



SEP
SECRETARÍA DE
EDUCACIÓN PÚBLICA

SESIÓN ORDINARIA

ACT/CT/SO/07/05/2019-R

Fecha:	07 de mayo de 2019	Lugar:	Donceles No. 100, Colonia Centro Histórico, Alcaldía Cuauhtémoc, Ciudad de México, C.P. 06020
--------	--------------------	--------	---

MIEMBROS DEL COMITÉ DE TRANSPARENCIA

Nombre	Unidad Administrativa	Firma
Lic. Salim Arturo Orci Magaña	Titular del Órgano Interno de Control en la Secretaría de Educación Pública.	
Lic. Mario Humberto Delgado González.	Responsable del Área Coordinadora de Archivos de la Secretaría de Educación Pública.	
Lic. Cuauhtémoc Rafael Montero Clavel	Director de Procesos Jurisdiccionales y suplente del Titular de la Unidad de Asuntos Jurídicos y Transparencia.	

ASUNTOS Y PUNTOS DE ACUERDO

Punto 1.-

ASUNTO QUE SE SOMETE A CONSIDERACIÓN: Confirmación de la clasificación de la información como reservada.

NÚMERO DE FOLIOS: 0001100766318



SEP

SECRETARÍA DE
EDUCACIÓN PÚBLICA

SESIÓN ORDINARIA

ACT/CT/SO/07/05/2019-R

NÚMERO DE RECURSO DE REVISIÓN: RRA 0561/19

ESTATUS DEL RECURSO DE REVISIÓN: Cumplimiento.

- I. **Solicitud de acceso a información pública**, misma que se describe a continuación:

“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 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. Por número de serie de cada uno de los equipos de cómputo en posesión del sujeto obligado requiero: a) Nombres comerciales de los sistemas operativos instalados. b) Nombres comerciales y versiones de los antivirus o software de seguridad en Internet, instalados. c) Inicio y término de la vigencia de cada licencia utilizada en los software mencionados en el anterior inciso b). 2. Por dirección web o URL (Localizador Uniforme de Recursos), de los protocolos HTTP (Protocolo de Transferencia de Hipertexto) y HTTPS (Protocolo seguro de transferencia de hipertexto), cual es utilizado en cada una de sus páginas electrónicas o webs oficiales, así como el tipo de protocolo de seguridad implementado, SSL (Capa de sockets seguros) o TLS (Seguridad de la capa de transporte). 3. De cada una de sus actuales páginas electrónicas o webs oficiales, fecha exacta y duración de todos los ataques de Denegación de Servicio (DoS) ó Denegación de Servicio Distribuida (DDoS) padecidos.” (SIC).

- II. La **Unidad de Transparencia** turnó la solicitud a la **Unidad de Administración y Finanzas (UAF)** y la **Dirección General de Tecnologías de la Información y Comunicaciones (DGTIC)**, quienes informaron lo siguiente:

“Siendo la respuesta de la Unidad de Administración y Finanzas (UAF) la siguiente:

“Al respecto, se hace de su conocimiento que la Dirección General de Tecnologías de la Información y Comunicaciones, en términos del artículo 38 del Reglamento Interior de la Secretaría de Educación Pública, es la Unidad Administrativa adscrita a la Unidad de Administración y Finanzas, responsable de dar atención a la solicitud planteada” (SIC)

Respondiendo la Dirección General de Tecnologías de la Información y Comunicaciones (DGTIC) lo subsecuente:

“Con la finalidad de dar atención a dicha solicitud de información, a continuación, se responden los siguientes puntos:



1.- Por número de serie de cada uno de los equipos de cómputo en posesión del sujeto obligado requerido, se adjunta archivo en formato PDF.

a. Nombre comercial de los sistemas operativos instalados.

Cada uno de los equipos en posesión de la Dirección General de Tecnologías de la Información y Comunicaciones, cuenta con los siguientes sistemas operativos instalados.

- Windows 10 Enterprise
- MacOS High Sierra 10.13.

b. Nombres comerciales y versiones de los antivirus o software de seguridad en Internet, instalados.

- Windows Defender

c. Inicio y término de la vigencia de cada licencia utilizada en los softwares mencionados en el anterior inciso b).

