

Procuraduría Federal de Protección al Ambiente
Comité de Transparencia

RESOLUCIÓN DE COMITÉ DE INFORMACIÓN N°: 0015/18
RECURSO DE REVISIÓN INAI RRA 4856/18
SOLICITUD DE INFORMACIÓN N°: 1613100050218

ANTECEDENTES

- I. El 11 de Junio de 2018, la Unidad de Transparencia de la Procuraduría Federal de Protección al Ambiente (PROFEPA) recibió a través de la Plataforma Nacional de Transparencia, la solicitud de acceso a información, y turnó a la Dirección General de Administración y a la Dirección de Atención Ciudadana y Comunicación Social, registrada con el número de folio 1613100050218:

"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. 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 con el 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 inglés Media Access Control) de cada tarjeta o adaptador de red (WIFI, BLUETOOTH, ETHERNET) de la que disponga cada equipo de cómputo." (Sic)

- II. Mediante oficios Nos. OP/UT/0925/18 y OP/UT/00939/18 ambos de fecha 12 de junio de 2018, la Unidad de Transparencia solicitó a la Dirección General de Administración y a la Dirección de Atención Ciudadana y Comunicación Social, si en esas unidades administrativas se cuenta con la información solicitada, dando contestación de manera puntual y precisa a todos y cada uno de los cuestionamientos contenidos en la referida solicitud de información.
- III. En seguimiento a lo anterior, mediante Oficio Nos. PFFPA/6.4/8C.27/125/18 de fecha 18 de junio de 2018, la Dirección General Adjunta de Evaluación e Informática, adscrita a la Dirección General de Administración y PFFPA/1.4/12C.6/0046-18 la Dirección de Atención Ciudadana y Comunicación Social hicieron del conocimiento de la Unidad de Transparencia esencialmente lo siguiente:

• Dirección General Adjunta de Evaluación e Informática

"1: 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."

R= Anexo al presente 14 fojas útiles con la relación de números de serie de los equipos con los que cuenta la PROFEPA, el navegador que bien preinstalado con los equipos de cómputo es internet Explorer.

"2. Motivos por los cuales son utilizados únicamente los navegadores de Internet a los que se haga referencia en relación con el punto anterior."

R= Es el navegador con el que viene instalado los equipos

"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."

**Procuraduría Federal de Protección al Ambiente
Comité de Transparencia**

**RESOLUCIÓN DE COMITÉ DE INFORMACIÓN N°: 0015/18
RECURSO DE REVISIÓN INAI RRA 4856/18
SOLICITUD DE INFORMACIÓN N°: 1613100050218**

R= No se tiene instalado en ningún equipo.

"4. NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DE TODOS LOS PROVEEDORES DE SERVICIOS DE TELECOMUNICACIONES. ESPECIFICANDO AQUELLOS QUE PROVEAN ACCESO A INTERNET."

R= Teléfonos de México, S.A. B. de C.V.

"5. SERVIDORES DNS (Domain Name System) UTILIZADOS PARA EL ACCESO A INTERNET."

R= Con fundamento en lo establecido en los artículos 113 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública y 116 párrafo tercero de la Ley General de Transparencia y Acceso a la Información Pública y al Cuadragésimo Cuarto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, SE SOLICITA AL Comité de Transparencia sea considerado como información Confidencial, debido a que estos servidores son generados con motivos comerciales, están resguardados en servidores que son del dominio público y le dan al proveedor una ventaja competitiva ante su competencia al no ser divulgados.

"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 inglés Media Access Control) de cada tarjeta o adaptador de red (WIFI, BLUETOOTH, ETHERNET) de la que disponga cada equipo de cómputo."

R= Los números de serie ya se enviaron en el punto número 1.

Los datos correspondientes a la dirección MAC, de cada tarjeta o adaptador de red, no se cuenta con ellos derivado de que no son proporcionados por el proveedor de servicio.

