Exp. RRA 8206/18
Folio número 1816400228518

ACTA DE LA PRIMERA SESIÓN EXTRAORDINARIA DEL COMITÉ DE TRANSPARENCIA DE LA COMISIÓN FEDERAL DE ELECTRICIDAD, CELEBRADA EL 16 DE ENERO DE 2019.

En la Ciudad de México, siendo las diez horas con diez minutos del miércoles dieciséis de enero del año dos mil diecinueve, se reunió el Comité de Transparencia de la propia Comisión, para celebrar su Primera Sesión Extraordinaria del año dos mil diecinueve.

En su carácter de integrantes del Comité asistió el Lic. Gustavo Sánchez Moreno, Coordinador de Proyectos Especiales y Racionalización de Activos de CFE, en suplencia Mtra. Martha Laura Bolívar Meza, Directora Corporativa de Administración y Presidenta del Comité de Transparencia; la Mtra. Gabriela Alejandra Baca Pérez de Tejada, Titular de la Unidad de Transparencia y el C. Carlos Alberto Peña Álvarez, Responsable del Área Coordinadora de Archivos.

El 20 de noviembre de 2018, a través del Sistema de Comunicación del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), se notificó el recurso de revisión correspondiente al expediente RRA 8206/18, respecto de la solicitud de información folio 1816400228518, en la que solicitaban:

ANTECEDENTES

I. De acuerdo con la solicitud 1816400228518, la información solicitada fue la siguiente:

(Transcripción original) *"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)*

II. La respuesta que la CFE dio a dicha solicitud fue:

(Transcripción original) *"Se elabora la presente constancia, y se transcribe la respuesta aprobada por el Comité de Transparencia; la cual fue proporcionada por el área competente de la* ***Dirección Corporativa de Administración*** *de esta Comisión.*

"En atención a su solicitud, se comunica que la información requerida es clasificada de acuerdo a los siguientes fundamentos y consideraciones:

La configuración de red que se encuentra vigente, el direccionamiento IP interno que se encuentra en uso, reglas y configuraciones de los equipos de seguridad, sistemas, versiones (Sistema Operativo, Programas y Aplicaciones), Inventario de activos de TIC' de la estrategia de seguridad de la información, Inventario de hardware (números de serie), que contiene información sobre: (BIOS, Procesadores, marca y modelo), Inventario de software, configuraciones de red (WPS, WIFI, WEP, WPA2, etc.), planes de continuidad de negocio, planes de recuperación de desastres (RMA). Los diagramas y textos relativos a la arquitectura de seguridad, configuración técnica, memorias técnicas, soporte preventivo, soporte correctivo, procedimientos, guías, estándares y plataformas tecnológicas), es información clasificada como RESERVADA y CONFIDENCIAL toda vez que el conocimiento de este diseño, configuración, programas de actualización, mantenimiento, procesos correctivos, revisiones, planes, contratos, anexos, diagramas, monitoreo de las redes de datos, inventario de equipos, su configuración y demás información relacionada con la seguridad de la información, puede poner en riesgo la operación total de las redes de voz y datos de la CFE ya que expone vulnerabilidades conocidas y no conocidas.

Estos "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 y "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), son clasificados como información reservada por su naturaleza, ya que ésta puede ser utilizada para estructurar y ejecutar un ataque cibernético que pudiera poner en riesgo sistemas críticos y sustantivos de la CFE, toda vez que estos permiten identificar la estrategia de protección que se está utilizando para la seguridad de los sistemas administrativos, comerciales y de comunicación de la empresa, por lo que resulta altamente probable que la difusión de esta información, pudiera facilitar información a terceros no autorizados sobre vulnerabilidades que estén presentes en los sistemas administrativos y comerciales de la CFE, afectando la continuidad operativa de la CFE y esta pueda ser utilizada con fines de ejecutar un ataque informático que pondría en riesgo la infraestructura de cómputo, así como la información digital que se encuentra en los servidores de la CFE y sus Empresas Productivas Subsidiarias por lo que consideramos que esta información debe ser clasificada como reservada, toda vez que la relación de información solicitada puede ser correlacionada para identificar códigos maliciosos o programas que permitan llevar a cabo un ataque dirigido hacia los sistemas informáticos de la CFE vulnerando la red eléctrica nacional.