- Vigencia del 2018 - 2020

1. Por dirección web o URL (Localizador Uniforme de Recursos), de los protocolos HTTP (Protocolo seguro de transferencia de hipertexto), cual es utilizado en cada una de sus paginas electrónicas o webs oficiales, así como el tipo de protocolo de seguridad implementado, SSL (Capa de sockets seguros) o TLS (Seguridad de la capa de transporte).

https://cedulaprofesional.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://cofedet.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://conapase.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://dgpvrf.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://e5cinco.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://interlocucioncondocentes.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://iena.sep.gob.mx/iena/	Capa de Sockets Seguros (SSL).
https://nistsirepve.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://portalaautoservicios.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://portalaautoservicios-df.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://portalaautoservicios-sems.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://registromodeloeducativo.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://renapo.sep.gob.mx/wsrenapo/	Capa de Sockets Seguros (SSL).
https://renapoprue.sep.gob.mx/wsrenapo/	Capa de Sockets Seguros (SSL).
https://sajja.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://seguridadweb.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://siapsepweb.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://siapsepweb-inehrm.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://siapsepweb-sems.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://siapsepweb-tnm.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://sicd1819.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://sidepaae.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://siho.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://sirep.sep.gob.mx	Capa de Sockets Seguros (SSL).



https://sirepve.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://sirvoes.sep.gob.mx/sirvoes	Capa de Sockets Seguros (SSL).
https://sise.sep.gob.mx/	Capa de Sockets Seguros (SSL).
https://sisrvoe.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://ssien.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://uaiyt.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://webdgrms.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://www.acosoescolar.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://www.cenni.sep.gob.mx/	Capa de Sockets Seguros (SSL).
https://www.citas.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://www.dgair.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://www.modeloeducativo.sep.gob.mx/	Capa de Sockets Seguros (SSL).
https://www.msirepve.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://www.murales.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://www.portalautoservicios-tnm.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://www.profesiones.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://www.repase.sep.gob.mx/	Capa de Sockets Seguros (SSL).
https://www.repase3.sep.gob.mx/	Capa de Sockets Seguros (SSL).
https://www.sas.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://www.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://www.siree.sep.gob.mx	Capa de Sockets Seguros (SSL).
https://www.sirsa.sep.gob.mx	Capa de Sockets Seguros (SSL).
www.normatecainterna.sep.gob.mx	Capa de Sockets Seguros (SSL).
www.programaveranosep-snte.sep.gob.mx	Capa de Sockets Seguros (SSL).
www.vestuariosep-snte.sep.gob.mx	Capa de Sockets Seguros (SSL).

http://asesores.sep.gob.mx	No Aplica
http://cambiosinterestatales.sep.gob.mx	No Aplica
http://cat.sep.gob.mx	No Aplica
http://cenni.sep.gob.mx	No Aplica
http://cenni.sep.gob.mx/cenni/CapturaSolicitud	No Aplica
http://cenni.sep.gob.mx/cenni/consulta/BusquedaCenni.jsp	No Aplica
http://dgfcms.sep.gob.mx	No Aplica
http://disep.sep.gob.mx	No Aplica
http://experienciasconapase.sep.gob.mx	No Aplica
http://forosdeconsulta2014.sep.gob.mx/	No Aplica
http://fortepadron.sep.gob.mx	No Aplica
http://inmuebles.sep.gob.mx	No Aplica
http://intracitas.sep.gob.mx	No Aplica
http://intranet.sep.gob.mx	No Aplica
http://ninastem.aprende.sep.gob.mx	No Aplica
http://pnca.sep.gob.mx	No Aplica
http://premionacionalciencias.sep.gob.mx	No Aplica
http://proedit.sep.gob.mx	No Aplica
http://registrormg.sep.gob.mx	No Aplica
http://repuce15.sep.gob.mx	No Aplica
http://repuce16.sep.gob.mx	No Aplica
http://rmg.sep.gob.mx	No Aplica
http://scca.sep.gob.mx/scca/	No Aplica
http://seguridadti.sep.gob.mx	No Aplica
http://serviciosweb.sep.gob.mx	No Aplica
http://sgsirvoems.sep.gob.mx/	No Aplica
http://sirede.sep.gob.mx/	No Aplica
http://sirvoems.sep.gob.mx/	No Aplica
http://sistablet.sep.gob.mx	No Aplica
http://teceducativas.sep.gob.mx	No Aplica
http://tips.sep.gob.mx	No Aplica
http://tramiteprof.sep.gob.mx	No Aplica
http://www.5pasos.sep.gob.mx	No Aplica
http://www.control escolar.sep.gob.mx	No Aplica



http://www.dgri.sep.gob.mx	No Aplica
http://www.educa.sep.gob.mx	No Aplica
http://www.educamorelos.sep.gob.mx	No Aplica
http://www.expcedula.sep.gob.mx	No Aplica
http://www.expcedula.sep.gob.mx/login.jsp	No Aplica
http://www.forte.sep.gob.mx	No Aplica
http://www.mexterior.sep.gob.mx	No Aplica
http://www.reformaeducativa.sep.gob.mx	No Aplica
http://www.repuce.sep.gob.mx	No Aplica
http://www.rsa.sep.gob.mx/	No Aplica
http://www.sdpc.sep.gob.mx	No Aplica
http://www.sicd.sep.gob.mx	No Aplica
http://www.telsep.sep.gob.mx	No Aplica
http://www.transparenciafocalizada.sep.gob.mx	No Aplica
http://www.upepe.sep.gob.mx	No Aplica
http://zprepav.sep.gob.mx/	No Aplica

2. De cada una de sus actuales paginas electrónicas o webs oficiales, fecha exacta y duración de todos los ataques de Denegación de Servicio (DoS) ó Denegación de Servicio Distribuida (DDoS) padecidos.

