

Exp. RRA 3632/18
Folio número 1816400098118**ACTA DE LA DÉCIMA SÉPTIMA SESIÓN EXTRAORDINARIA DEL COMITÉ DE TRANSPARENCIA DE LA COMISIÓN FEDERAL DE ELECTRICIDAD, CELEBRADA EL LUNES 13 DE AGOSTO DE 2018.**

En la Ciudad de México, siendo las doce horas con quince minutos del lunes trece de agosto del año dos mil dieciocho, se reunió el Comité de Transparencia de la propia Comisión, para celebrar su Décima Séptima Sesión Extraordinaria del año dos mil dieciocho.

En su carácter de integrantes del Comité asistió el Lic. Jesús Manuel Ponce Salas, por instrucciones del Mtro. Diódoro J. Siller Argüello, Coordinador de Proyectos Especiales y Racionalización de Activos de CFE, en suplencia de Héctor De la Cruz, Director Corporativo de Administración y Presidente 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 03 de agosto 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 3632/18, respecto de la solicitud de información folio 1816400098118, en la que solicitaban:

ANTECEDENTES**I. De acuerdo con la solicitud 1816400098118, 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. De cada uno de los equipos de cómputo en posesión del sujeto obligado: a. Número de serie y de parte. b. Versión de la BIOS (siglas en inglés de Basic Input/Output System). c. Marca. d. Si se cuenta con contraseña para acceder a la configuración de la BIOS (siglas en inglés de Basic Input/Output System). e. Procesador. f. Capacidad de almacenamiento en el Disco Duro. g. Conforme al organigrama estructural, unidad, área u órgano que hace uso del equipo de cómputo." (Sig)

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

(Transcripción original) **Dirección General**

En atención a su solicitud, se informa lo siguiente:

Nos permitimos informar que los detalles a este nivel de segregación y vinculados por virtud de los datos requeridos, conforman los Diagramas de red que se encuentran vigentes, 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 que contiene información sobre: (BIOS, MAC ADDRESS, Procesadores, número de serie y marca), Inventario de software, 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 y estándares y Plataformas, tecnologías), 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 y su configuración y demás información relacionada con la seguridad de la información puede poner en riesgo la operación total de la red de voz y datos de la CFE ya que expone vulnerabilidades conocidas y no conocidas.

La información respecto a las configuraciones de los equipos de cómputo de escritorio y servidores (BIOS, MAC ADDRESS, procesadores, números de serie y marca) es información reservada por su naturaleza, ya que esta puede ser utilizada para estructurar y ejecutar un ataque cibernético que pudiera poner en riesgo sistemas críticos y sustantivos de la CFE, como son los sistemas de operación vinculados al sistema eléctrico nacional.

Al existir sistemas que por razones de operación requieren mantener cierta versión de BIOS, MAC ADDRESS, procesador, esta información puede ser utilizada para identificar vulnerabilidades o debilidades de equipos de cómputo y a partir de ahí afectar maliciosamente la operación de sistemas críticos o sustantivos.

De darse a conocer la información de los detalles técnicos de los equipos de cómputo, pondría en riesgo la operación de los equipos de cómputo y servidores de la CFE ya que podrían exponer vulnerabilidades conocidas y no conocidas. Además de que resulta altamente probable que la difusión de la información contenida en la información solicitada, pudiera afectar la seguridad de la red de voz, datos y sistemas informáticos de la Dirección General de CFE y por tanto, la continuidad de las actividades relativas a garantizar la operación de los sistemas internos de la Dirección General de CFE, adicionalmente la protección a los sistemas que controlan las redes eléctricas y así poder garantizar la operación del sistema eléctrico nacional, toda vez que la seguridad perimetral esta para evitar cualquier tipo de amenazas internas y externas.

A mayor abundamiento, los datos requeridos, por su naturaleza estructurada, no pueden ser proporcionados ya que se tendría un alto riesgo al ser utilizado 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 esta información debe ser clasificada como reservada, en virtud que la relación de información solicitada puede ser correlacionada para identificar el código malicioso o programa específico que permita llevar a cabo un ataque dirigido hacia los sistemas informáticos de la CFE, y de esta manera vulnerar la red eléctrica nacional. Tener esta información vinculada permite identificar específicamente si el equipo de cómputo presenta alguna vulnerabilidad de hardware y cómo explotarla con base a la información específica de los procesadores instalados en los equipos. Las investigaciones en materia de ciberseguridad han identificado vulnerabilidades de la arquitectura de procesadores de ciertas marcas que podrían ser explotadas con fines maliciosos.

Algunos de estos datos, consisten en identificadores únicos que se les asigna a las interfaces de redes. Las tarjetas de red inalámbrica o las de red Ethernet, los módems, los routers, las impresoras, etc., todos tienen un identificador propio de 48 bits que no se repite en todo el mundo, es como su propia huella digital para poder comunicarse. Por tanto, dicha situación genera que en una red informática los equipos puedan ser identificados de esta manera además de poderse hacer a través de la dirección IP. En este sentido los datos requeridos son elementos importantes de la vida digital de los dispositivos ya que permite un nivel muy elevado de identificación de los equipos.

Por las razones expuestas, se considera que los datos requeridos son información CLASIFICADA como RESERVADA y CONFIDENCIAL con fundamento en:

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: 11 de abril de 2018.

Periodo de Reserva: 5 años

Coordinación de Comunicación Corporativa

En atención a la solicitud de información, esta unidad administrativa hace de su conocimiento lo siguiente:

Nos permitimos informar que los detalles a este nivel de segregación y vinculados por virtud de los datos requeridos, conforman los Diagramas de red que se encuentran vigentes, 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 que contiene información sobre: (BIOS, MAC ADDRESS, Procesadores, número de serie y marca), Inventario de software, 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 y estándares y Plataformas, tecnologías), 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 y su configuración y demás información relacionada con la seguridad de la información puede poner en riesgo la operación total de la redes de voz y datos de la CFE ya que expone vulnerabilidades conocidas y no conocidas.

La información respecto a las configuraciones de los equipos de cómputo de escritorio y servidores (BIOS, MAC ADDRESS, procesadores, números de serie y marca) es información reservada por su naturaleza, ya que esta puede

ser utilizada para estructurar y ejecutar un ataque cibernético que pudiera poner en riesgo sistemas críticos y sustantivos de la CFE, como son los sistemas de operación vinculados al sistema eléctrico nacional.

Al existir sistemas que por razones de operación requieren mantener cierta versión de BIOS, MAC ADDRESS, procesador, esta información puede ser utilizada para identificar vulnerabilidades o debilidades de equipos de cómputo y a partir de ahí afectar maliciosamente la operación de sistemas críticos o sustantivos.

De darse a conocer la información de los detalles técnicos de los equipos de cómputo, pondría en riesgo la operación de los equipos de cómputo y servidores de la CFE ya que podrían exponer vulnerabilidades conocidas y no conocidas. Además de que resulta altamente probable que la difusión de la información contenida en la información solicitada, pudiera afectar la seguridad de la red de voz, datos y sistemas informáticos de la Coordinación de Comunicación Corporativa de CFE y por tanto, la continuidad de las actividades relativas a garantizar la operación de los sistemas internos de la Coordinación de Comunicación Corporativa de CFE, adicionalmente la protección a los sistemas que controlan las redes eléctricas y así poder garantizar la operación del sistema eléctrico nacional, toda vez que la seguridad perimetral esta para evitar cualquier tipo de amenazas internas y externas.

A mayor abundamiento, los datos requeridos, por su naturaleza estructurada, no pueden ser proporcionados ya que se tendría un alto riesgo al ser utilizado 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 esta información debe ser clasificada como reservada, en virtud que la relación de información solicitada puede ser correlacionada para identificar el código malicioso o programa específico que permita llevar a cabo un ataque dirigido hacia los sistemas informáticos de la CFE, y de esta manera vulnerar la red eléctrica nacional. Tener esta información vinculada permite identificar específicamente si el equipo de cómputo presenta alguna vulnerabilidad de hardware y cómo explotarla con base a la información específica de los procesadores instalados en los equipos. Las investigaciones en materia de ciberseguridad han identificado vulnerabilidades de la arquitectura de procesadores de ciertas marcas que podrían ser explotadas con fines maliciosos.

Algunos de estos datos, consisten en identificadores únicos que se les asigna a las interfaces de redes. Las tarjetas de red inalámbrica o las de red Ethernet, los módems, los routers, las impresoras, etc., todos tienen un identificador propio de 48 bits que no se repite en todo el mundo, es como su propia huella digital para poder comunicarse. Por tanto, dicha situación genera que en una red informática los equipos puedan ser identificados de esta manera además de poderse hacer a través de la dirección IP. En este sentido los datos requeridos son elementos importantes de la vida digital de los dispositivos ya que permite un nivel muy elevado de identificación de los equipos.

Por las razones expuestas, se considera que los datos requeridos son información CLASIFICADA como RESERVADA y CONFIDENCIAL con fundamento en:

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: 11 de abril de 2018.

Periodo de Reserva: 5 años

Auditoría Interna

En atención a la solicitud de acceso a la información pública, se informa lo siguiente:

La Auditoría Interna se ajusta y adhiere a lo manifestado por la Coordinación de Servicios Tecnológicos toda vez que es la instancia oficial para atención y administración de la seguridad de las Tecnologías de Información y Comunicaciones, es decir, a la Red de voz y datos de la CFE. En consecuencia esta área manifiesta que: "...los detalles a este nivel de segregación y vinculados por virtud de los datos requeridos, conforman los Diagramas de red que se encuentran vigentes, 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 que contiene información sobre: (BIOS, MAC ADDRESS, Procesadores, número de serie y marca), Inventario de software, 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 y estándares y Plataformas, tecnologías), 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 y su

configuración y demás información relacionada con la seguridad de la información puede poner en riesgo la operación total de la redes de voz y datos de la CFE ya que expone vulnerabilidades conocidas y no conocidas.