Los "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 y "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), constituyen el inventario de activos de TIC de la CFE, asimismo su configuración es parte fundamental de la protección que la CFE dispone para la protección de los sistemas comerciales y administrativos de la CFE y en estos se mantiene información confidencial de nuestros clientes, así como información comercial que representa ventajas competitivas a la CFE en el mercado, la información sobre "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 y "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) debe mantenerse como reservada por formar parte de la estrategia de seguridad de la información que la CFE dispone para la protección de las instalaciones y secretos comerciales con fundamento con los artículos 113 fracciones I y II de la Ley Federal de Transparencia y Acceso a la Información Pública. Ya que el acceso a esta información podría vulnerar la estrategia de protección de los sistemas comerciales y administrativos, así como su información confidencial, al poner de conocimiento de terceros no autorizados información sobre los controles de protección de la información.

Por las razones expuestas, se considera que los rubros requeridos como los "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 y "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) son información CLASIFICADA como RESERVADA y CONFIDENCIAL dado que la divulgación de la información:

- *Permitiría el acceso ilícito a sus sistemas y equipos informáticos, intentando la suplantación de los mismos;*
- *Potenciaría la posibilidad de vulnerar la seguridad de su infraestructura tecnológica;*
- *Establecería con un alto grado de precisión la información técnica referente a sus equipos de cómputo y su forma de identificación en la red, la forma y el medio de conexión, los protocolos de seguridad y las características de la infraestructura instalada;*
- *Pondría en un estado vulnerable a la institución, facilitando la intervención de las comunicaciones y permitiendo usurpar permisos requeridos en la red para obtener información;*
- *Daría a conocer puntos de vulnerabilidad para la seguridad de la infraestructura de cómputo;*
- *Revelaría aspectos específicos de la operación y funcionamiento de su infraestructura tecnológica;*
- *Vulneraría sus sistemas informáticos, así como la información contenida en éstos;*
- *Atentaría en contra de su infraestructura tecnológica, afectando el ejercicio de sus labores sustantivas; y*
- *Modificaría, destruiría o provocaría pérdida de información contenida en sus equipos de cómputo y sistemas.*

La negativa de acceso a la información se motiva en pretender evitar o prevenir la comisión del delito de acceso ilícito a sus equipos y sistemas de informática.

Al respecto, el Código Penal Federal dispone lo siguiente:

Acceso ilícito a sistemas y equipos de informática

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.

De la normatividad señalada se advierte que comente 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.

Aunado a lo anterior, con la publicidad de dichos datos se generaría un riesgo potencial para la infraestructura tecnológica de esta Comisión Federal de Electricidad, ya que pueden ser utilizadas para propiciar ataques informáticos de diversa índole.

Asimismo, con la entrega de los datos que se solicitan, además de causar un riesgo a un ataque cibernético, se afectarían los registros, licencias y garantías de los mismos, derivados del robo de identidad.

Se solicita la reserva toda vez que la entrega de "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 y "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), podría ocasionar lo siguiente:

I. Un potencial riesgo real, demostrable e identificable a esta Comisión Federal de Electricidad toda vez que se le colocaría en un estado de vulnerabilidad que permitiría el acceso ilícito a sus sistemas y equipos informáticos, facilitando:

a. Una posible intervención de sus comunicaciones,

b. La usurpación de sus permisos,

c. La suplantación de sus equipos y de la información que almacena en sus servidores;

d. El robo de la información que obra en sus archivos digitales, y

e. El detrimento de sus instalaciones tecnológicas.

Cuestiones que se materializan con la comisión de delitos de carácter cibernético, que sin duda afectarían severamente el ejercicio de las labores cotidianas y sustantivas.

II. Un perjuicio significativo al interés público, toda vez que la CFE es una empresa productiva del Estado, de propiedad exclusiva del Gobierno Federal, encargada de prestar el servicio público de transmisión y distribución de energía eléctrica, por cuenta y orden del Estado Mexicano, por lo que si la infraestructura tecnológica fuera vulnerada mediante un ataque a sus sistemas y equipos, se podrían revelar aspectos específicos de su operación y labores sustantivas; asimismo, se podría modificar, destruir o provocar la pérdida de información toral para el desarrollo de sus funciones.