A continuación, se muestran los ataques de Denegación de servicio por mes de manera general a las páginas del dominio sep.gob.mx como lo muestra la herramienta de monitoreo, cabe mencionar que dichos ataques van dirigidos al sitio central donde se hospedan los servidores de la Secretaria de Educación Pública, y estos fueron detenidos y bloqueados por la Infraestructura de Seguridad Informática, sin causar afectación a los servicios publicados.

Cabe mencionar que la herramienta de monitoreo muestra los acumulados hits (firmas que se activan) durante el mes, sin embargo, no muestra fecha exacta o duración del mismo a menos que se trate de un ataque con afectación.

**ATAQUES DE
DENEGACIÓN DE
SERVICIOS 2018**

Mes	Ataques	Denegación de Servicio	Detectada y Bloqueada
Enero	62 Denegación de Servicio Detectada y Bloqueada		
Febrero	631	Denegación de Servicio	Detectada y Bloqueada
Marzo	12,500 Denegación de Servicio Detectada y Bloqueada		
Abril	46,300	Denegación de Servicio	Detectada y Bloqueada
Mayo	97 Denegación de Servicio Detectada y Bloqueada		
Junio	1,232,200	Denegación de Servicio	Detectada y Bloqueada
Julio	682,100 Denegación de Servicio Detectada y Bloqueada		



Agosto	295,000	Denegación de Servicio	Detectada y Bloqueada
Septiembre	1,500,000 Denegación de Servicio Detectada y Bloqueada		
Octubre	452,000	Denegación de Servicio	Detectada y Bloqueada
Noviembre	425,000 Denegación de Servicio Detectada y Bloqueada		
Diciembre	56,000	Denegación de Servicio	Detectada y Bloqueada

" (SIC)

III. Inconforme con la respuesta proporcionada, el particular interpuso recurso de revisión manifestando:

"RECURSO DE REVISIÓN

NUMERO DE SOLICITUD: 0001100766318

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES

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 6º, apartado A fracción IV constitucional, artículos 146, 147, 148, 149, 151 párrafo 2º y demás relativos de la Ley Federal de Transparencia y Acceso a la Información Pública, interpongo el recurso de revisión en contra de la entrega de información incompleta, efectuada por la Secretaria de Educación Pública (SEP) en respuesta a la solicitud de información número de folio 0001100766318.

I.- RAZONES Y MOTIVOS DE INCONFORMIDAD

AGRAVIO ÚNICO.- Violación a los principios de máxima publicidad, exhaustividad y congruencia.

ARTÍCULOS TRANSGREDIDOS: 6º DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, 1º, 4º, 11 Y 12 DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA, 3º y 59 DE LA LEY FEDERAL DE PROCEDIMIENTO ADMINISTRATIVO, DE APLICACIÓN SUPLETORIA, 1º, 3º, 7º y 133 DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA.

Inicialmente es conveniente traer a la memoria los alcances y efectos jurídicos de los principios de exhaustividad y congruencia; ambos de aplicación imperativa en materia de transparencia y acceso a la información.

De acuerdo con el criterio interpretativo 02/17 pronunciado por este Instituto, se delimito que el principio de exhaustividad tiende a garantizar a los solicitantes de información, que los sujetos obligados se refieran expresamente a cada uno de los puntos señalados en la solicitud;



SEP

SECRETARÍA DE
EDUCACIÓN PÚBLICA

SESIÓN ORDINARIA

ACT/CT/SO/07/05/2019-R

mientras que el principio de congruencia garantiza que los sujetos obligados emitan respuestas en concordancia a lo requerido.

Segunda Época

Criterio 02/17

CONGRUENCIA Y EXHAUSTIVIDAD. SUS ALCANCES PARA GARANTIZAR EL DERECHO DE ACCESO A LA INFORMACIÓN.

De conformidad con el artículo 3 de la Ley Federal de Procedimiento Administrativo, de aplicación supletoria a la Ley Federal de Transparencia y Acceso a la Información Pública, en términos de su artículo 7; todo acto administrativo debe cumplir con los principios de congruencia y exhaustividad. Para el efectivo ejercicio del derecho de acceso a la información, la congruencia implica que exista concordancia entre el requerimiento formulado por el particular y la respuesta proporcionada por el sujeto obligado; mientras que la exhaustividad significa que dicha respuesta se refiera expresamente a cada uno de los puntos solicitados. Por lo anterior, los sujetos obligados cumplirán con los principios de congruencia y exhaustividad, cuando las respuestas que emitan guarden una relación lógica con lo solicitado y atiendan de manera puntual y expresa, cada uno de los contenidos de información.