Así mismo, la información respecto a las configuraciones de los equipos de cómputo de escritorio y servidores (BIOS, MAC ADDRESS, procesadores, números de serie y marca) es información reservada por su naturaleza, ya que esta puede ser utilizada para estructurar y ejecutar un ataque cibemético que pudiera poner en riesgo sistemas críticos y sustantivos de la CFE, como son los sistemas de operación vinculados al sistema eléctrico nacional.

Al existir sistemas que por razones de operación requieren mantener cierta versión de BIOS, MAC ADDRESS, procesador, esta información puede ser utilizada para identificar vulnerabilidades o debilidades de equipos de cómputo y a partir de ahí afectar maliciosamente la operación de sistemas críticos o sustantivos.

De darse a conocer la información de los detalles técnicos de los equipos de cómputo, pondría en riesgo la operación de los equipos de cómputo y servidores de la CFE ya que podrían exponer vulnerabilidades conocidas y no conocidas. Además de que resulta altamente probable que la difusión de la información contenida en la información solicitada, pudiera afectar la seguridad de la red de voz, datos y sistemas informáticos de la Auditoría Interna de CFE y por tanto, la continuidad de las actividades relativas a garantizar la operación de los sistemas internos de la Auditoría Interna de CFE, adicionalmente la protección a los sistemas que controlan las redes eléctricas y así poder garantizar la operación del sistema eléctrico nacional, toda vez que la seguridad perimetral esta para evitar cualquier tipo de amenazas internas y externas.

A mayor abundamiento, los datos requeridos, por su naturaleza estructurada, no pueden ser proporcionados ya que se tendría un alto riesgo al ser utilizado 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 esta información debe ser clasificada como reservada, en virtud que la relación de información solicitada puede ser correlacionada para identificar el código malicioso o programa específico que permita llevar a cabo un ataque dirigido hacia los sistemas informáticos de la CFE, y de esta manera vulnerar la red eléctrica nacional. Tener esta información vinculada permite identificar específicamente si el equipo de cómputo presenta alguna vulnerabilidad de hardware y cómo explotarla con base a la información específica de los procesadores instalados en los equipos. Las investigaciones en materia de ciberseguridad han identificado vulnerabilidades de la arquitectura de procesadores de ciertas marcas que podrían ser explotadas con fines maliciosos.

Algunos de estos datos, consisten en identificadores únicos que se les asigna a las interfaces de redes. Las tarjetas de red inalámbrica o las de red Ethernet, los módems, los routers, las impresoras, etc., todos tienen un identificador propio de 48 bits que no se repite en todo el mundo, es como su propia huella digital para poder comunicarse. Por tanto, dicha situación genera que en una red informática los equipos puedan ser identificados de esta manera además de poderse hacer a través de la dirección IP. En este sentido los datos requeridos son elementos importantes de la vida digital de los dispositivos ya que permite un nivel muy elevado de identificación de los equipos.

Por las razones expuestas, se considera que los datos requeridos son información CLASIFICADA como RESERVADA y CONFIDENCIAL con fundamento en:

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: 11 de abril de 2018.

Periodo de Reserva: 5 años"

Dirección Corporativa de Operaciones

En atención a la solicitud de información, la Dirección Corporativa de Operaciones hace de su conocimiento lo siguiente en relación a su requerimiento:

Nos permitimos informar que los detalles a este nivel de segregación y vinculados por virtud de los datos requeridos, conforman los Diagramas de red que se encuentran vigentes, 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 que contiene información sobre: (BIOS, MAC ADDRESS, Procesadores, número de serie y marca), Inventario de software, 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 y estándares y Plataformas, tecnologías), 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 y su configuración y demás información relacionada con la seguridad de la información puede poner en riesgo la operación total de la redes de voz y datos de la CFE ya que expone vulnerabilidades conocidas y no conocidas.

La información respecto a las configuraciones de los equipos de cómputo de escritorio y servidores (BIOS, MAC ADDRESS, procesadores, números de serie y marca) es información reservada por su naturaleza, ya que esta puede ser utilizada para estructurar y ejecutar un ataque cibernético que pudiera poner en riesgo sistemas críticos y sustantivos de la CFE, como son los sistemas de operación vinculados al sistema eléctrico nacional.

Al existir sistemas que por razones de operación requieren mantener cierta versión de BIOS, MAC ADDRESS, procesador, esta información puede ser utilizada para identificar vulnerabilidades o debilidades de equipos de cómputo y a partir de ahí afectar maliciosamente la operación de sistemas críticos o sustantivos.

De darse a conocer la información de los detalles técnicos de los equipos de cómputo, pondría en riesgo la operación de los equipos de cómputo y servidores de la CFE ya que podrían exponer vulnerabilidades conocidas y no conocidas. Además de que resulta altamente probable que la difusión de la información contenida en la información solicitada, pudiera afectar la seguridad de la red de voz, datos y sistemas informáticos de la Dirección Corporativa de Operaciones de CFE y por tanto, la continuidad de las actividades relativas a garantizar la operación de los sistemas internos de la Dirección Corporativa de Operaciones de CFE, adicionalmente la protección a los sistemas que controlan las redes eléctricas y así poder garantizar la operación del sistema eléctrico nacional, toda vez que la seguridad perimetral esta para evitar cualquier tipo de amenazas internas y externas.

A mayor abundamiento, los datos requeridos, por su naturaleza estructurada, no pueden ser proporcionados ya que se tendría un alto riesgo al ser utilizado 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 esta información debe ser clasificada como reservada, en virtud que la relación de información solicitada puede ser correlacionada para identificar el código malicioso o programa específico que permita llevar a cabo un ataque dirigido hacia los sistemas informáticos de la CFE, y de esta manera vulnerar la red eléctrica nacional. Tener esta información vinculada permite identificar específicamente si el equipo de cómputo presenta alguna vulnerabilidad de hardware y cómo explotarla con base a la información específica de los procesadores instalados en los equipos. Las investigaciones en materia de ciberseguridad han identificado vulnerabilidades de la arquitectura de procesadores de ciertas marcas que podrían ser explotadas con fines maliciosos.

Algunos de estos datos, consisten en identificadores únicos que se les asigna a las interfaces de redes. Las tarjetas de red inalámbrica o las de red Ethernet, los módems, los routers, las impresoras, etc., todos tienen un identificador propio de 48 bits que no se repite en todo el mundo, es como su propia huella digital para poder comunicarse. Por tanto, dicha situación genera que en una red informática los equipos puedan ser identificados de esta manera además de poderse hacer a través de la dirección IP. En este sentido los datos requeridos son elementos importantes de la vida digital de los dispositivos ya que permite un nivel muy elevado de identificación de los equipos.

Por las razones expuestas, se considera que los datos requeridos son información CLASIFICADA como RESERVADA y CONFIDENCIAL con fundamento en:

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: 11 de abril de 2018.

Periodo de Reserva: 5 años

Dirección Corporativa de Negocios Comerciales

Estimado solicitante, en atención a su solicitud, la Dirección Corporativa de Negocios Comerciales (DCNC) hace de su conocimiento que la información solicitada se encuentra clasificada, derivado a que los detalles a este nivel de segregación y vinculados por virtud de los datos requeridos, conforman los Diagramas de red que se encuentran vigentes, 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 que contiene información sobre: (BIOS, MAC ADDRESS, Procesadores, número de serie y marca), Inventario de software, 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 y estándares y Plataformas, tecnologías), 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 y su configuración y demás información relacionada con la seguridad de la información puede poner en riesgo la operación total de la redes de voz y datos de la CFE ya que expone vulnerabilidades conocidas y no conocidas.

La información respecto a las configuraciones de los equipos de cómputo de escritorio y servidores (BIOS, MAC ADDRESS, procesadores, números de serie y marca) es información reservada por su naturaleza, ya que esta puede ser utilizada para estructurar y ejecutar un ataque cibernético que pudiera poner en riesgo sistemas críticos y sustantivos de la CFE, como son los sistemas de operación vinculados al sistema eléctrico nacional.

Al existir sistemas que por razones de operación requieren mantener cierta versión de BIOS, MAC ADDRESS, procesador, esta información puede ser utilizada para identificar vulnerabilidades o debilidades de equipos de cómputo y a partir de ahí afectar maliciosamente la operación de sistemas críticos o sustantivos.

De darse a conocer la información de los detalles técnicos de los equipos de cómputo, pondría en riesgo la operación de los equipos de cómputo y servidores de la CFE ya que podrían exponer vulnerabilidades conocidas y no conocidas. Además de que resulta altamente probable que la difusión de la información contenida en la información solicitada, pudiera afectar la seguridad de la red de voz, datos y sistemas informáticos de la Dirección Corporativa de Negocios Comerciales de CFE y por tanto, la continuidad de las actividades relativas a garantizar la operación de los sistemas internos de la Dirección Corporativa de Negocios Comerciales de CFE, adicionalmente la protección a los sistemas que controlan las redes eléctricas y así poder garantizar la operación del sistema eléctrico nacional, toda vez que la seguridad perimetral esta para evitar cualquier tipo de amenazas internas y externas.

A mayor abundamiento, los datos requeridos, por su naturaleza estructurada, no pueden ser proporcionados ya que se tendría un alto riesgo al ser utilizado 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 esta información debe ser clasificada como reservada, en virtud que la relación de información solicitada puede ser correlacionada para identificar el código malicioso o programa específico que permita llevar a cabo un ataque dirigido hacia los sistemas informáticos de la CFE, y de esta manera vulnerar la red eléctrica nacional. Tener esta información vinculada permite identificar específicamente si el equipo de cómputo presenta alguna vulnerabilidad de hardware y cómo explotarla con base a la información específica de los procesadores instalados en los equipos. Las investigaciones en materia de ciberseguridad han identificado vulnerabilidades de la arquitectura de procesadores de ciertas marcas que podrían ser explotadas con fines maliciosos.