Con base en lo anterior, el riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda la información, ya que el resguardo de los datos requeridos por el solicitante implica la prevención del delito de acceso ilícito a sistemas y equipos de informática tipificado en el Código Penal Federal, lo cual cobra importancia si se considera que dicha conducta implica conocer, copiar, modificar, destruir o provocar la pérdida de información contenida en sistemas o equipos de informática.

Asimismo, la limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir la conducta antijurídica tipificada (acceso ilícito a sistemas y equipos de informática), misma que de llevarse a cabo podría permitir la realización de diversos ataques a la infraestructura tecnológica y de sistemas del sujeto obligado, los cuales podrían traer como consecuencia la inoperatividad de sus funciones, por un periodo indeterminado.

Por todo lo anterior, se advierte que difundir la información requerida 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 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 esta empresa, es que se colige que dar a conocer la misma facilitaría que personas expertas en informática perturben el sistema de la infraestructura tecnológica de esta Comisión Federal de Electricidad, 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 y permitiendo usurpar permisos requeridos en la red para obtener información.

Por lo anterior, se solicita que los "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 y "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), se considere información reservada, de conformidad con lo dispuesto en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, ello por un periodo de 5 años.
1. Reservada. Por seguridad de las instalaciones y por secreto comercial con fundamento en los artículos 110 fracciones I y IV (último supuesto normativo) de la LFTAIP y artículo 113 fracciones I y IV (último supuesto normativo) de la LGTAIP.
2. Confidencial. Por secreto comercial con fundamento en el artículo 113 fracción II de la LFTAIP con relación al artículo 82 de la Ley de Propiedad Industrial.
Fecha de clasificación: 29 de octubre de 2018.
Periodo de Reserva: 5 años." (Sic)

III. El 12 de noviembre de 2018 el Instituto recibió por parte del recurrente, la impugnación de la respuesta antes citada, en los siguientes términos:

(Transcripción original) "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 menester evocar 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.
...
La información peticionada en el inciso c) de la solicitud 1816400228518 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 1816400228518 pusieran en riesgo la seguridad informática implementada por el sujeto obligado; el Servicio de Administración Tributaria (SAT), el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE), el Instituto Nacional de las Mujeres, el Instituto Federal de Telecomunicaciones (IFT), la Auditoria Superior de la Federación (ASF), las Secretarias de Comunicaciones y Transportes (SCT), de Energía (SENER), de Agricultura, Ganadería, Desarrollo Rural, Pesca y Alimentación (SAGARPA), de Desarrollo Agrario, Territorial y Urbano (SEDATU), del Trabajo y Previsión Social (STPS), 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, 0063700544518, 0610400019618, 0912100054218, 0110000049118, 0000900168418, 0001800080118, 0000800304018, 0001400083818, 0001500096918, 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 es 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 1816400228518 no actualiza algún supuesto de reservada o confidencialidad previsto en la Ley Federal y en la Ley General.
AGRAVIO SEGUNDO.- Falta de notificación de la Resolución del Comité de Transparencia, por la cual se clasifico 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.
...
AGRAVIO TERCERO.- Violación a los principios de máxima publicidad, exhaustividad y congruencia.
ARTÍCULOS TRANSGREDIDOS: *6° DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS,* ***1°, 4°, 11 Y 12*** *DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA,* ***3° y 59*** *DE LA LEY FEDERAL DE PROCEDIMIENTO ADMINISTRATIVO,* ***DE APLICACIÓN SUPLETORIA, 1°, 3°, 7° y 133*** *DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA.*

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; mientras que el principio de congruencia garantiza que los sujetos obligados emitan respuestas en concordancia a lo requerido.
...
Respecto del principio de máxima publicidad enunciado en los artículos 11 y 12 de la Ley General, recomendamos remitirse a lo argumentado en el agravio primero del presente recurso.
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 de información incompleta; lo anterior toda vez que hace falta lo precisado en los incisos a), b) y d) de la solicitud 1816400228518.
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 y confidencialidad de la información precisada en la solicitud de información pública número 1816400228518.*
...
***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)*

IV. Ante lo que la Dirección Corporativa de Administración informó lo siguiente:

(Transcripción original)** "Se solicita la clasificación como reservada de la información relativa a "...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), de conformidad con la fracción **VII del artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública, por un periodo de 5 años.