Página 1 de 2

Respecto del 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), podemos indicar que este 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

Artículo 11. Toda la información en posesión de los sujetos obligados será pública, completa, oportuna y accesible, sujeta a un claro régimen de excepciones que deberán estar definidas y ser además legítimas y estrictamente necesarias en una sociedad democrática.

Artículo 12. Toda la información pública generada, obtenida, adquirida, transformada o en posesión de los sujetos obligados es pública y será accesible a cualquier persona, para lo que se deberán habilitar todos los medios, acciones y esfuerzos disponibles en los términos y condiciones que establezca esta Ley, la Ley Federal y las correspondientes de las Entidades Federativas, así como demás normas aplicables.

Ahora bien, en contravención a estos principios protectores del derecho fundamental de acceso a la información reconocido constitucional y convencionalmente en favor de mi persona, el sujeto obligado entrega información incompleta; toda vez que hace falta lo petitionado en el numeral 1 de la solicitud 0001100766318, por cuanto hace a los números de serie de cada equipo de computo.

PRUEBAS



A. 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. Previo estudio en función del principio de máxima publicidad, 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.

Página 2 de 2

“(SIC).”

- IV. La **Secretaría de Educación Pública (SEP)**, a través de la Unidad de Transparencia, rindió los alegatos respectivos al Recurso de Revisión mediante los cuales la **Dirección General de Tecnologías de la Información y Comunicaciones (DGTIC)** manifestó lo siguiente:

”ALEGATOS

“Con el propósito de verter el presente escrito, la Unidad de Transparencia turnó el medio de impugnación a la Dirección General de Tecnologías de la Información y Telecomunicaciones (DGTIC) misma que después de una búsqueda exhaustiva y razonable manifestó lo siguiente:

Respecto del supuesto agravio que pretende hacer valer el recurrente, se manifiesta que es inoperante al caso concreto, ya que el recurrente menciona que falto responder lo peticionado en el numeral 1 de dicha solicitud, en donde menciona lo siguiente:

“1. Por número de serie de cada uno de los equipos de cómputo en posesión de los sujetos obligados requiero.” (SIC).

Al respecto es importante señalar que de la manera en la que el requirente realiza la petición se desprende que solicita información correspondiente a los incisos subsecuentes, entendiéndose el uso de los dos puntos como lo define la Real Academia Española:



“dos puntos. Signo de puntuación (:) que representa una pausa mayor que la de la coma y menor que la del punto. Detienen el discurso para llamar la atención sobre lo que sigue, que siempre está en estrecha relación con el texto precedente. Se escriben pegados a la palabra o el signo que los antecede, y separados por un espacio de la palabra o el signo que los sigue.

1. Usos lingüísticos

1.1. Preceden a una enumeración de carácter explicativo: Ayer me compré dos libros: uno de Carlos Fuentes y otro de Cortázar.”

Ahora bien, en ese caso se entiende como sigue:

- *“1. Por número de serie de cada uno de los equipos de cómputo en posesión del sujeto obligado requiero: a) Nombres comerciales de los sistemas operativos instalados”.*

Ante tal cuestionamiento se respondió:

“Cada uno de los equipos en posesión de la Dirección General de Tecnologías de la Información y Comunicaciones, cuenta con los siguientes sistemas operativos instalados.

- *Windows 10 Enterprise*
- *MacOS High Sierra 10.13”.*

El recurrente manifiesta que la respuesta no es exhaustiva y congruente, sin embargo, de la afirmación universal: “Cada uno de los equipos (...)”, se desprende que todos los equipos de cómputo en posesión de la Dirección General de Tecnologías de la Información y Comunicaciones cuentan con los mismos sistemas operativos instalados, por lo que resulta innecesario desglosar y relacionar cada número de serie correspondiente a cada equipo de cómputo con dichos sistemas operativos.

- *“1. Por número de serie de cada uno de los equipos de cómputo en posesión del sujeto obligado requiero: b) Nombres comerciales y versiones de los antivirus o software de seguridad en Internet, instalados”.*

Ante tal cuestionamiento, se respondió:

- *“Windows Defender”.*

La respuesta se abordó en el mismo sentido que la anterior, de tal manera que se abarca en su totalidad ya que no existe algún equipo de cómputo que cuente con alguna diferencia en cuanto al software de seguridad instalado.