Algunos de estos datos, consisten en identificadores únicos que se les asigna a las interfaces de redes. Las tarjetas de red inalámbrica o las de red Ethernet, los módems, los routers, las impresoras, etc., todos tienen un identificador propio de 48 bits que no se repite en todo el mundo, es como su propia huella digital para poder comunicarse. Por tanto, dicha situación genera que en una red informática los equipos puedan ser identificados de esta manera además de poderse hacer a través de la dirección IP. En este sentido los datos requeridos son elementos importantes de la vida digital de los dispositivos ya que permite un nivel muy elevado de identificación de los equipos.

Por las razones expuestas, se considera que los datos requeridos son información CLASIFICADA como RESERVADA y CONFIDENCIAL con fundamento en:

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: 11 de abril de 2018.

Periodo de Reserva: 5 años

Subdirección Corporativa de Estrategia y Regulación

En atención al requerimiento de información, la Subdirección Corporativa de Estrategia y Regulación hace de su conocimiento lo siguiente:

Nos permitimos informar que los detalles a este nivel de segregación y vinculados por virtud de los datos requeridos, conforman los Diagramas de red que se encuentran vigentes, 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 que contiene información sobre: (BIOS, MAC ADDRESS, Procesadores, número de serie y marca), Inventario de software, 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 y estándares y Plataformas, tecnologías), 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 y su configuración y demás información relacionada con la seguridad de la información puede poner en riesgo la operación total de la redes de voz y datos de la Subdirección Corporativa de Estrategia y Regulación ya que expone vulnerabilidades conocidas y no conocidas.

La información respecto a las configuraciones de los equipos de cómputo de escritorio y servidores (BIOS, MAC ADDRESS, procesadores, números de serie y marca) es información reservada por su naturaleza, ya que esta puede ser utilizada para estructurar y ejecutar un ataque cibernético que pudiera poner en riesgo sistemas críticos y sustantivos de la Subdirección Corporativa de Estrategia y Regulación, como son los sistemas de operación vinculados al sistema eléctrico nacional.

Al existir sistemas que por razones de operación requieren mantener cierta versión de BIOS, MAC ADDRESS, procesador, esta información puede ser utilizada para identificar vulnerabilidades o debilidades de equipos de cómputo y a partir de ahí afectar maliciosamente la operación de sistemas críticos o sustantivos.

De darse a conocer la información de los detalles técnicos de los equipos de cómputo, pondría en riesgo la operación de los equipos de cómputo y servidores de la Subdirección Corporativa de Estrategia y Regulación ya que podrían exponer vulnerabilidades conocidas y no conocidas.

Además de que resulta altamente probable que la difusión de la información contenida en la información solicitada, pudiera afectar la seguridad de la red de voz, datos y sistemas informáticos de la Subdirección Corporativa de Estrategia y Regulación de CFE y por tanto, la continuidad de las actividades relativas a garantizar la operación de los sistemas internos de la Subdirección Corporativa de Estrategia y Regulación de CFE, adicionalmente la protección a los sistemas que controlan las redes eléctricas y así poder garantizar la operación del sistema eléctrico nacional, toda vez que la seguridad perimetral esta para evitar cualquier tipo de amenazas internas y externas.

A mayor abundamiento, los datos requeridos, por su naturaleza estructurada, no pueden ser proporcionados ya que se tendría un alto riesgo al ser utilizado 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 Subdirección Corporativa de Estrategia y Regulación por lo que consideramos esta información debe ser clasificada como reservada, en virtud que la relación de información solicitada puede ser correlacionada para identificar el código malicioso o programa específico que permita llevar a cabo un ataque dirigido hacia los sistemas informáticos de la Subdirección Corporativa de Estrategia y Regulación, y de esta manera vulnerar la red eléctrica nacional. Tener esta información vinculada permite identificar específicamente si el equipo de cómputo presenta alguna vulnerabilidad de hardware y cómo explotarla con base a la información específica de los procesadores instalados en los equipos. Las investigaciones en materia de ciberseguridad han identificado vulnerabilidades de la arquitectura de procesadores de ciertas marcas que podrían ser explotadas con fines maliciosos.

Algunos de estos datos, consisten en identificadores únicos que se les asigna a las interfaces de redes. Las tarjetas de red inalámbrica o las de red Ethernet, los módems, los routers, las impresoras, etc., todos tienen un identificador propio de 48 bits que no se repite en todo el mundo, es como su propia huella digital para poder comunicarse. Por tanto, dicha situación genera que en una red informática los equipos puedan ser identificados de esta manera además de poderse hacer a través de la dirección IP. En este sentido los datos requeridos son elementos importantes de la vida digital de los dispositivos ya que permite un nivel muy elevado de identificación de los equipos.

Por las razones expuestas, se considera que los datos requeridos son información CLASIFICADA como RESERVADA y CONFIDENCIAL con fundamento en:

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: 11 de abril de 2018.

Periodo de Reserva: 5 años

Oficina del Abogado General

En atención a su solicitud de información, nos permitimos comunicar que la Oficina del Abogado General considera que la información es de carácter RESERVADA y CONFIDENCIAL, toda vez que divulgar la diversa información solicitada puede poner en riesgo la operación total de la redes de voz y datos de la Comisión Federal de Electricidad ya que expone vulnerabilidades conocidas y no conocidas. Por lo anterior, 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, y en el artículo 113 fracción II de la LFTAIP con relación al artículo 82 de la Ley de Propiedad Industrial. Nos permitimos informar que los detalles a este nivel de segregación y vinculados por virtud de los datos requeridos, conforman los Diagramas de red que se encuentran vigentes, 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 que contiene información sobre: (BIOS, MAC ADDRESS, Procesadores, número de serie y marca), Inventario de software, 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 y estándares y Plataformas, tecnologías), 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 y su configuración y demás información relacionada con la seguridad de la información puede poner en riesgo la operación total de la redes de voz y datos de la CFE ya que expone vulnerabilidades conocidas y no conocidas.

La información respecto a las configuraciones de los equipos de cómputo de escritorio y servidores (BIOS, MAC ADDRESS, procesadores, números de serie y marca) es información reservada por su naturaleza, ya que esta puede ser utilizada para estructurar y ejecutar un ataque cibernético que pudiera poner en riesgo sistemas críticos y sustantivos de la CFE, como son los sistemas de operación vinculados al sistema eléctrico nacional.

Al existir sistemas que por razones de operación requieren mantener cierta versión de BIOS, MAC ADDRESS, procesador, esta información puede ser utilizada para identificar vulnerabilidades o debilidades de equipos de cómputo y a partir de ahí afectar maliciosamente la operación de sistemas críticos o sustantivos.

De darse a conocer la información de los detalles técnicos de los equipos de cómputo, pondría en riesgo la operación de los equipos de cómputo y servidores de la CFE ya que podrían exponer vulnerabilidades conocidas y no conocidas. Además de que resulta altamente probable que la difusión de la información contenida en la información solicitada, pudiera afectar la seguridad de la red de voz, datos y sistemas informáticos de la Oficina del Abogado General de CFE y por tanto, la continuidad de las actividades relativas a garantizar la operación de los sistemas internos de la CFE, adicionalmente la protección a los sistemas que controlan las redes eléctricas y así poder garantizar la operación del sistema eléctrico nacional, toda vez que la seguridad perimetral esta para evitar cualquier tipo de amenazas internas y externas.

A mayor abundamiento, los datos requeridos, por su naturaleza estructurada, no pueden ser proporcionados ya que se tendría un alto riesgo al ser utilizado 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 esta información debe ser clasificada como reservada, en virtud que la relación de información solicitada puede ser correlacionada para identificar el código malicioso o programa específico que permita llevar a cabo un ataque dirigido hacia los sistemas informáticos de la CFE, y de esta manera vulnerar la red eléctrica nacional. Tener esta información vinculada permite identificar específicamente si el equipo de cómputo presenta alguna vulnerabilidad de hardware y cómo explotarla con base a la información específica de los procesadores instalados en los equipos. Las investigaciones en materia de ciberseguridad han identificado vulnerabilidades de la arquitectura de procesadores de ciertas marcas que podrían ser explotadas con fines maliciosos.

Algunos de estos datos, consisten en identificadores únicos que se les asigna a las interfaces de redes. Las tarjetas de red inalámbrica o las de red Ethernet, los módems, los routers, las impresoras, etc., todos tienen un identificador

propio de 48 bits que no se repite en todo el mundo, es como su propia huella digital para poder comunicarse. Por tanto, dicha situación genera que en una red informática los equipos puedan ser identificados de esta manera además de poderse hacer a través de la dirección IP. En este sentido los datos requeridos son elementos importantes de la vida digital de los dispositivos ya que permite un nivel muy elevado de identificación de los equipos.

Por las razones expuestas, se considera que los datos requeridos son información CLASIFICADA como RESERVADA y CONFIDENCIAL con fundamento en:

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: 11 de abril de 2018.

Periodo de Reserva: 5 años

Dirección Corporativa de Administración

En atención a su solicitud se comunica lo siguiente:

Nos permitimos informar que los detalles a este nivel de segregación y vinculados por virtud de los datos requeridos, conforman los Diagramas de red que se encuentran vigentes, 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 que contiene información sobre: (BIOS, Procesadores y marca), Inventario de software, 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 y estándares y Plataformas, tecnologías); 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 y 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.

La información solicitada respecto a las configuraciones de los equipos de cómputo de escritorio y servidores (BIOS, procesadores y marca) es información reservada por su naturaleza, ya que esta puede ser utilizada para estructurar y ejecutar un ataque cibernético que pudiera poner en riesgo sistemas críticos y sustantivos de la CFE, como son los sistemas de operación vinculados al sistema eléctrico nacional.

Al existir sistemas que por razones de operación requieren mantener cierta versión de BIOS, procesador, esta información puede ser utilizada para identificar vulnerabilidades o debilidades de equipos de cómputo y a partir de ahí afectar maliciosamente la operación de sistemas críticos o sustantivos.