Dirección de Atención Ciudadana y Comunicación Social

Las redes sociales oficiales utilizadas por la Procuraduría Federal de Protección al Ambiente son:

- Facebook.
- Twitter
- Instagram
- YouTube
- Flickr

Motivos por los cuales son utilizadas únicamente las redes sociales previamente mencionadas:

Tomando en cuenta datos de la Asociación de internet. Mx en México el 90% de la población utiliza un Smartphone y las redes sociales, las más utilizadas en México se encuentran: Facebook, YouTube, Twitter e Instagram (en ese orden).

Facebook sigue siendo la red social por excelencia en nuestro país, razón por la cual se tiene una cuenta para tener comunicación bidireccional con los ciudadanos mexicanos. Un medio de transmisión para eventos o conferencias de prensa "en vivo"

Youtube: Nuestro canal es apoyo visual a las televisoras, ilustrativo de los boletines enviados por la Dirección de Atención Ciudadana y de Comunicación Social. Inclusive un medio de transmisión para eventos o conferencias de prensa "en vivo".

Twitter: Permite enviar y recibir la información con un tiempo más corto de respuesta. Ideal para narrativas de eventos, conferencias de prensa o orientación a la población sobre algún fenómeno o accidente.

**Procuraduría Federal de Protección al Ambiente
Comité de Transparencia**

**RESOLUCIÓN DE COMITÉ DE INFORMACIÓN N°: 0015/18
RECURSO DE REVISIÓN INAI RRA 4856/18
SOLICITUD DE INFORMACIÓN N°: 1613100050218**

Instagram: Muestra una creciente tendencia de uso en la población mexicana. Para la cuenta de la PROFEPA, es usada más para fines educativos y de conciencia ambiental. Menos bidireccional que Twitter o Facebook pero con contenido más ilustrativo, persuasivo y noble.

Flickr: Permite subir fotografías, artes o diseños con excelente calidad, por lo cual se emplea para proveer álbumenes fotográficos ilustrativos de los boletines que se envían a medios.

No se cuenta con una cuenta en la red social VK (Vkontakte)

- IV. Este Comité de Transparencia mediante resolución No. 0008/18 confirmó la confidencialidad en relación al cuestionamiento de SERVIDORES DNS (Domain Name System) UTILIZADOS PARA EL ACCESO A INTERNET, con fundamento en lo señalado por el artículo 113 fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública y 116 de la Ley General de Transparencia y Acceso a la Información Pública, por los argumentos hechos valer por la citada Unidad Administrativa; por lo que en seguimiento a lo instruido por el citado Comité, mediante oficio No. PFPA/1.7/12C.6/01032/18, de fecha 26 de junio de 2018, enviado a través del Sistema de Solicitudes de Información INFOMEX, la Unidad de Transparencia hizo del conocimiento del solicitante la respuesta.
- V. Con fecha 08 de agosto de 2018, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, notificó a esta Procuraduría Federal de Protección al Ambiente, mediante Herramienta de Comunicación, el Acuerdo de Admisión del recurso de revisión interpuesto, en contra de la respuesta otorgada por esta Procuraduría a través de la Unidad de Transparencia, a la solicitud de información con número de folio 1613100050218.
- VI. Mediante oficio PFPA/1.7/12C.6/01196/18 de fecha 09 de agosto de 2018, la Unidad de Transparencia hizo del conocimiento de la Dirección General Adjunta de Evaluación e Informática el recurso de revisión interpuesto, en contra de la respuesta otorgada por esta Procuraduría a través de la Unidad de Transparencia, a su solicitud de información con número de folio 1613100050218.
- VII. Mediante oficio No. PFPA/6.4/8C.28/176/18 de fecha 13 de agosto de 2018, la Dirección General Adjunta de Evaluación e Informática señaló a la Unidad de Transparencia lo siguiente:

'5. SERVIDORES DNS (Domain Name System) UTILIZADOS PARA EL ACCESO A INTERNET.'