- *“1. Por número de serie de cada uno de los equipos de cómputo en posesión del sujeto obligado requiero: c) Inicio y término de la vigencia de cada licencia utilizada en los softwares mencionados en el anterior inciso b)”.*

Ante tal cuestionamiento, se respondió:

- *“Vigencia del 2018 – 2020”.*

Con la respuesta otorgada se afirma de tal manera que dicha vigencia abarca la licencia utilizada en la totalidad de equipos de cómputo en posesión de ésta Dirección, por lo tanto, es innecesario vincular uno por uno los números de serie contenidos en cada equipo.

Al respecto es importante señalar que el recurrente en ningún momento hace mención expresa de requerir exclusivamente los números de serie de los equipos de cómputo ya que



en reiteradas ocasiones ha tratado de obtener dicha información de la cual el Instituto ha velado por la seguridad de los datos personales en posesión de este sujeto obligado al confirmar la reserva de información en las siguientes resoluciones:

RRA 5585/18, de fecha: 09 de octubre de 2018

"... se advierte que difundir la información relativa a los números de serie y números de parte, así como, la forma en que cada equipo obtiene o asigna dirección IP, incrementa sustancialmente la posibilidad de que aquella persona que conozca dicha información cometa algún ilícito, accediendo de forma no autorizada a los sistemas de datos que no son públicos en posesión del sujeto obligado, conociendo con un alto grado de precisión la información técnica referente a sus equipos de cómputo, los protocolos de seguridad y las características de la infraestructura instalada.

En este sentido, derivado de la naturaleza y el grado de especificidad del tipo de información que se requiere, pus se trata de un elemento relevante al ponderar cualquier posible vulneración a la seguridad de la infraestructura tecnológica de la autoridad obligada, es que se colige que dar a conocer la misma facilitaría que personas expertas en informática perturben el sistema de la infraestructura tecnológica de la Secretaría de Educación Pública, ejecuten programas informáticos perjudiciales que modifiquen o destruyan información relevante; situación que pondría en un estado vulnerable la información que en ella se contiene, facilitando la intervención de las comunicaciones.

(...)

Ahora bien, en relación con el periodo de reserva, previsto en los artículos 99 y 100 de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el Trigésimo Cuarto de los Lineamientos Generales en materia de clasificación y desclasificación de la información así como para la elaboración de versiones públicas en los que se dispone que la información clasificada podrá permanecer con tal carácter hasta por un periodo de cinco años, este Instituto considera que debe establecerse un plazo de cinco años, toda vez que es proporcional al tipo de información que se requiere, a fin de asegurar la vida, seguridad de una o varias personas físicas".

Expedientes: RRA/3831/18 y su acumulado RRA 4377/18 de fecha: 29 de agosto de 2018.

"De la normatividad señalada, se advierte que comete el delito de acceso ilícito a sistemas y equipos de informática todo aquel que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, sean o no propiedad del Estado. Asimismo, al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrá de seis meses a dos años de prisión y de cien a trescientos días de multa.

Sobre el particular, cabe recordar que, con base en las opiniones que formuló la Dirección General de Tecnologías de la Información de éste Instituto, vertidas en párrafos anteriores,



se puede concluir que, el proporcionar el número de serie o parte, el nombre de los navegadores, servidores DNS (Domain Name System), direcciones MAC (Media Access Control) de cada tarjeta o adaptador de red, modelos de los módems, ruteadores y puntos de acceso inalámbrico, puede ocasionar intrusiones, robo de identidad, afectación en las comunicaciones y por ende un ataque masivo a los equipos de cómputo que se encuentran conectados en la red interna de la Secretaría de Educación Pública.

De esta forma, con la publicidad de los datos de interés del particular, a saber, los contenidos en los puntos 1), 5), 9) y 10) de la solicitud, se generaría un riesgo potencial para la infraestructura tecnológica de la referida Secretaría, ya que pueden ser utilizados para propiciar ataques informáticos de diversa índole.

(...)

“En conclusión, este Instituto advierte que es procedente la reserva invocada por la Secretaría de Educación Pública, con fundamento en el artículo 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública, respecto de la información requerida en los puntos 1), 5), 9) y 10) de la solicitud, consistente en: el número de serie, de parte, nombre de los navegadores,, servidores DNS (Domain Name System), direcciones MAC (Media Access Control) de cada tarjeta o adaptador de red, modelo de los MODEMS, ROUTERS (rúters) o Puntos de acceso inalámbricos, de cada uno de los equipos de cómputo en posesión del sujeto obligado”.

RRV 3830/18 de fecha: 29 de agosto de 2018.

“En este orden de ideas, este Instituto advierte ineludible que, en cumplimiento a lo establecido en el artículo 140. Fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública, el sujeto obligado formalice la reserva de la información, incluyendo el razonamiento expresado durante la diligencia de acceso a la información clasificada, esto es, que los datos consistentes en el número de serie, de parte, marca, modelo y seguridad de cada uno de los módems, rúters o puntos de acceso inalámbrico con los que cuenta, de manera concatenada a las unidades administrativas, áreas u órganos que hacen uso de los mismos, permitiría vulnerar la seguridad implementada en sus redes de telecomunicaciones, constituyendo un riesgo inminente de la comisión de delitos cibernéticos, esto con fundamento en la fracción VII del artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública.