- *Dado que la divulgación de la información:*
- *Permitiría el acceso ilícito a sus sistemas y equipos informáticos, intentando la suplantación de los mismos;*
- *Potenciaría la posibilidad de vulnerar la seguridad de su infraestructura tecnológica;*
- *Establecería con un alto grado de precisión la información técnica referente a sus equipos de cómputo y su forma de identificación en la red, la forma y el medio de conexión, los protocolos de seguridad y las características de la infraestructura instalada;*
- *Pondría en un estado vulnerable a la institución, facilitando la intervención de las comunicaciones y permitiendo usurpar permisos requeridos en la red para obtener información;*
- *Daría a conocer puntos de vulnerabilidad para la seguridad de la infraestructura de cómputo;*
- *Revelaría aspectos específicos de la operación y funcionamiento de su infraestructura tecnológica;*
- *Vulneraría sus sistemas informáticos, así como la información contenida en éstos;*
- *Atentaría en contra de su infraestructura tecnológica, afectando el ejercicio de sus labores sustantivas; y*
- *Modificaría, destruiría o provocaría pérdida de información contenida en sus equipos de cómputo y sistemas.*

*Se advierte la negativa de acceso a la información se motiva en pretender **evitar o prevenir la comisión del delito de acceso ilícito a sus equipos y sistemas de informática**.*
Al respecto, el Código Penal Federal dispone lo siguiente:

Acceso ilícito a sistemas y equipos de informática

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.*

De la normatividad señalada se advierte que comente 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, para reafirmar lo anterior, la Ponencia que sustanció la presente resolución realizó un requerimiento de información adicional a la Dirección General de Tecnologías de la Información concluyendo que con la ***publicidad de dichos datos se generaría un riesgo potencial para la infraestructura tecnológica de esta Comisión Federal de Electricidad****, ya que pueden ser utilizadas para propiciar* ***ataques informáticos de diversa índole****.*

Asimismo, se advirtió que con la entrega de los datos que se analizan, además de causar un riesgo a un ataque cibernético, se afectarían los registros, licencias y garantías de los mismos, derivados del robo de identidad.

Así, la entrega del conjunto de datos informáticos requeridos, podría ocasionar lo siguiente:

I. *Un potencial* ***riesgo real, demostrable e identificable*** *a esta Comisión Federal de Electricidad toda vez que se le colocaría en un estado de* ***vulnerabilidad*** *que permitiría el acceso ilícito a sus sistemas y equipos informáticos, facilitando:*

a*. Una posible intervención de sus comunicaciones,*

b. La usurpación de sus permisos,

c. *La suplantación de sus equipos y de la información que almacena en sus servidores;*

d. El robo de la información que obra en sus archivos digitales, y

e. El detrimento de sus instalaciones tecnológicas.

Cuestiones que se materializan con la comisión de delitos de carácter cibernético, que sin duda afectarían severamente el ejercicio de las labores cotidianas y sustantivas.

II. *Un* ***perjuicio significativo al interés público****, ya que el sujeto obligado es una empresa productiva del Estado, de propiedad exclusiva del Gobierno Federal, encargada de prestar el servicio público de transmisión y distribución de energía eléctrica, por cuenta y orden del Estado Mexicano, por lo que si la infraestructura tecnológica fuera vulnerada mediante un ataque a sus sistemas y equipos, se podrían revelar aspectos específicos de su operación y labores sustantivas; asimismo, se podría modificar, destruir o provocar la pérdida de información toral para el desarrollo de sus funciones.*

Con base en lo anterior, ***el riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda la información****, ya que el resguardo de los datos requeridos por el solicitante implica la* ***prevención del delito de acceso ilícito a sistemas y equipos de informática tipificado en el Código Penal Federal****, lo cual cobra importancia si se considera que dicha conducta implica conocer, copiar, modificar, destruir o provocar la pérdida de información contenida en sistemas o equipos de informática.*