Respuesta: Con fundamento en lo establecido en los artículo 113 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública y 116 párrafo tercero de la Ley General de Transparencia y Acceso a la Información Pública y al Cuadragésimo Cuarto de los Lineamientos Generales en materia de Clasificación y Desclasificación de la información, se solicita al Comité de Transparencia sea considerado como información confidencial, debido a que estos servidores son generados con motivos comerciales, están resguardados en servidores que no son del dominio público y le dan al proveedor una ventaja competitiva ante su competencia al no ser divulgados.

Aunado a este tema, el conocimiento de esta información por externos puede ser una ventana de vulnerabilidad para los equipos y la red de la PROFEPA, exponiéndolos a un ataque informático, estos datos como se menciona mal utilizados pueden provocar daño a la información de esta Procuraduría.

'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 inglés Media Access Control) de cada tarjeta o adaptador de red (WIFI, BLUETOOTH, ETHERNET) de la que disponga cada equipo de cómputo.'

Respuesta: Los número de serie ya se enviaron en el punto número 1 de la solicitud.

**Procuraduría Federal de Protección al Ambiente
Comité de Transparencia**

**RESOLUCIÓN DE COMITÉ DE INFORMACIÓN N°: 0015/18
RECURSO DE REVISIÓN INAI RRA 4856/18
SOLICITUD DE INFORMACIÓN N°: 1613100050218**

Los datos correspondientes a la dirección MAC, de cada tarjeta o adaptador de red, no se cuenta con ellos derivado de que no son proporcionados por el proveedor del servicio, en virtud de que esta información le permite una ventaja competitiva frente a terceros.

La contratación se refiere a un servicio administrado con equipos propiedad del prestador del servicio, por lo tanto, los equipos no son propiedad de la Procuraduría y es responsabilidad única y exclusivamente del mismo, conocerlos.

VIII. Con fecha 17 de agosto de 2018, mediante el oficio sin número la PROFEPA remitió su escrito de alegatos.

IX. El día 01 de octubre de 2018, la Unidad de Transparencia recibió a través del Sistema "Herramienta de Comunicación" la Resolución, emitida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales en el expediente número RRA 4856/18, a través de la cual el Pleno de ese Instituto, resolvió lo siguiente:

*"...Por todo lo anterior, con fundamento en el artículo 157, fracción III, de la Ley Federal de Transparencia y Acceso a la Información Pública, este Instituto considera procedente **MODIFICAR** la respuesta emitida por la Procuraduría Federal de Protección al Ambiente, a efecto de que:*

• Siguiendo el procedimiento previsto en la Ley Federal de Transparencia y Acceso a la Información Pública ante el Comité de Transparencia, clasifique como información reservada los Servidores DNS (Domain Name System) utilizados para el acceso a internet y la dirección MAC (por sus siglas en inglés Media Access Control) de cada tarjeta o adaptador de red (wifi, bluetooth, ethernet) de la que disponga cada equipo de cómputo que tiene en posesión, de conformidad con el artículo 110, fracciones VII. en la vertiente de prevención del delito, de la Ley Federal de Transparencia y Acceso a la Información Pública; cumpliendo con la prueba de daño, el plazo de reserva será por un periodo de 5 años."

X. Mediante oficio PFPA/1.7/12C.6/02461/18 la Unidad de Transparencia hizo del conocimiento de la Dirección General Adjunta de Evaluación e Informática la resolución del Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales en el recurso de revisión RRA 4856/18

XI. Mediante oficio PFPA/6.4.1/8C.17.3/72/18 la Dirección General Adjunta de Evaluación e Informática manifestó lo siguiente:

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 los 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, (vulnerabilidades de día 0) 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.