De darse a conocer la información de los detalles técnicos de los equipos de cómputo, pondría en riesgo la operación de los equipos de cómputo y servidores de la CFE ya que podrían exponer vulnerabilidades conocidas y no conocidas. Además de que resulta altamente probable que la difusión de la información contenida en la información solicitada, pudiera afectar la seguridad de la red de voz, datos y sistemas informáticos de la Dirección Corporativa de Administración de CFE y por tanto, la continuidad de las actividades relativas a garantizar la operación de los sistemas internos de la Dirección Corporativa de Administración de CFE, adicionalmente la protección a los sistemas que controlan las redes eléctricas y así poder garantizar la operación del sistema eléctrico nacional, toda vez que la seguridad perimetral está para evitar cualquier tipo de amenazas internas y externas.

A mayor abundamiento, los datos requeridos, por su naturaleza estructurada, no pueden ser proporcionados ya que pueden ser utilizados 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 esta información debe ser clasificada como reservada, en virtud que la relación de información solicitada puede ser correlacionada para identificar el código malicioso o programa específico que permita llevar a cabo un ataque dirigido hacia los sistemas informáticos de la CFE, y de esta manera vulnerar la red eléctrica nacional. Tener esta información vinculada permite identificar específicamente si el equipo de cómputo presenta alguna vulnerabilidad de hardware y cómo explotarla con base a la información específica de los procesadores instalados en los equipos. Las investigaciones en materia de ciberseguridad han identificado vulnerabilidades de la arquitectura de procesadores de ciertas marcas que podrían ser explotadas con fines maliciosos.

Algunos de estos datos, consisten en identificadores únicos que se les asigna a las interfaces de redes. Las tarjetas de red inalámbrica o las de red Ethernet, los routers, las impresoras, etc., todos tienen un identificador propio de 48 bits que no se repite en todo el mundo, es como su propia huella digital para poder comunicarse. Por tanto, dicha situación genera que en una red informática los equipos puedan ser identificados de esta manera además de poderse hacer a través de la dirección IP. En este sentido los datos requeridos son elementos importantes de la vida digital de los dispositivos ya que permite un nivel muy elevado de identificación de los equipos.

Por las razones expuestas, se considera que los datos requeridos son información CLASIFICADA como RESERVADA y CONFIDENCIAL con fundamento en:

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: 11 de abril de 2018.

Periodo de Reserva: 5 años.

Dirección Corporativa de Finanzas

En atención a la solicitud, se da respuesta enviada por la Jefatura de la Dirección Corporativa de Finanzas.

Nos permitimos informar que los detalles a este nivel de segregación y vinculados por virtud de los datos requeridos, conforman los Diagramas de red que se encuentran vigentes, 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 que contiene información sobre: (BIOS, Procesadores y marca), Inventario de software, 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 y estándares y Plataformas, tecnologías), 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 y su configuración y demás información relacionada con la seguridad de la información puede poner en riesgo la operación total de la red de voz y datos de la CFE ya que expone vulnerabilidades conocidas y no conocidas.

La información solicitada respecto a las configuraciones de los equipos de cómputo de escritorio y servidores (BIOS, procesadores y marca) es información reservada por su naturaleza, ya que esta puede ser utilizada para estructurar y ejecutar un ataque cibernético que pudiera poner en riesgo sistemas críticos y sustantivos de la CFE, como son los sistemas de operación vinculados al sistema eléctrico nacional.

Al existir sistemas que por razones de operación requieren mantener cierta versión de BIOS, procesador, esta información puede ser utilizada para identificar vulnerabilidades o debilidades de equipos de cómputo y a partir de ahí afectar maliciosamente la operación de sistemas críticos o sustantivos.

De darse a conocer la información de los detalles técnicos de los equipos de cómputo, pondría en riesgo la operación de los equipos de cómputo y servidores de la CFE ya que podrían exponer vulnerabilidades conocidas y no conocidas. Además de que resulta altamente probable que la difusión de la información contenida en la información solicitada, pudiera afectar la seguridad de la red de voz, datos y sistemas informáticos de la Dirección Corporativa de Finanzas y por tanto, la continuidad de las actividades relativas a garantizar la operación de los sistemas internos de la Dirección Corporativa de Finanzas, adicionalmente la protección a los sistemas que controlan las redes eléctricas y así poder garantizar la operación del sistema eléctrico nacional, toda vez que la seguridad perimetral esta para evitar cualquier tipo de amenazas internas y externas.

A mayor abundamiento, los datos requeridos, por su naturaleza estructurada, no pueden ser proporcionados ya que pueden ser utilizado 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 esta información debe ser clasificada como reservada, en virtud que la relación de información solicitada puede ser correlacionada para identificar el código malicioso o programa específico que permita llevar a cabo un ataque dirigido hacia los sistemas informáticos de la CFE, y de esta manera vulnerar la red eléctrica nacional. Tener esta información vinculada permite identificar específicamente si el equipo de cómputo presenta alguna vulnerabilidad de hardware y cómo explotarla con base a la información específica de los procesadores instalados en los equipos. Las investigaciones en materia de ciberseguridad han identificado vulnerabilidades de la arquitectura de procesadores de ciertas marcas que podrían ser explotadas con fines maliciosos.

Algunos de estos datos, consisten en identificadores únicos que se les asigna a las interfaces de redes. Las tarjetas de red inalámbrica o las de red Ethernet, los routers, las impresoras, etc., todos tienen un identificador propio de 48 bits que no se repite en todo el mundo, es como su propia huella digital para poder comunicarse. Por tanto, dicha situación genera que en una red informática los equipos puedan ser identificados de esta manera además de poderse hacer a través de la dirección IP. En este sentido los datos requeridos son elementos importantes de la vida digital de los dispositivos ya que permite un nivel muy elevado de identificación de los equipos.

Por las razones expuestas, se considera que los datos requeridos son información CLASIFICADA como RESERVADA y CONFIDENCIAL con fundamento en:

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: 11 de abril de 2018.

Periodo de Reserva: 5 años

Dirección Corporativa de Ingeniería y Proyectos de Infraestructura

La Dirección Corporativa de Ingeniería y Proyectos de Infraestructura (DCIPI) informa que los detalles a este nivel de segregación y vinculados por virtud de los datos requeridos, conforman los Diagramas de red que se encuentran vigentes, 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 que contiene información sobre: (BIOS, MAC ADDRESS, Procesadores, número de serie y marca), Inventario de software, 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 y estándares y Plataformas, tecnologías), 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 y su configuración y demás información relacionada con la seguridad de la información puede poner en riesgo la operación total de la redes de voz y datos de la CFE ya que expone vulnerabilidades conocidas y no conocidas.

La información respecto a las configuraciones de los equipos de cómputo de escritorio y servidores (BIOS, MAC ADDRESS, procesadores, números de serie y marca) es información reservada por su naturaleza, ya que esta puede ser utilizada para estructurar y ejecutar un ataque cibemético que pudiera poner en riesgo sistemas críticos y sustantivos de la CFE, como son los sistemas de operación vinculados al sistema eléctrico nacional.

Al existir sistemas que por razones de operación requieren mantener cierta versión de BIOS, MAC ADDRESS, procesador, esta información puede ser utilizada para identificar vulnerabilidades o debilidades de equipos de cómputo y a partir de ahí afectar maliciosamente la operación de sistemas críticos o sustantivos.

De darse a conocer la información de los detalles técnicos de los equipos de cómputo, pondría en riesgo la operación de los equipos de cómputo y servidores de la CFE ya que podrían exponer vulnerabilidades conocidas y no conocidas. Además de que resulta altamente probable que la difusión de la información contenida en la información solicitada, pudiera afectar la seguridad de la red de voz, datos y sistemas informáticos de la Dirección Corporativa de Ingeniería y Proyectos de Infraestructura de CFE y por tanto, la continuidad de las actividades relativas a garantizar la operación de los sistemas internos de la Dirección Corporativa de Ingeniería y Proyectos de Infraestructura de CFE, adicionalmente la protección a los sistemas que controlan las redes eléctricas y así poder garantizar la operación del sistema eléctrico nacional, toda vez que la seguridad perimetral esta para evitar cualquier tipo de amenazas internas y externas.

A mayor abundamiento, los datos requeridos, por su naturaleza estructurada, no pueden ser proporcionados ya que se tendría un alto riesgo al ser utilizado 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 esta información debe ser clasificada como reservada, en virtud que la relación de información solicitada puede ser correlacionada para identificar el código malicioso o programa específico que permita llevar a cabo un ataque dirigido hacia los sistemas informáticos de la CFE, y de esta manera vulnerar la red eléctrica nacional. Tener esta información vinculada permite identificar específicamente si el equipo de cómputo presenta alguna vulnerabilidad de hardware y cómo explotarla con base a la información específica de los procesadores instalados en los equipos. Las investigaciones en materia de ciberseguridad han identificado

vulnerabilidades de la arquitectura de procesadores de ciertas marcas que podrían ser explotadas con fines maliciosos.

Algunos de estos datos, consisten en identificadores únicos que se les asigna a las interfaces de redes. Las tarjetas de red inalámbrica o las de red Ethernet, los módems, los routers, las impresoras, etc., todos tienen un identificador propio de 48 bits que no se repite en todo el mundo, es como su propia huella digital para poder comunicarse. Por tanto, dicha situación genera que en una red informática los equipos puedan ser identificados de esta manera además de poderse hacer a través de la dirección IP. En este sentido los datos requeridos son elementos importantes de la vida digital de los dispositivos ya que permite un nivel muy elevado de identificación de los equipos.

Por las razones expuestas, se considera que los datos requeridos son información CLASIFICADA como RESERVADA y CONFIDENCIAL con fundamento en:

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: 11 de abril de 2018.

Periodo de Reserva: 5 años

PAESE

En atención a la solicitud, el Programa de Ahorro de Energía del Sector Eléctrico (PAESE), informa que los detalles a este nivel de segregación y vinculados por virtud de los datos requeridos, conforman los Diagramas de red que se encuentran vigentes, 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 que contiene información sobre: (BIOS, MAC ADDRESS, Procesadores, número de serie y marca), Inventario de software, 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 y estándares y Plataformas, tecnologías), 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 y su configuración y demás información relacionada con la seguridad de la información puede poner en riesgo la operación total de la redes de voz y datos de la CFE ya que exponen vulnerabilidades conocidas y no conocidas.