Asimismo, la ***limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio****, toda vez que* ***la pretensión de fondo que persigue la reserva de la información consiste en prevenir la conducta antijurídica tipificada*** *(acceso ilícito a sistemas y equipos de informática), misma que de llevarse a cabo podría permitir la realización de diversos* ***ataques*** *a la infraestructura tecnológica y de sistemas del sujeto obligado, los cuales podrían traer como consecuencia la* ***inoperatividad*** *de sus funciones, por un periodo indeterminado.*

Por todo lo anterior, se advierte que ***difundir*** *la información requerida* ***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 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 ***perturben el sistema de la infraestructura tecnológica*** *de esta Comisión Federal de Electricidad, 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 y permitiendo usurpar permisos requeridos en la red para obtener información; resultando, por lo tanto,* ***procedente su reserva****, de conformidad con el precepto jurídico que se analiza.*

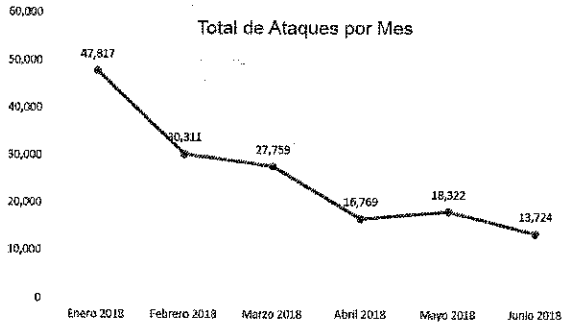
Por lo anterior informado, se concluye que la información relativa a: "1. Ordenado por Número de serie, de cada uno de los equipos de cómputo y de cada uno de los MODEMS, ROUTERS (rúters) o Puntos de acceso inalámbricos, en posesión del sujeto obligado. a. Nombre de aquellas personas físicas que cuentan 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, se considera información ***reservada,*** *de conformidad con lo dispuesto en el artículo* ***110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, ello por un periodo de 5 años.***

CONSIDERANDO

PRIMERO.- Los integrantes del Comité de Transparencia de la CFE, son competentes en términos de lo establecido en el artículo 65, fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública, publicada en el Diario Oficial de la Federación el nueve de mayo de dos mil dieciséis, para: confirmar la clasificación como reservada.

SEGUNDO.- Este Comité de Transparencia confirma la reserva de la información. Al mismo tiempo los miembros precisan que la clasificación atiende al hecho de que el proporcionar de forma asociada los números de serie, las marcas y la ubicación de las terminales de cómputo permite que el poseedor de dichos datos, a través de las empresas fabricantes, obtengan información técnica más detallada de cada una de ellas, lo que vulnera su seguridad y contenido.

Adicionalmente, la Titular de la Unidad de Transparencia recordó a los miembros del Comité que en el periodo de enero a junio de 2018, se registraron las siguientes cifras en ataques a la ciberseguridad de CFE.



Gráfica 2 Total de Ataques por Mes

Información de la que se tomó conocimiento pues corresponde a la respuesta proporcionada a la solicitud de información pública identificada con el número de folio 1816400154018.

RESUELVE

PRIMERO.- Con fundamento en el artículo 65, fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública, se confirma la reserva de *"...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),* ello de conformidad con lo dispuesto en el artículo **110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, ello por un periodo de 5 años.**

SEGUNDO.- Se precisa que la clasificación como reservada fue solicitada por la Dirección Corporativa de Administración.

No habiendo otro asunto que tratar, se dio por terminada la reunión, siendo las once horas con cuarenta y cinco minutos del día de su fecha, rubricando cada hoja y firmando al calce, para constancia, los asistentes a la reunión.

Comité de Transparencia de la CFE

Lic. Gustavo Sánchez Moreno
Coordinador de Proyectos Especiales y Racionalización de Activos de CFE, en suplencia de la Presidenta del Comité

Mtra. Gabriela Alejandra Baca Pérez de Tejada
Titular de la Unidad de Transparencia

C. Carlos Alberto Peña Álvarez
Responsable del Área Coordinadora de Archivos.