**Procuraduría Federal de Protección al Ambiente
Comité de Transparencia**

**RESOLUCIÓN DE COMITÉ DE INFORMACIÓN N°: 0015/18
RECURSO DE REVISIÓN INAI RRA 4856/18
SOLICITUD DE INFORMACIÓN N°: 1613100050218**

Para formar una red, los equipos de cómputo deben estar interconectados a través de una interfaz que les permite comunicarse, esta interfaz se conoce como tarjeta de red o NIC (Network Interface Controller). Cada tarjeta de red NIC tiene asignado un identificador único llamado MAC (Media Access Control) o dirección física, dicha dirección está formada por 12 dígitos:

- Los seis primeros dígitos identifican al fabricante o proveedor y, de ese modo, abarcan el Identificador Exclusivo de Organización (OUI);
- Los seis dígitos restantes abarcan el número de serie de interfaz, u otro valor administrado por el proveedor específico.

Que respecto a si el dar a conocer las direcciones MAC podría representar un riesgo para la seguridad tecnológica de los equipos de cómputo y/o sistemas a los que pertenecen, uno de los principales riesgos es a través de la materialización de un ataque conocido como "MAC Spoofing" (falsificación de la dirección MAC), la cual es una técnica para cambiar la dirección MAC de un dispositivo de red. La materialización de un ataque de MAC Spoofing podría llevar a fines maliciosos como:

- Asignación de IP estática: existe la posibilidad de que un posible atacante obtenga una IP que normalmente se asigna a un equipo a través del conocimiento de la dirección MAC.
- Filtrado de direcciones MAC: falsificar direcciones MAC.
- Seguimiento del dispositivo: Como son únicas, las direcciones MAC se pueden usar como medio de rastreo.

Una vez que el atacante ha obtenido algún acceso a través de la materialización de una vulnerabilidad convertida en un ataque (por ejemplo, MAC Spoofing), éste tiene como prioridad mantener el acceso en los dispositivos afectados e incluso migrar el ataque a otros elementos conectados a la red. Las actividades en este punto son variadas, con los recursos puede lanzar nuevos ataques a otros sistemas, obtener o colocar algún archivo, afectar las aplicaciones instaladas o modificar información o archivos.

Por lo anterior, es importante que dicha información se encuentra reservada por el lapso de 5 años, ya que otorgar pone en riesgo la integridad de la información de la Institución.

CONSIDERANDOS

- I. Que este Comité de Transparencia es competente para confirmar, modificar o revocar la clasificación de información que realicen los titulares de las Áreas de la **PROFEPA**, en los términos que establecen los artículos 65, fracción II, 102 y 140, segundo párrafo de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); 44, fracción II, 103 y 137, segundo párrafo de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), así como el Vigésimo quinto de los Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública.
- II. Que las fracciones VII del artículo 110 de la LFTAIP y VII del artículo 113 de la LGTAIP, establecen que se podrá clasificar como información reservada aquella que cuya publicación obstruya la prevención o persecución de los delitos.
- III. Que el Lineamiento Vigésimo Sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas dispone que de conformidad con el artículo 113, fracción VII de la LGTAIP, podrá considerarse como información reservada, aquella que vulnere la conducción de los expedientes judiciales o de los procedimientos administrativos seguidos en forma de juicio. Para tal efecto, el sujeto obligado deberá acreditar lo siguiente:

"Vigésimo sexto. De conformidad con el artículo 113, fracción VII de la Ley General, podrá considerarse como información reservada, aquella que obstruya la prevención de delitos al obstaculizar las acciones implementadas por

**Procuraduría Federal de Protección al Ambiente
Comité de Transparencia**

**RESOLUCIÓN DE COMITÉ DE INFORMACIÓN N°: 0015/18
RECURSO DE REVISIÓN INAI RRA 4856/18
SOLICITUD DE INFORMACIÓN N°: 1613100050218**

las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos.