La información respecto a las configuraciones de los equipos de cómputo de escritorio y servidores (BIOS, MAC ADDRESS, procesadores, números de serie y marca) es información reservada por su naturaleza, ya que esta puede ser utilizada para estructurar y ejecutar un ataque cibernético que pudiera poner en riesgo sistemas críticos y sustantivos de la CFE, como son los sistemas de operación vinculados al sistema eléctrico nacional.

Al existir sistemas que por razones de operación requieren mantener cierta versión de BIOS, MAC ADDRESS, procesador, esta información puede ser utilizada para identificar vulnerabilidades o debilidades de equipos de cómputo y a partir de ahí afectar maliciosamente la operación de sistemas críticos o sustantivos.

De darse a conocer la información de los detalles técnicos de los equipos de cómputo, pondría en riesgo la operación de los equipos de cómputo y servidores de la CFE ya que podrían exponer vulnerabilidades conocidas y no conocidas. Además de que resulta altamente probable que la difusión de la información contenida en la información solicitada, pudiera afectar la seguridad de la red de voz, datos y sistemas informáticos del Programa de Ahorro de Energía del Sector Eléctrico y por tanto, la continuidad de las actividades relativas a garantizar la operación de los sistemas internos del Programa de Ahorro de Energía del Sector Eléctrico, adicionalmente la protección a los sistemas que controlan las redes eléctricas y así poder garantizar la operación del sistema eléctrico nacional, toda vez que la seguridad perimetral esta para evitar cualquier tipo de amenazas internas y externas.

A mayor abundamiento, los datos requeridos, por su naturaleza estructurada, no pueden ser proporcionados ya que se tendría un alto riesgo al ser utilizado 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 esta información debe ser clasificada como reservada, en virtud que la relación de información solicitada puede ser correlacionada para identificar el código malicioso o programa específico que permita llevar a cabo un ataque dirigido hacia los sistemas informáticos de la CFE, y de esta manera vulnerar la red eléctrica nacional. Tener esta información vinculada permite identificar específicamente si el equipo de

cómputo presenta alguna vulnerabilidad de hardware y cómo explotarla con base a la información específica de los procesadores instalados en los equipos. Las investigaciones en materia de ciberseguridad han identificado vulnerabilidades de la arquitectura de procesadores de ciertas marcas que podrían ser explotadas con fines maliciosos.

Algunos de estos datos, consisten en identificadores únicos que se les asigna a las interfaces de redes. Las tarjetas de red inalámbrica o las de red Ethernet, los módems, los routers, las impresoras, etc., todos tienen un identificador propio de 48 bits que no se repite en todo el mundo, es como su propia huella digital para poder comunicarse. Por tanto, dicha situación genera que en una red informática los equipos puedan ser identificados de esta manera además de poderse hacer a través de la dirección IP. En este sentido los datos requeridos son elementos importantes de la vida digital de los dispositivos ya que permite un nivel muy elevado de identificación de los equipos.

Por las razones expuestas, se considera que los datos requeridos son información CLASIFICADA como RESERVADA y CONFIDENCIAL con fundamento en:

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: 11 de abril de 2018.

Periodo de Reserva: 5 años"

Con fundamento en el Acuerdo aprobado por el Comité de Transparencia de la CFE, en su Trigésima Séptima Sesión Extraordinaria de fecha 1 de noviembre de 2016; en el sentido de que la Unidad de Enlace para la Información Pública (actualmente Unidad de Transparencia) y el Comité de Transparencia de la Comisión Federal de Electricidad, continúen dando cumplimiento a las obligaciones de Transparencia, Acceso a la Información Pública, Protección de Datos y Organización y Conservación de Archivos de las Empresas Productivas Subsidiarias, hasta en tanto se concluyan las acciones durante el proceso de transición y resulten operativas; se hace de su conocimiento que las Empresas Productivas Subsidiarias correspondientes informan lo siguiente:

"Subsidiaria Distribución

Nos permitimos informar que los detalles a este nivel de segregación y vinculados por virtud de los datos requeridos, conforman los Diagramas de red que se encuentran vigentes, 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 que contiene información sobre: (BIOS, MAC ADDRESS, Procesadores, número de serie y marca), Inventario de software, 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 y estándares y Plataformas, tecnologías), 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 y su configuración y demás información relacionada con la seguridad de la información puede poner en riesgo la operación total de la redes de voz y datos de la CFE ya que expone vulnerabilidades conocidas y no conocidas.

La información respecto a las configuraciones de los equipos de cómputo de escritorio y servidores (BIOS, MAC ADDRESS, procesadores, números de serie y marca) es información reservada por su naturaleza, ya que esta puede ser utilizada para estructurar y ejecutar un ataque cibernético que pudiera poner en riesgo sistemas críticos y sustantivos de la CFE, como son los sistemas de operación vinculados al sistema eléctrico nacional.

Al existir sistemas que por razones de operación requieren mantener cierta versión de BIOS, MAC ADDRESS, procesador, esta información puede ser utilizada para identificar vulnerabilidades o debilidades de equipos de cómputo y a partir de ahí afectar maliciosamente la operación de sistemas críticos o sustantivos.

De darse a conocer la información de los detalles técnicos de los equipos de cómputo, pondría en riesgo la operación de los equipos de cómputo y servidores de la CFE ya que podrían exponer vulnerabilidades conocidas y no conocidas. Además de que resulta altamente probable que la difusión de la información contenida en la información solicitada, pudiera afectar la seguridad de la red de voz, datos y sistemas informáticos de la CFE Subsidiaria de Distribución y por tanto, la continuidad de las actividades relativas a garantizar la operación de los sistemas internos de la CFE Subsidiaria de Distribución, adicionalmente la protección a los sistemas que controlan las redes eléctricas y así poder

garantizar la operación del sistema eléctrico nacional, toda vez que la seguridad perimetral esta para evitar cualquier tipo de amenazas internas y externas.

A mayor abundamiento, los datos requeridos, por su naturaleza estructurada, no pueden ser proporcionados ya que se tendría un alto riesgo al ser utilizado 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 esta información debe ser clasificada como reservada, en virtud que la relación de información solicitada puede ser correlacionada para identificar el código malicioso o programa específico que permita llevar a cabo un ataque dirigido hacia los sistemas informáticos de la CFE, y de esta manera vulnerar la red eléctrica nacional. Tener esta información vinculada permite identificar específicamente si el equipo de cómputo presenta alguna vulnerabilidad de hardware y cómo explotarla con base a la información específica de los procesadores instalados en los equipos. Las investigaciones en materia de ciberseguridad han identificado vulnerabilidades de la arquitectura de procesadores de ciertas marcas que podrían ser explotadas con fines maliciosos.

Algunos de estos datos, consisten en identificadores únicos que se les asigna a las interfaces de redes. Las tarjetas de red inalámbrica o las de red Ethernet, los módems, los routers, las impresoras, etc., todos tienen un identificador propio de 48 bits que no se repite en todo el mundo, es como su propia huella digital para poder comunicarse. Por tanto, dicha situación genera que en una red informática los equipos puedan ser identificados de esta manera además de poderse hacer a través de la dirección IP. En este sentido los datos requeridos son elementos importantes de la vida digital de los dispositivos ya que permite un nivel muy elevado de identificación de los equipos.

Por las razones expuestas, se considera que los datos requeridos son información CLASIFICADA como RESERVADA y CONFIDENCIAL con fundamento en:

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: 11 de abril de 2018.

Periodo de Reserva: 5 años

Subsidiaria Transmisión

Con relación a la solicitud, nos permitimos informar que los detalles a este nivel de segregación y vinculados por virtud de los datos requeridos, conforman los Diagramas de red que se encuentran vigentes, 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 que contiene información sobre: (BIOS, MAC ADDRESS, Procesadores, número de serie y marca), Inventario de software, 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 y estándares y Plataformas, tecnologías), 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 y su configuración y demás información relacionada con la seguridad de la información puede poner en riesgo la operación total de la redes de voz y datos de la CFE ya que expone vulnerabilidades conocidas y no conocidas.

La información respecto a las configuraciones de los equipos de cómputo de escritorio y servidores (BIOS, MAC ADDRESS, procesadores, números de serie y marca) es información reservada por su naturaleza, ya que esta puede ser utilizada para estructurar y ejecutar un ataque cibernético que pudiera poner en riesgo sistemas críticos y sustantivos de la CFE, como son los sistemas de operación vinculados al sistema eléctrico nacional.

Al existir sistemas que por razones de operación requieren mantener cierta versión de BIOS, MAC ADDRESS, procesador, esta información puede ser utilizada para identificar vulnerabilidades o debilidades de equipos de cómputo y a partir de ahí afectar maliciosamente la operación de sistemas críticos o sustantivos.

De darse a conocer la información de los detalles técnicos de los equipos de cómputo, pondría en riesgo la operación de los equipos de cómputo y servidores de la CFE ya que podrían exponer vulnerabilidades conocidas y no conocidas. Además de que resulta altamente probable que la difusión de la información contenida en la información solicitada, pudiera afectar la seguridad de la red de voz, datos y sistemas informáticos de la CFE Subsidiaria de Transmisión y

por tanto, la continuidad de las actividades relativas a garantizar la operación de los sistemas internos de la CFE Subsidiaria de Transmisión, adicionalmente la protección a los sistemas que controlan las redes eléctricas y así poder garantizar la operación del sistema eléctrico nacional, toda vez que la seguridad perimetral esta para evitar cualquier tipo de amenazas internas y externas.

A mayor abundamiento, los datos requeridos, por su naturaleza estructurada, no pueden ser proporcionados ya que se tendría un alto riesgo al ser utilizado 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 esta información debe ser clasificada como reservada, en virtud que la relación de información solicitada puede ser correlacionada para identificar el código malicioso o programa específico que permita llevar a cabo un ataque dirigido hacia los sistemas informáticos de la CFE, y de esta manera vulnerar la red eléctrica nacional. Tener esta información vinculada permite identificar específicamente si el equipo de cómputo presenta alguna vulnerabilidad de hardware y cómo explotarla con base a la información específica de los procesadores instalados en los equipos. Las investigaciones en materia de ciberseguridad han identificado vulnerabilidades de la arquitectura de procesadores de ciertas marcas que podrían ser explotadas con fines maliciosos.