Una vez expuesto lo anterior, no debe eludirse que además de los datos consistentes en número de serie, de parte, de modelo, marca, seguridad o cifrado implementado en la conexión WIFI, relativo a los módems, routers (rúters) o puntos de acceso inalámbrico, así como las unidades administrativas que hace uso de los mismos ...”

Derivado de lo anterior, se hace notar que el recurrente sistemáticamente ha realizado múltiples solicitudes de información clasificada como reservada y que en su conjunto facilitan únicamente los ataques a la red de telecomunicaciones y que no contribuye a la transparencia ni a la rendición de cuentas, pues no documentan la gestión pública y



actualiza el riesgo de facilitar la transgresión a varios principios jurídicos tutelados tal como la protección de datos y la prevención de delitos”.

Aunado a lo anterior, cabe destacar que se cometió un error humano al transcribir la pregunta del requirente correspondiente al numeral 1, en la que se menciona lo siguiente:

“1.- Por número de serie de cada uno de los equipos de cómputo en posesión del sujeto obligado requerido, se adjunta archivo en formato PDF”. (SIC).

Se agregó por error la palabra “requerido” en lugar de “requiero”, seguida de la frase “se adjunta archivo en formato PDF.” (SIC), siendo que la solicitud de información que realizó el requirente termina hasta la coma (,) donde realmente se encuentran dos puntos (:), es decir la solicitud originalmente dice:

“1.- Por número de serie de cada uno de los equipos de cómputo en posesión del sujeto obligado requiero.”. (SIC).

Por lo anterior, se entiende de manera errónea que el solicitante requirió que dicha información se adjuntará en archivo PDF, siendo que se debió meramente a un error humano en la transcripción de dicha solicitud. No obstante, se reitera la respuesta que se brindó en cada uno de los incisos siguientes, debido a que el mencionado error no cambia en nada la sustancia contenida en la misma, y la respuesta atiende a los principios de máxima publicidad, exhaustividad y congruencia.” (SIC)

- V. El 24 de abril de 2019, el Pleno del **Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales**, aprobó por mayoría la resolución recaída en el recurso de revisión **RRA 0561/19**, donde entre otros asuntos, manifestó lo siguiente:

“



QUINTO. Efectos de la Resolución.

Por lo expuesto, con fundamento en lo dispuesto en el artículo 157, fracción III de la LFTAIP, resulta procedente **modifica** la respuesta emitida por el sujeto obligado y se le **instruye** a efecto de que realice lo siguiente:

- Emita a través de su Comité de Transparencia, la resolución en la que confirme la clasificación como reservada de los números de serie de cada uno de los equipos de cómputo que posee el sujeto obligado, aplicando la prueba de daño y el plazo de reserva conforme al análisis realizado en la presente determinación de conformidad con lo dispuesto por el artículo 110, fracción VII de la LFTAIP, misma que deberá remitir a la particular.

El sujeto obligado deberá entregar a la recurrente resolución respectiva, a través de su correo electrónico, o ponerla a su disposición en un sitio de Internet y comunicarle los datos que le permitan acceder a la misma, de conformidad con lo dispuesto en el párrafo primero del artículo 132 de la Ley Federal de Transparencia y Acceso a la Información Pública.

...“(SIC)”

VI. La Unidad de Transparencia turnó la resolución del recurso **RRA 0561/19** emitida por el Pleno del **INAI** a la **Dirección General de Tecnologías de la Información y Comunicaciones (DGTIC)**, a efecto de que se diera cumplimiento a la misma, la cual después de realizar una búsqueda exhaustiva y razonable, manifiesta lo siguiente:

“Toda vez que se recibió solicitud de información con número de folio 0001100766318 en el cual requieren información que debe ser reservada por seguridad de la información, se solicita su intervención a efecto de solicitar al Comité de Transparencia y Acceso a la Información Pública la RESERVA de la siguiente información:

Área: Dirección General de Tecnologías de la información y Comunicaciones.

Nombre del expediente o documento:

Número de serie de cada uno de los equipos de cómputo en posesión de la Secretaría de Educación Pública.

Tema: Seguridad Informática y seguridad de la información

Momento de la clasificación de la información como reservada: Momento de recibir la solicitud de información pública con número de folio 0001100766318

Plazo de reserva: Cinco años.

Fecha de inicio de la clasificación: 07 de mayo de 2019.

Fecha de término de la clasificación: 07 de mayo de 2024.