Para que se verifique el supuesto de reserva, cuando se cause un perjuicio a las actividades de persecución de los delitos, deben de actualizarse los siguientes elementos:

I. La existencia de un proceso penal en sustanciación o una carpeta de investigación en trámite;

II. Que se acredite el vínculo que existe entre la información solicitada y la carpeta de investigación, o el proceso penal, según sea el caso, y

Que la difusión de la información pueda impedir u obstruir las funciones que ejerce el Ministerio Público o su equivalente durante la etapa de investigación o ante los tribunales judiciales con motivo del ejercicio de la acción penal."

- IV. Que la Dirección General Adjunta de Evaluación e Informática manifestó sobre la información de los Servidores DNS (Domain Name System) utilizados para el acceso a internet y la dirección MAC (por sus siglas en inglés Media Access Control) de cada tarjeta o adaptador de red de los equipos de cómputo con que cuenta esta Procuraduría Federal de Protección al Ambiente, lo siguiente:

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 los 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, (vulnerabilidades de día 0) 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.

Para formar una red, los equipos de cómputo deben estar interconectados a través de una interfaz que les permite comunicarse, esta interfaz se conoce como tarjeta de red o NIC (Network Interface Controller). Cada tarjeta de red NIC tiene asignado un identificador único llamado MAC (Media Access Control) o dirección física, dicha dirección está formada por 12 dígitos:

- Los seis primeros dígitos identifican al fabricante o proveedor y, de ese modo, abarcan el Identificador Exclusivo de Organización (OUI);*
- Los seis dígitos restantes abarcan el número de serie de interfaz, u otro valor administrado por el proveedor específico.*

Que respecto a si el dar a conocer las direcciones MAC podría representar un riesgo para la seguridad tecnológica de los equipos de cómputo y/o sistemas a los que pertenecen, uno de los principales riesgos es a través de la materialización de un ataque conocido como "MAC Spoofing" (falsificación de la dirección MAC), la cual es una técnica para cambiar la dirección MAC de un dispositivo de red. La materialización de un ataque de MAC Spoofing podría llevar a fines maliciosos como:

- Asignación de IP estática: existe la posibilidad de que un posible atacante obtenga una IP que normalmente se asigna a un equipo a través del conocimiento de la dirección MAC.*
- Filtrado de direcciones MAC: falsificar direcciones MAC.*

Procuraduría Federal de Protección al Ambiente
Comité de Transparencia

RESOLUCIÓN DE COMITÉ DE INFORMACIÓN N°: 0015/18
RECURSO DE REVISIÓN INAI RRA 4856/18
SOLICITUD DE INFORMACIÓN N°: 1613100050218

- Seguimiento del dispositivo: Como son únicas, las direcciones MAC se pueden usar como medio de rastreo.

Una vez que el atacante ha obtenido algún acceso a través de la materialización de una vulnerabilidad convertida en un ataque (por ejemplo, MAC Spoofing), éste tiene como prioridad mantener el acceso en los dispositivos afectados e incluso migrar el ataque a otros elementos conectados a la red. Las actividades en este punto son variadas, con los recursos puede lanzar nuevos ataques a otros sistemas, obtener o colocar algún archivo, afectar las aplicaciones instaladas o modificar información o archivos.

Por lo anterior, es importante que dicha información se encuentra reservada por el lapso de 5 años, ya que otorgar pone en riesgo la integridad de la información de la Institución.

- V. Que el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales en la resolución del recurso de revisión RRA 4856/18 manifestó en el análisis de la reserva de información establecida en la fracción VII del artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública, entre otros, los siguientes argumentos:

"...de las manifestaciones vertidas por el sujeto obligado, se desprende en esencia, que busca prevenir la comisión de un delito de carácter cibernético, pues de divulgarse los servidores DNS instalados en sus equipos de cómputo, podrían sufrir diversos tipos de ataques (Ataque DDoS, Typosquatting, Intoxicar la caché); ya que su único propósito es salvaguardar la operación de la red de PROFEPA, así como la integridad de su información.