Algunos de estos datos, consisten en identificadores únicos que se les asigna a las interfaces de redes. Las tarjetas de red inalámbrica o las de red Ethernet, los módems, los routers, las impresoras, etc., todos tienen un identificador propio de 48 bits que no se repite en todo el mundo, es como su propia huella digital para poder comunicarse. Por tanto, dicha situación genera que en una red informática los equipos puedan ser identificados de esta manera además de poderse hacer a través de la dirección IP. En este sentido los datos requeridos son elementos importantes de la vida digital de los dispositivos ya que permite un nivel muy elevado de identificación de los equipos.

Por las razones expuestas, se considera que los datos requeridos son información CLASIFICADA como RESERVADA y CONFIDENCIAL con fundamento en:

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: 11 de abril de 2018.

Periodo de Reserva: 5 años

Subsidiaria Suministrador de Servicios Básicos

En atención a la solicitud, nos permitimos informar que los detalles a este nivel de segregación y vinculados por virtud de los datos requeridos, conforman los Diagramas de red que se encuentran vigentes, 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 que contiene información sobre: (BIOS, MAC ADDRESS, Procesadores, número de serie y marca), Inventario de software, 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 y estándares y Plataformas, tecnologías), 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 y su configuración y demás información relacionada con la seguridad de la información puede poner en riesgo la operación total de la redes de voz y datos de la CFE ya que expone vulnerabilidades conocidas y no conocidas.

La información respecto a las configuraciones de los equipos de cómputo de escritorio y servidores (BIOS, MAC ADDRESS, procesadores, números de serie y marca) es información reservada por su naturaleza, ya que esta puede ser utilizada para estructurar y ejecutar un ataque cibemético que pudiera poner en riesgo sistemas críticos y sustantivos de la CFE, como son los sistemas de operación vinculados al sistema eléctrico nacional.

Al existir sistemas que por razones de operación requieren mantener cierta versión de BIOS, MAC ADDRESS, procesador, esta información puede ser utilizada para identificar vulnerabilidades o debilidades de equipos de cómputo y a partir de ahí afectar maliciosamente la operación de sistemas críticos o sustantivos.

De darse a conocer la información de los detalles técnicos de los equipos de cómputo, pondría en riesgo la operación de los equipos de cómputo y servidores de la CFE ya que podrían exponer vulnerabilidades conocidas y no conocidas.

Además de que resulta altamente probable que la difusión de la información contenida en la información solicitada, pudiera afectar la seguridad de la red de voz, datos y sistemas informáticos de la CFE Subsidiaria Suministros Básicos y por tanto, la continuidad de las actividades relativas a garantizar la operación de los sistemas internos de la CFE Subsidiaria Suministros Básicos, adicionalmente la protección a los sistemas que controlan las redes eléctricas y así poder garantizar la operación del sistema eléctrico nacional, toda vez que la seguridad perimetral esta para evitar cualquier tipo de amenazas internas y externas.

A mayor abundamiento, los datos requeridos, por su naturaleza estructurada, no pueden ser proporcionados ya que se tendría un alto riesgo al ser utilizado 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 esta información debe ser clasificada como reservada, en virtud que la relación de información solicitada puede ser correlacionada para identificar el código malicioso o programa específico que permita llevar a cabo un ataque dirigido hacia los sistemas informáticos de la CFE, y de esta manera vulnerar la red eléctrica nacional. Tener esta información vinculada permite identificar específicamente si el equipo de cómputo presenta alguna vulnerabilidad de hardware y cómo explotarla con base a la información específica de los procesadores instalados en los equipos. Las investigaciones en materia de ciberseguridad han identificado vulnerabilidades de la arquitectura de procesadores de ciertas marcas que podrían ser explotadas con fines maliciosos.

Algunos de estos datos, consisten en identificadores únicos que se les asigna a las interfaces de redes. Las tarjetas de red inalámbrica o las de red Ethernet, los módems, los routers, las impresoras, etc., todos tienen un identificador propio de 48 bits que no se repite en todo el mundo, es como su propia huella digital para poder comunicarse. Por tanto, dicha situación genera que en una red informática los equipos puedan ser identificados de esta manera además de poderse hacer a través de la dirección IP. En este sentido los datos requeridos son elementos importantes de la vida digital de los dispositivos ya que permite un nivel muy elevado de identificación de los equipos.

Por las razones expuestas, se considera que los datos requeridos son información CLASIFICADA como RESERVADA y CONFIDENCIAL con fundamento en:

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: 11 de abril de 2018.

Periodo de Reserva: 5 años

Subsidiaria Generación I

Nos permitimos informar que los detalles a este nivel de segregación y vinculados por virtud de los datos requeridos, conforman los Diagramas de red que se encuentran vigentes, 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 que contiene información sobre: (BIOS, Procesadores y marca), Inventario de software, 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 y estándares y Plataformas, tecnologías), 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 y su configuración y demás información relacionada con la seguridad de la información puede poner en riesgo la operación total de la redes de voz y datos de la CFE ya que expone vulnerabilidades conocidas y no conocidas.

La información solicitada respecto a las configuraciones de los equipos de cómputo de escritorio y servidores (BIOS, procesadores y marca) es información reservada por su naturaleza, ya que esta puede ser utilizada para estructurar y ejecutar un ataque cibernético que pudiera poner en riesgo sistemas críticos y sustantivos de la CFE, como son los sistemas de operación vinculados al sistema eléctrico nacional.

Al existir sistemas que por razones de operación requieren mantener cierta versión de BIOS, procesador, esta información puede ser utilizada para identificar vulnerabilidades o debilidades de equipos de cómputo y a partir de ahí afectar maliciosamente la operación de sistemas críticos o sustantivos.

De darse a conocer la información de los detalles técnicos de los equipos de cómputo, pondría en riesgo la operación de los equipos de cómputo y servidores de la CFE ya que podrían exponer vulnerabilidades conocidas y no conocidas. Además de que resulta altamente probable que la difusión de la información contenida en la información solicitada, pudiera afectar la seguridad de la red de voz, datos y sistemas informáticos de CFE Generación I y por tanto, la continuidad de las actividades relativas a garantizar la operación de los sistemas internos de CFE Generación I, adicionalmente la protección a los sistemas que controlan las redes eléctricas y así poder garantizar la operación del sistema eléctrico nacional, toda vez que la seguridad perimetral esta para evitar cualquier tipo de amenazas internas y externas.

A mayor abundamiento, los datos requeridos, por su naturaleza estructurada, no pueden ser proporcionados ya que pueden ser utilizado 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 esta información debe ser clasificada como reservada, en virtud que la relación de información solicitada puede ser correlacionada para identificar el código malicioso o programa específico que permita llevar a cabo un ataque dirigido hacia los sistemas informáticos de la CFE, y de esta manera vulnerar la red eléctrica nacional. Tener esta información vinculada permite identificar específicamente si el equipo de cómputo presenta alguna vulnerabilidad de hardware y cómo explotarla con base a la información específica de los procesadores instalados en los equipos. Las investigaciones en materia de ciberseguridad han identificado vulnerabilidades de la arquitectura de procesadores de ciertas marcas que podrían ser explotadas con fines maliciosos.

Algunos de estos datos, consisten en identificadores únicos que se les asigna a las interfaces de redes. Las tarjetas de red inalámbrica o las de red Ethernet, los routers, las impresoras, etc., todos tienen un identificador propio de 48 bits que no se repite en todo el mundo, es como su propia huella digital para poder comunicarse. Por tanto, dicha situación genera que en una red informática los equipos puedan ser identificados de esta manera además de poderse hacer a través de la dirección IP. En este sentido los datos requeridos son elementos importantes de la vida digital de los dispositivos ya que permite un nivel muy elevado de identificación de los equipos.

Por las razones expuestas, se considera que los datos requeridos son información CLASIFICADA como RESERVADA y CONFIDENCIAL con fundamento en:

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: 11 de abril de 2018.

Periodo de Reserva: 5 años

Subsidiaria Generación II

En atención a la solicitud de información, se hace de su conocimiento lo siguiente:

Nos permitimos informar que los detalles a este nivel de segregación y vinculados por virtud de los datos requeridos, conforman los Diagramas de red que se encuentran vigentes, 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 que contiene información sobre: (BIOS, Procesadores y marca), Inventario de software, 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 y estándares y Plataformas, tecnologías), 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 y su configuración y demás información relacionada con la seguridad de la información puede poner en riesgo la operación total de la redes de voz y datos de la CFE ya que expone vulnerabilidades conocidas y no conocidas.

La información solicitada respecto a las configuraciones de los equipos de cómputo de escritorio y servidores (BIOS, procesadores y marca) es información reservada por su naturaleza, ya que esta puede ser utilizada para estructurar y ejecutar un ataque cibernético que pudiera poner en riesgo sistemas críticos y sustantivos de CFE Generación II, como son los sistemas de operación vinculados al sistema eléctrico nacional.

Al existir sistemas que por razones de operación requieren mantener cierta versión de BIOS, procesador, esta información puede ser utilizada para identificar vulnerabilidades o debilidades de equipos de cómputo y a partir de ahí afectar maliciosamente la operación de sistemas críticos o sustantivos.

De darse a conocer la información de los detalles técnicos de los equipos de cómputo, pondría en riesgo la operación de los equipos de cómputo y servidores de CFE Generación II ya que podrían exponer vulnerabilidades conocidas y no conocidas.

Además de que resulta altamente probable que la difusión de la información contenida en la información solicitada, pudiera afectar la seguridad de la red de voz, datos y sistemas informáticos de CFE Generación II y por tanto, la continuidad de las actividades relativas a garantizar la operación de los sistemas internos de CFE Generación II, adicionalmente la protección a los sistemas que controlan las redes eléctricas y así poder garantizar la operación del sistema eléctrico nacional, toda vez que la seguridad perimetral esta para evitar cualquier tipo de amenazas internas y externas.

