computadoras de la Secretaría.
- Infectar el portal web de la Secretaría.
- Paralizar las actividades de la red de computadoras de la Secretaría.

Por otra parte, no se omite señalar que, a través de su oficio de alegatos la Secretaría, hizo de conocimiento a este Instituto, diversos casos de ataques cibernéticos sufridos en distintas Secretarías de la administración pública, así como en las instancias administrativas, en los que se ha visto afectadas las funciones que desempeñan y se ha filtrado información de carácter confidencial, en razón, precisamente, de conocer los datos que hoy se pretenden conseguir.

En rezón de lo anterior, se estima procedente la reserva de la información solicitada, esto es, respecto de cada uno de los equipos de cómputo y de cada uno de los MODEMS, ROUTERS (rúters) o puntos de acceso inalámbricos en posesión del sujeto obligado, y ordenado **por número de serie,** entre otra información, la **forma en que cada equipo obtiene o asigna, según sea el caso, la dirección IP**, con fundamento en la fracción I del artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública.

Finalmente, no se omite señalar que el particular manifestó que el sujeto obligado omitió notificar el acta a través de la cual el Comité de Transparencia del sujeto obligado confirmó la reserva de la información requerida. No obstante, con base en las constancias que integran el expediente en que se actúa se advierte que desde la respuesta inicial la dependencia remitió como parte de su respuesta el acta número CTA-21718, a través de la cual el Comité de Transparencia resolvió confirmar la reserva de la información con fundamento en la fracción I del artículo 110 de la Ley en la materia, por tanto, no resulta procedente la manifestación del particular.

En consecuencia, se determina como **parcialmente fundado** el agravio de la ahora recurrente.

En razón de lo anterior, y de conformidad con lo dispuesto en el artículo 157, fracción III de la Ley Federal de Transparencia y Acceso a la Información Pública, este Instituto

determina que lo procedente para el caso que nos ocupa es **MODIFICAR** la respuesta de la Secretaría de Relaciones Exteriores, a efecto de que:

- Realizar una nueva búsqueda de la información requerida, correspondiente **incisos a y b**, esto es, el nombre da las personas que cuentan con las contraseñas administrativas o su equivalente -permisos informáticos, credenciales administrativas, privilegios de súper usuario o su "root" para el manejo, administración y control de la configuración de cada equipo; y **el tipo de contratación, empleo, cargo o comisión que desempeñan;** turnado a todas las unidades administrativas entre las que no deberá omitir **Dirección General de Tecnologías de Información e Innovación,** y sus unidades administrativas adscritas que resulten competentes, así como, la **Oficialía Mayor** e informe el resultado de la búsqueda.

  De localizar dicha información deberá conceder su acceso, o bien, si determina que tiene el carácter de acceso restringido, deberá clasificarla siguiendo el procedimiento establecido en el artículo 140 de la Ley Federal de Transparencia y Acceso a la Información Pública.

En este sentido y toda vez que ya no es posible atender la solicitud en la modalidad elegida por la particular, a saber "Entrega por internet en el INFOMEX", el sujeto obligado deberá entregar la información requerida, por medio del correo electrónico señalado para tales efectos, o ponerla a su disposición en un sitio de internet, y comunicarle los datos que le permitan acceder a la misma. Lo anterior, de conformidad con lo establecido en la Ley Federal de Transparencia y Acceso a la Información Pública.

Por lo expuesto y fundado, el Pleno:

RESUELVE

PRIMERO. MODIFICAR la respuesta emitida por el sujeto obligado, de acuerdo a la presente resolución.

SEGUNDO. Instruir al sujeto obligado para que, cumpla con lo ordenado en la presente resolución, **en un plazo máximo de diez días hábiles**, contados a partir del día hábil

siguiente a aquel en que se haya notificado; asimismo, en un término no mayor a los tres días después de transcurrido dicho plazo para su cumplimiento, lo informe a este Instituto de conformidad al último párrafo del artículo 159 de la ley federal de la materia.

TERCERO. En caso de incumplimiento, parcial o total, de la resolución dentro del plazo ordenado, este Instituto procederá de conformidad con lo dispuesto en el Título Sexto de la Ley Federal de Transparencia y Acceso a la Información Pública.

CUARTO. Instruir a la Secretaria Técnica del Pleno, para que, a través de la Dirección General de Cumplimientos y Responsabilidades de este Instituto, verifique que el sujeto obligado cumpla con la presente resolución y dé el seguimiento que corresponda.

QUINTO. Notificar a las partes y publicar la presente resolución de conformidad al primer párrafo del artículo 159 de la Ley Federal de Transparencia y Acceso a la Información Pública.

SEXTO. Se hace del conocimiento de la parte recurrente que, en caso de encontrarse insatisfecha con la presente resolución, le asiste el derecho de impugnarla ante el Poder Judicial de la Federación, con fundamento en el artículo 165 de la Ley Federal de Transparencia y Acceso a la Información Pública.

SÉPTIMO. Poner a disposición de la parte recurrente el número telefónico 01 800 TEL INAI (835 4324) y el correo electrónico vigilancia@inai.org.mx, para que comunique a este Instituto sobre cualquier incumplimiento a la presente resolución.

Así, por unanimidad, lo resolvieron y firman los Comisionados del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, Francisco Javier Acuña Llamas, Oscar Mauricio Guerra Ford, Blanca Lilia Ibarra Cadena, María Patricia Kurczyn Villalobos, Rosendoevgueni Monterrey Chepov y Carlos Alberto Bonnin Erales, siendo ponente el último de los mencionados, en sesión celebrada el veinticuatro de octubre de dos mil dieciocho, ante Hugo Alejandro Córdova Díaz, Secretario Técnico del Pleno.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Expediente: RRA 6073/18
Sujeto obligado: Secretaría de Relaciones Exteriores
Folio de la solicitud: 0000500130518
Comisionado Ponente: Carlos Alberto Bonnin Erales

Francisco Javier Acuña Llamas
Comisionado Presidente

Carlos Alberto Bonnin Erales
Comisionado

Oscar Mauricio Guerra Ford
Comisionado

Blanca Lilia Ibarra Cadena
Comisionada

María Patricia Kurczyn Villalobos
Comisionada

Rosendoevgueni Monterrey Chepov
Comisionado

Hugo Alejandro Córdova Díaz
Secretario Técnico del Pleno

Esta foja corresponde a la resolución del recurso de revisión **RRA 6073/18**, emitida por el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el **24 de octubre de 2018**.