Fundamento legal de la clasificación: Artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública en relación con el artículo 113, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública y Lineamientos Generales en materia de Clasificación y Desclasificación en su artículo Vigésimo Sexto.

Justificación:

Entregar los datos concernientes al número de serie de equipos de cómputo en posesión de la Secretaría de Educación Pública, representa un riesgo de ataque informático, ya que incrementa sustancialmente la posibilidad de que aquella persona que conozca dicha información cometa algún ilícito, accediendo de forma no autorizada a los sistemas de datos que no son públicos en posesión del sujeto obligado.

En este sentido, derivado de la naturaleza y el grado de especificidad del tipo de información que se requiere, se trata de un elemento relevante al ponderar cualquier posible vulneración a la seguridad de la infraestructura tecnológica de la Secretaría de Educación Pública, es que se colige que dar a conocer la misma facilitaría que personas expertas en informática perturben el sistema de la infraestructura tecnológica de la Secretaría de Educación Pública, ejecuten programas informáticos perjudiciales que modifiquen o destruyan información relevante; situación que pondría en un estado vulnerable la información que en ella se contiene, por lo tanto, en términos de lo dispuesto por los artículos 106 de la Ley General de Transparencia y Acceso a la Información Pública fracción I, 113, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública, su análogo en el 110, fracciones VII de la Ley Federal de Transparencia y Acceso a la Información Pública, así como en los Lineamientos Generales en materia de Clasificación y Desclasificación en su artículo Vigésimo Sexto, puede tener la calidad de Información reservada.

Razones y motivos de la clasificación:

En caso de proporcionar dichos números de serie, se pone en riesgo la seguridad informática y la seguridad de la información de conformidad con el siguiente detalle que consta de la solicitud y las razones para reservar la información requerida:

Proporcionar el número de serie de equipos de cómputo del sujeto obligado, puede ocasionar intrusiones, robo de identidad, afectación en las comunicaciones y por ende un ataque masivo a los equipos de cómputo que se encuentren conectados en la red interna de la Secretaría de Educación Pública y con ello, una afectación en los equipos informáticos y la información contenida en estos.

De esta forma, con la publicidad de los números de serie se generaría un riesgo potencial para la infraestructura tecnológica de la Secretaría de Educación Pública, ya que pueden ser utilizados para la realización de ataques informáticos de diversa índole.



Por lo anterior, y con fundamento en los artículos 104 de la Ley General de Transparencia y Acceso a la Información Pública, y 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, y en concordancia en los "Lineamientos Generales en Materia de Clasificación y desclasificación de la Información, así como para la Elaboración de las Versiones Públicas", en su apartado, Décimo séptimo, último párrafo, Décimo octavo, Décimo noveno y Vigésimo

segundo, fracción I, se procede al correspondiente análisis de la PRUEBA DE DAÑO, en los siguientes términos:

Difundir o hacer del conocimiento público la información solicitada supondría una enorme ventaja para cualquier atacante de sistemas y redes de telecomunicaciones al proporcionarle herramientas para facilitar un ataque a los sistemas de telecomunicaciones con que cuenta la Secretaría poniendo en riesgo la información contenida tanto en los equipos de cómputo como la contenida en los equipos de servidores que procesan información que dependiendo el área de la Secretaría que sea atacado supondría, por ejemplo, un ataque equipos del Órgano Interno de Control o a la Unidad de Asuntos Jurídicos que podría obstruir el seguimiento de procesos administrativos en forma de juicio o entorpecer investigaciones, conocer la ubicación física de una persona identificada o identificable, realizar una suplantación de identidad.

La divulgación de la información relativa a los números de serie de los equipos de cómputo de la Secretaría de Educación Pública representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público, toda vez que se colocaría en estado de vulnerabilidad que permitiría el acceso ilícito de los equipos de cómputo e información contenida en estos.

RIESGO REAL

La divulgación de la información representa un riesgo real ya que de entregarse, se proporcionaría información para llevar a cabo ataques informáticos a los equipos de cómputo y equipos de procesamiento de aplicativos que cuentan con bases de datos con datos personales de ciudadanos usuarios de sistemas y portales web de la Secretaría, en concordancia con lo mencionado, cabe señalar que la SEP realiza esfuerzos para mantener la seguridad de sus equipos y sistemas, por lo cual actualmente devenga recursos para contar con un servicio administrado de seguridad informática que previene los ataques mencionados, entre otros, por lo que proporcionar información que facilite un ataque, supone un aumento en la probabilidad de éxito de un atacante informático, poniendo en riesgo la seguridad y la estabilidad de los sistemas y redes de telecomunicaciones de esta Secretaría.

El riesgo de perjuicio que supondría la divulgación de información supera el interés público general de que se difunda, toda vez que la misma no resulta útil a la ciudadanía en general, sino específicamente a especialistas en informática que pueden obtener



información a partir de la solicitada como puede ser atacar y obtener información de los equipos, redes y conocer información crítica.