A mayor abundamiento, los datos requeridos, por su naturaleza estructurada, no pueden ser proporcionados ya que pueden ser utilizado 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 esta información debe ser clasificada como reservada, en virtud que la relación de información solicitada puede ser correlacionada para identificar el código malicioso o programa específico que permita llevar a cabo un ataque dirigido hacia los sistemas informáticos de la CFE, y de esta manera vulnerar la red eléctrica nacional. Tener esta información vinculada permite identificar específicamente si el equipo de cómputo presenta alguna vulnerabilidad de hardware y cómo explotarla con base a la información específica de los procesadores instalados en los equipos. Las investigaciones en materia de ciberseguridad han identificado vulnerabilidades de la arquitectura de procesadores de ciertas marcas que podrían ser explotadas con fines maliciosos.

Algunos de estos datos, consisten en identificadores únicos que se les asigna a las interfaces de redes. Las tarjetas de red inalámbrica o las de red Ethernet, los routers, las impresoras, etc., todos tienen un identificador propio de 48 bits que no se repite en todo el mundo, es como su propia huella digital para poder comunicarse. Por tanto, dicha situación genera que en una red informática los equipos puedan ser identificados de esta manera además de poderse hacer a través de la dirección IP. En este sentido los datos requeridos son elementos importantes de la vida digital de los dispositivos ya que permite un nivel muy elevado de identificación de los equipos.

Por las razones expuestas, se considera que los datos requeridos son información CLASIFICADA como RESERVADA y CONFIDENCIAL con fundamento en:

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: 11 de abril de 2018.

Periodo de Reserva: 5 años

Subsidiaria Generación III

En atención a su solicitud, al respecto se comunica que conforme lo informó el área de Tecnologías de Información de CFE Generación III se contesta de la siguiente manera en relación a los numerales de la SAIP que nos ocupa:

1. De cada uno de los equipos de cómputo en posesión del sujeto obligado:

a. Número de serie y de parte. b. Versión de la BIOS (siglas en ingles de Basic Input/Output System). c. Marca. d. Si se cuenta con contraseña para acceder a la configuración de la BIOS (siglas en ingles de Basic Input/Output System). e. Procesador. f. Capacidad de almacenamiento en el Disco Duro. g. Conforme al organigrama estructural, unidad, área u órgano que hace uso del equipo de cómputo.

Nos permitimos informar que los detalles a este nivel de segregación y vinculados por virtud de los datos requeridos, conforman los Diagramas de red que se encuentran vigentes, el Direcccionamiento 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 que contiene información sobre: (BIOS, MAC ADDRESS, Procesadores, número de serie y marca), Inventario de software, 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 y estándares y Plataformas, tecnologías), 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 y su configuración y demás información relacionada con la seguridad de la información puede poner en riesgo la operación total de la redes de voz y datos de la CFE ya que expone vulnerabilidades conocidas y no conocidas.

La información respecto a las configuraciones de los equipos de cómputo de escritorio y servidores (BIOS, MAC ADDRESS, procesadores, números de serie y marca) es información reservada por su naturaleza, ya que esta puede ser utilizada para estructurar y ejecutar un ataque cibernético que pudiera poner en riesgo sistemas críticos y sustantivos de CFE Generación III, como son los sistemas de operación vinculados al sistema eléctrico nacional.

Al existir sistemas que por razones de operación requieren mantener cierta versión de BIOS, MAC ADDRESS, procesador, esta información puede ser utilizada para identificar vulnerabilidades o debilidades de equipos de cómputo y a partir de ahí afectar maliciosamente la operación de sistemas críticos o sustantivos.

De darse a conocer la información de los detalles técnicos de los equipos de cómputo, pondría en riesgo la operación de los equipos de cómputo y servidores de la CFE Generación III ya que podrían exponer vulnerabilidades conocidas y no conocidas.

Además de que resulta altamente probable que la difusión de la información contenida en la información solicitada, pudiera afectar la seguridad de la red de voz, datos y sistemas informáticos de CFE Generación III y por tanto, la continuidad de las actividades relativas a garantizar la operación de los sistemas internos de la CFE Generación III, adicionalmente la protección a los sistemas que controlan las redes eléctricas y así poder garantizar la operación del sistema eléctrico nacional, toda vez que la seguridad perimetral esta para evitar cualquier tipo de amenazas internas y externas.

A mayor abundamiento, los datos requeridos, por su naturaleza estructurada, no pueden ser proporcionados ya que se tendría un alto riesgo al ser utilizado 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 esta información debe ser clasificada como reservada, en virtud que la relación de información solicitada puede ser correlacionada para identificar el código malicioso o programa específico que permita llevar a cabo un ataque dirigido hacia los sistemas informáticos de CFE Generación III, y de esta manera vulnerar la red eléctrica nacional. Tener esta información vinculada permite identificar específicamente si el equipo de cómputo presenta alguna vulnerabilidad de hardware y cómo explotarla con base a la información específica de los procesadores instalados en los equipos. Las investigaciones en materia de ciberseguridad han identificado vulnerabilidades de la arquitectura de procesadores de ciertas marcas que podrían ser explotadas con fines maliciosos.

Algunos de estos datos, consisten en identificadores únicos que se les asigna a las interfaces de redes. Las tarjetas de red inalámbrica o las de red Ethernet, los módems, los routers, las impresoras, etc., todos tienen un identificador propio de 48 bits que no se repite en todo el mundo, es como su propia huella digital para poder comunicarse. Por tanto, dicha situación genera que en una red informática los equipos puedan ser identificados de esta manera además de poderse hacer a través de la dirección IP. En este sentido los datos requeridos son elementos importantes de la vida digital de los dispositivos ya que permite un nivel muy elevado de identificación de los equipos.

Por las razones expuestas, se considera que los datos requeridos son información CLASIFICADA como RESERVADA y CONFIDENCIAL con fundamento en:

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: 11 de abril de 2018.

Periodo de Reserva: 5 años

Subsidiaria Generación IV

En relación a su solicitud, esta EPS Generación IV hace de su conocimiento lo siguiente:

Nos permitimos informar que los detalles a este nivel de segregación y vinculados por virtud de los datos requeridos, conforman los Diagramas de red que se encuentran vigentes, 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 que contiene información sobre: (BIOS, MAC ADDRESS, Procesadores, número de serie y marca), Inventario de software, 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 y estándares y Plataformas, tecnologías), 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 y su configuración y demás información relacionada con la seguridad de la información puede poner en riesgo la operación total de la redes de voz y datos de la CFE ya que expone vulnerabilidades conocidas y no conocidas.

La información respecto a las configuraciones de los equipos de cómputo de escritorio y servidores (BIOS, MAC ADDRESS, procesadores, números de serie y marca) es información reservada por su naturaleza, ya que esta puede ser utilizada para estructurar y ejecutar un ataque cibernético que pudiera poner en riesgo sistemas críticos y sustantivos de la CFE, como son los sistemas de operación vinculados al sistema eléctrico nacional.

Al existir sistemas que por razones de operación requieren mantener cierta versión de BIOS, MAC ADDRESS, procesador, esta información puede ser utilizada para identificar vulnerabilidades o debilidades de equipos de cómputo y a partir de ahí afectar maliciosamente la operación de sistemas críticos o sustantivos.

De darse a conocer la información de los detalles técnicos de los equipos de cómputo, pondría en riesgo la operación de los equipos de cómputo y servidores de la CFE ya que podrían exponer vulnerabilidades conocidas y no conocidas. Además de que resulta altamente probable que la difusión de la información contenida en la información solicitada, pudiera afectar la seguridad de la red de voz, datos y sistemas informáticos de la CFE Generación IV y por tanto, la continuidad de las actividades relativas a garantizar la operación de los sistemas internos de la CFE Generación IV, adicionalmente la protección a los sistemas que controlan las redes eléctricas y así poder garantizar la operación del sistema eléctrico nacional, toda vez que la seguridad perimetral esta para evitar cualquier tipo de amenazas internas y externas.

A mayor abundamiento, los datos requeridos, por su naturaleza estructurada, no pueden ser proporcionados ya que se tendría un alto riesgo al ser utilizado 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 esta información debe ser clasificada como reservada, en virtud que la relación de información solicitada puede ser correlacionada para identificar el código malicioso o programa específico que permita llevar a cabo un ataque dirigido hacia los sistemas informáticos de la CFE, y de esta manera vulnerar la red eléctrica nacional. Tener esta información vinculada permite identificar específicamente si el equipo de cómputo presenta alguna vulnerabilidad de hardware y cómo explotarla con base a la información específica de los procesadores instalados en los equipos. Las investigaciones en materia de ciberseguridad han identificado vulnerabilidades de la arquitectura de procesadores de ciertas marcas que podrían ser explotadas con fines maliciosos.

Algunos de estos datos, consisten en identificadores únicos que se les asigna a las interfaces de redes. Las tarjetas de red inalámbrica o las de red Ethernet, los módems, los routers, las impresoras, etc., todos tienen un identificador propio de 48 bits que no se repite en todo el mundo, es como su propia huella digital para poder comunicarse. Por tanto, dicha situación genera que en una red informática los equipos puedan ser identificados de esta manera además de poderse hacer a través de la dirección IP. En este sentido los datos requeridos son elementos importantes de la vida digital de los dispositivos ya que permite un nivel muy elevado de identificación de los equipos.

Por las razones expuestas, se considera que los datos requeridos son información CLASIFICADA como RESERVADA y CONFIDENCIAL con fundamento en:

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: 11 de abril de 2018.

Periodo de Reserva: 5 años

Subsidiaria Generación V

La información respecto a las configuraciones de los equipos de cómputo de escritorio y servidores (BIOS, MAC ADDRESS, procesadores, números de serie y marca) es información reservada por su naturaleza, ya que esta puede ser utilizada para estructurar y ejecutar un ataque cibernético que pudiera poner en riesgo sistemas críticos y sustantivos de la CFE, como son los sistemas de operación vinculados al sistema eléctrico nacional.