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 impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Ahora bien, con base en la opinión que emitió la Dirección General de Tecnologías de la Información de este Instituto en el diverso recurso de revisión RRA 3342/18, vertida 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, modelo de los módems, ruteadores y puntos de acceso inalámbrico, puede ocasionar intrusiones, robo de identidad, afectación en las comunicaciones y por ende un ataque cibernético a los equipos de cómputo que se encuentren conectados en la red interna, como lo sería para la Procuraduría Federal de Protección al Ambiente.

De esta forma, con la publicidad de dichos datos se generaría un riesgo potencial para la infraestructura tecnológica del referido sujeto obligado, quien busca salvaguardar la operación de la red de Procuraduría Federal de Protección al Ambiente, así como la integridad de su información.

Además, se podrían afectar vulnerabilidades del equipo aún desconocidas por el mismo fabricante, de los dispositivos 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.)

Así, de conformidad con el artículo 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, en concatenación con el diverso 104 de la Ley General de la materia, este Instituto considera que la entrega de la información relativa a los Servidores DNS (Domain Name System) utilizados para el acceso a internet en los equipos de cómputo en posesión del sujeto obligado (punto 5 de la solicitud), ocasionaría una ventana de vulnerabilidad para los equipos y la red de la Procuraduría Federal de Protección al Ambiente, exponiéndolos a un ataque informático, lo que a su vez, provocaría un daño a la información de dicha Procuraduría.

En esa tónica, derivado de la naturaleza y el grado de especificidad del tipo de información que se requiere, pues 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

**Procuraduría Federal de Protección al Ambiente
Comité de Transparencia**

**RESOLUCIÓN DE COMITÉ DE INFORMACIÓN N°: 0015/18
RECURSO DE REVISIÓN INAI RRA 4856/18
SOLICITUD DE INFORMACIÓN N°: 1613100050218**

perturben el sistema de la infraestructura tecnológica de la Procuraduría Federal de Protección al Ambiente, o bien, ejecuten ataques cibernéticos, pues conociendo la IP de los servidores se podría acceder fácilmente a los equipos de cómputo.

En conclusión, la Procuraduría Federal de Protección al Ambiente debió clasificar como reservada la información concerniente a los Servidores DNS (Domain Name System) utilizados para el acceso a internet en los equipos de cómputo que tiene en su posesión, de conformidad con el artículo 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública, así como cumplir con su respectiva prueba de daño, toda vez que, de darse a conocer dicha información a terceras personas, generaría un riesgo potencial de recibir algún ataque informático o cibernético.

Ahora bien, en relación con el periodo de reserva, el segundo párrafo del artículo 99 de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el Trigésimo Cuarto de los Lineamientos Generales, disponen que la información clasificada podrá permanecer con tal carácter hasta por un periodo de cinco años.

En relación con lo anterior, el artículo 100 de la Ley Federal de la materia, establece la obligación de determinar un periodo de reserva considerando el periodo máximo de la misma.

Así, en el caso concreto, este Instituto considera pertinente que el sujeto obligado señale un periodo de reserva de cinco años, pues dicho plazo es proporcional a la naturaleza y el grado de especificidad del tipo de información de que se trata.

...

*En tales consideraciones, el recurso de revisión interpuesto por el particular sólo resulta **fundado de manera parcial**, pues si bien la información identificada con el numeral 9 (segunda parte), no debió decretar su inexistencia, sino protegerla como información reservada, en términos de la fracción VII del artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública, conforme a lo argumentado en el dato relativo a los Servidores DNS (Domain Name System) utilizados para el acceso a internet, analizado anteriormente.*

*Toda vez que, como se refirió anteriormente, se trata de información relevante al ponderar cualquier posible vulneración a la seguridad de la infraestructura tecnológica de la autoridad obligada, por lo que darse a conocer la misma facilitaría que personas expertas en informática **perturben el sistema de la infraestructura tecnológica de la Procuraduría Federal de Protección al Ambiente.***