RIESGO DEMOSTRABLE

En razón de que es altamente probable y de inminente peligro que dar a conocer la información solicitada, materializaría el riesgo que se busca evitar al contar con un servicio de seguridad informática, con lo cual se busca minimizar efectos negativos en la infraestructura tecnológica de la Secretaría, ejemplo de ello es que actualmente se cuenta con un servicio a administrado de seguridad informática y que el Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y comunicaciones así como de la Seguridad en la Información privilegia la seguridad en los sistemas y redes de telecomunicaciones de la Administración Pública Federal.

La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar un perjuicio ya que únicamente se están solicitando reservar los conceptos de información que puede poner en riesgo a la infraestructura tecnológica de la Secretaría.

RIESGO IDENTIFICABLE

En el caso que nos ocupa, el riesgo identificable es el uso que se le dé a la información solicitada puesto que el mal uso de ella causaría una vulnerabilidad específica en los sistemas, equipos y redes de telecomunicaciones de la Secretaría pudiendo inhabilitar segmentos red, identificando ubicación física de los usuarios, intentos de ataque de tipo de intrusión y robo de datos, una posible intervención en la comunicación, la suplantación de equipos de la información que se almacena en el servidor, el detrimento de las instalaciones tecnológicas, el hackeo de los sistemas informáticos.

Cuestiones que se materializan con la comisión de delitos de carácter cibernético, que sin duda afectaría severamente el funcionamiento de la infraestructura tecnológica.

Lo anterior resulta relevante, ya que, de la negativa de acceso a la información se motiva en razón de prevenir la comisión de un delito de carácter cibernético que afectaría los equipos informáticos y la información contenida en estos.

Lo anterior en relación con el Código Penal Federal sobre el acceso ilícito a sistemas y equipos de informática dispuesto en los siguientes:

Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.



Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá, además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Artículo 211 bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

En este sentido divulgar la información solicitada, permitiría que terceros contaran con los elementos para intentar algún tipo de ataque cibernético para ingresar sin autorización, a todos y cada uno de los equipos de cómputo de esta Secretaría, lo que permitiría la comisión de delitos, como podrían ser los relacionados con el acceso ilícito a sistemas y equipos informáticos, entre otros.

Ahora bien, la divulgación de esta información reservada representa un riesgo real, demostrable e identificable y de perjuicio significativo al interés público, toda vez que al hacerla pública se proveen elementos técnicos que podrían obstruir la prevención de delitos demostrables e identificables, como los de suplantación de identidad y de acceso ilícito a sistemas y equipos informáticos.

Con base en lo anterior, en este caso particular, concurre tanto el derecho de acceso a la información como la obligación de los sujetos obligados de clasificar como información reservada aquella que obstruya la prevención o persecución de los delitos, ambos constituyen fines legítimos, los cuales están consagrados en el artículo 6 de nuestra Constitución Política de los Estados Unidos Mexicanos y normatividad aludidos. De esta forma, al ponderar entre tales derechos se considera que en este caso concreto debe prevalecer la reserva de la información para no obstaculizar la prevención de delitos, lo cual tiene sustento en el marco jurídico mencionado.



De acuerdo con el principio de proporcionalidad, se concluye que la afectación que podría traer la divulgación de la información solicitada es mayor que el interés público de que se difunda, por lo que se considera que en este caso debe prevalecer la reserva, pues ello representa el medio menos restrictivo disponible para evitar un perjuicio a la prevención de delitos demostrables e identificables.” (SIC)

Por lo tanto, la **Dirección General de Tecnologías de la Información y Comunicaciones (DGTIC)**, solicita a este H. Comité, la confirmación de la clasificación de la información como reservada por un periodo de 05 (cinco) años, en los términos descritos con anterioridad.

ACUERDO DE COMITÉ: ACT/CT/SO/07/05/2019-R.1.- CON FUNDAMENTO EN EL ARTÍCULO 65, FRACCIÓN II DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA, EL COMITÉ DE TRANSPARENCIA DE LA SECRETARÍA DE EDUCACIÓN PÚBLICA, CONFIRMA POR MAYORÍA LA CLASIFICACIÓN DE LA INFORMACIÓN COMO RESERVADA POR UN PERIODO DE 05 (CINCO) AÑOS, ATENDIENDO LOS ARGUMENTOS VERTIDOS CON ANTERIORIDAD, Y CON FUNDAMENTO EN LOS ARTÍCULOS 113, FRACCIÓN VII DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA; ASÍ COMO 110, FRACCIÓN VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA, Y LOS NUMERALES TRIGÉSIMO, 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.

No habiendo más asuntos que tratar, se da por terminada la sesión, firmando al inicio los que en ella intervinieron.