*En conclusión, la Procuraduría Federal de Protección al Ambiente debió clasificar como reservada la **dirección MAC** (por sus siglas en inglés Media Access Control) **de cada tarjeta o adaptador de red** (wifi, bluetooth, ethernet) de la que disponga cada equipo de cómputo que tenga en posesión, de conformidad con el artículo 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública, así como cumplir con su respectiva prueba de daño, toda vez que, de darse a conocer dicha información a terceras personas, generaría un riesgo potencial de recibir algún ataque informático o cibernético.*

*Dicha información debe resguardarse por periodo de reserva de **cinco años**, de conformidad con lo señalado en el artículo 100 de la Ley Federal de la materia.*

Por lo anterior, este Comité estima procedente la reserva de la información señalada en el Antecedente IX, en virtud de que se actualiza el supuesto previsto en el artículo 110, fracción VII de la LFTAIP.

- VI. Que de conformidad con lo ordenado en el artículo 101, segundo párrafo de la LGTAIP y el artículo 99, segundo párrafo de la LFTAIP, la información clasificada como reservada, podrá permanecer con tal carácter hasta por un periodo de cinco años. Adicionalmente, el lineamiento Trigésimo cuarto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, señala que los titulares de las áreas deberán determinar que el plazo de reserva sea el estrictamente necesario para proteger la información mientras subsistan las causas que dieron origen a la clasificación, salvaguardando el interés público protegido y tomarán en cuenta las razones que justifican el

**Procuraduría Federal de Protección al Ambiente
Comité de Transparencia**

**RESOLUCIÓN DE COMITÉ DE INFORMACIÓN N°: 0015/18
RECURSO DE REVISIÓN INAI RRA 4856/18
SOLICITUD DE INFORMACIÓN N°: 1613100050218**

periodo de reserva establecido. Asimismo, deberán señalar las razones por las cuales se estableció el plazo de reserva determinado.

Con base en lo expuesto en los Considerandos que anteceden, este Comité de Transparencia analizó la clasificación de la información referida en el Antecedente VII, lo anterior, con fundamento en lo dispuesto en los artículos 99 y 110, fracción VII de la LFTAIP, 102, 104 y 113, fracción VII de la LGTAIP; en correlación con los Lineamientos 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, por lo que se emiten los siguientes:

RESOLUTIVOS

PRIMERO.- Se **confirma** la clasificación de la **información reservada** la relacionada con los Servidores DNS (Domain Name System) utilizados para el acceso a internet y la dirección MAC (por sus siglas en ingles Media Access Control) de cada tarjeta o adaptador de red (wifi, bluetooth, ethernet) de cada equipo de cómputo con que cuenta esta Procuraduría Federal de Protección al Ambiente, de conformidad con lo expuesto en la parte Considerativa de la presente Resolución, por el periodo de cinco años, lo anterior con fundamento en los artículos 113, fracción VII y 101 de la LGTAIP; 110, fracción VII y 99 de la LFTAIP.

SEGUNDO.- Se instruye a la Unidad de Transparencia de la PROFEPA para notificar la presente Resolución a la Dirección General Adjunta de Evaluación e Informática, así como al Recurrente y al INAI como parte del Cumplimiento a la Resolución del Recurso de Revisión RRA 4856/18.

Así lo resolvió el Comité de Transparencia de la PROFEPA, el 08 de octubre de 2018.


LIC. JORGE ALBERTO VALENCIA SANDOVAL
Coordinador de Archivos de la Procuraduría
Federal de Protección al Ambiente


MTRA. LUZ MARÍA GARCÍA RANGEL
Suplente del Titular del Órgano Interno de Control en la Secretaría
de Medio Ambiente y Recursos Naturales, en el Comité de Transparencia
de la Procuraduría Federal de Protección al Ambiente


LIC. ELVIRA DEL CARMEN YÁÑEZ OROPEZA
Titular de la Unidad de Transparencia de la
Procuraduría Federal de Protección al Ambiente