Al existir sistemas que por razones de operación requieren mantener cierta versión de BIOS, MAC ADDRESS, procesador, esta información puede ser utilizada para identificar vulnerabilidades o debilidades de equipos de cómputo y a partir de ahí afectar maliciosamente la operación de sistemas críticos o sustantivos.

De darse a conocer la información de los detalles técnicos de los equipos de cómputo, pondría en riesgo la operación de los equipos de cómputo y servidores de la CFE ya que podrían exponer vulnerabilidades conocidas y no conocidas. Además de que resulta altamente probable que la difusión de la información contenida en la información solicitada, pudiera afectar la seguridad de la red de voz, datos y sistemas informáticos de la CFE Generación V y por tanto, la continuidad de las actividades relativas a garantizar la operación de los sistemas internos de la CFE Generación V, adicionalmente la protección a los sistemas que controlan las redes eléctricas y así poder garantizar la operación del sistema eléctrico nacional, toda vez que la seguridad perimetral esta para evitar cualquier tipo de amenazas internas y externas.

A mayor abundamiento, los datos requeridos, por su naturaleza estructurada, no pueden ser proporcionados ya que se tendría un alto riesgo al ser utilizado 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 esta información debe ser clasificada como reservada, en virtud que la relación de información solicitada puede ser correlacionada para identificar el código malicioso o programa específico que permita llevar a cabo un ataque dirigido hacia los sistemas informáticos de la CFE, y de esta manera vulnerar la red eléctrica nacional. Tener esta información vinculada permite identificar específicamente si el equipo de cómputo presenta alguna vulnerabilidad de hardware y cómo explotarla con base a la información específica de los procesadores instalados en los equipos. Las investigaciones en materia de ciberseguridad han identificado vulnerabilidades de la arquitectura de procesadores de ciertas marcas que podrían ser explotadas con fines maliciosos.

Algunos de estos datos, consisten en identificadores únicos que se les asigna a las interfaces de redes. Las tarjetas de red inalámbrica o las de red Ethernet, los módems, los routers, las impresoras, etc., todos tienen un identificador propio de 48 bits que no se repite en todo el mundo, es como su propia huella digital para poder comunicarse. Por tanto, dicha situación genera que en una red informática los equipos puedan ser identificados de esta manera además de poderse hacer a través de la dirección IP. En este sentido los datos requeridos son elementos importantes de la vida digital de los dispositivos ya que permite un nivel muy elevado de identificación de los equipos.

Por las razones expuestas, se considera que los datos requeridos son información CLASIFICADA como RESERVADA y CONFIDENCIAL con fundamento en:

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.

Subsidiaria Generación VI

En atención a la solicitud, y de conformidad con lo notificado por la Subdirección de Negocios No Regulados, la Gerencia de Telecomunicaciones e Informática y el Departamento de Tecnologías de la Información de esta EPS CFE Generación VI, nos permitimos informar que los detalles a este nivel de segregación y vinculados por virtud de los datos requeridos, conforman los Diagramas de red que se encuentran vigentes, 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 que contiene información sobre: (BIOS, Procesadores y marca), Inventario de software, 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 y estándares y Plataformas, tecnologías), 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 y 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.

La información solicitada respecto a las configuraciones de los equipos de cómputo de escritorio y servidores (BIOS, procesadores y marca) es información reservada por su naturaleza, ya que esta puede ser utilizada para estructurar y ejecutar un ataque cibernético que pudiera poner en riesgo sistemas críticos y sustantivos de la CFE, como son los sistemas de operación vinculados al sistema eléctrico nacional.

Al existir sistemas que por razones de operación requieren mantener cierta versión de BIOS, procesador, esta información puede ser utilizada para identificar vulnerabilidades o debilidades de equipos de cómputo y a partir de ahí afectar maliciosamente la operación de sistemas críticos o sustantivos.

De darse a conocer la información de los detalles técnicos de los equipos de cómputo, pondría en riesgo la operación de los equipos de cómputo y servidores de la CFE ya que podrían exponer vulnerabilidades conocidas y no conocidas. Además de que resulta altamente probable que la difusión de la información contenida en la información solicitada, pudiera afectar la seguridad de la red de voz, datos y sistemas informáticos de la CFE Generación VI y por tanto, la continuidad de las actividades relativas a garantizar la operación de los sistemas internos de la CFE Generación VI, adicionalmente la protección a los sistemas que controlan las redes eléctricas y así poder garantizar la operación del sistema eléctrico nacional, toda vez que la seguridad perimetral está para evitar cualquier tipo de amenazas internas y externas.

A mayor abundamiento, los datos requeridos, por su naturaleza estructurada, no pueden ser proporcionados ya que pueden ser utilizados 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 esta información debe ser clasificada como reservada, en virtud que la relación de información solicitada puede ser correlacionada para identificar el código malicioso o programa específico que permita llevar a cabo un ataque dirigido hacia los sistemas informáticos de la CFE, y de esta manera vulnerar la red eléctrica nacional. Tener esta información vinculada permite identificar específicamente si el equipo de cómputo presenta alguna vulnerabilidad de hardware y cómo explotarla con base a la información específica de los procesadores instalados en los equipos. Las investigaciones en materia de ciberseguridad han identificado vulnerabilidades de la arquitectura de procesadores de ciertas marcas que podrían ser explotadas con fines maliciosos.

Algunos de estos datos, consisten en identificadores únicos que se les asigna a las interfaces de redes. Las tarjetas de red inalámbrica o las de red Ethernet, los routers, las impresoras, etc., todos tienen un identificador propio de 48 bits que no se repite en todo el mundo, es como su propia huella digital para poder comunicarse. Por tanto, dicha situación genera que en una red informática los equipos puedan ser identificados de esta manera además de poderse hacer a través de la dirección IP. En este sentido los datos requeridos son elementos importantes de la vida digital de los dispositivos ya que permite un nivel muy elevado de identificación de los equipos.

Por las razones expuestas, se considera que los datos requeridos son información CLASIFICADA como RESERVADA y CONFIDENCIAL con fundamento en:

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: 11 de abril de 2018.

Periodo de Reserva: 5 años

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: 11 de abril de 2018.

Periodo de Reserva: 5 años." (Sic)

III. El 30 de mayo de 2018 el Instituto recibió por parte del recurrente, la impugnación de la respuesta antes citada, en los siguientes términos:

(Transcripción original) "RECURSO DE REVISIÓN NUMERO DE SOLICITUD: 1816400098118 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: focalizada@mail.ru única y exclusivamente este último, como medio para recibir notificaciones; con

fundamento en el artículo 6°, apartado A fracción IV constitucional, artículos 146, 147, 148, 149, 151 párrafo 2° y demás relativos de la Ley Federal de Transparencia y Acceso a la Información Pública, interpongo el recurso de revisión en contra de la clasificación de información, efectuada por la Comisión Federal de Electricidad (CFE) en respuesta a la solicitud de información número de folio 1816400098118. 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. 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, como se evidenciará a priori en las subsecuentes líneas, la clasificación de información efectuada por el sujeto obligado en atención a la solicitud 1816400098118 transgrede el principio de máxima publicidad de la información. Sin embargo, es de advertirse antes que en función de lo dispuesto en el artículo 20 de la Ley General, la carga de la prueba recae directamente sobre el sujeto obligado. Página 1 de 7 LEY GENERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 04-05-2015 Artículo 20. Ante la negativa del acceso a la información o su inexistencia, el sujeto obligado deberá demostrar que la información solicitada está prevista en alguna de las excepciones contenidas en esta Ley o, en su caso, demostrar que la información no se refiere a alguna de sus facultades, competencias o funciones. Como se mencionó, el principio de máxima publicidad únicamente puede verse limitado por la actualización de algún supuesto previsto en el régimen de excepciones, es decir, ante la presencia de información clasificada como confidencial o reservada. Los artículos 113 de la Ley General y 110 de la Ley Federal de Transparencia y Acceso a la Información Pública (en lo subsecuente Ley Federal) establecen que información será considerada como reservada. LEY GENERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 04-05-2015 Artículo 113. Como información reservada podrá clasificarse aquella cuya publicación: I. Comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable; II. Pueda menoscabar la conducción de las negociaciones y relaciones internacionales; III. Se entregue al Estado mexicano expresamente con ese carácter o el de confidencial por otro u otros sujetos de derecho internacional, excepto cuando se trate de violaciones graves de derechos humanos o delitos de lesa humanidad de conformidad con el derecho internacional; IV. Pueda afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; pueda poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país, pueda comprometer la seguridad en la provisión de moneda nacional al país, o pueda incrementar el costo de operaciones financieras que realicen los sujetos obligados del sector público federal; V. Pueda poner en riesgo la vida, seguridad o salud de una persona física; VI. Obstruya las actividades de verificación, inspección y auditoría relativas al cumplimiento de las leyes o afecte la recaudación de contribuciones; VII. Obstruya la prevención o persecución de los delitos; VIII. La que contenga las opiniones, recomendaciones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos, hasta en tanto no sea adoptada la decisión definitiva, la cual deberá estar documentada; IX. Obstruya los procedimientos para fincar responsabilidad a los Servidores Públicos, en tanto no se haya dictado la resolución administrativa; X. Afecte los derechos del debido proceso; XI. Vulnere la conducción de los Expedientes judiciales o de los procedimientos administrativos seguidos en forma de juicio, en tanto no hayan causado estado; XII. Se encuentre contenida dentro de las investigaciones de hechos que la ley señale como delitos y se tramiten ante el Ministerio Público, y XIII. Las que por disposición expresa de una ley tengan tal carácter, siempre que sean acordes con las bases, principios y disposiciones establecidos en esta Ley y no la contravengan; así como las previstas en tratados internacionales. LEY FEDERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 09-05-2016 Artículo 110. Conforme a lo dispuesto por el artículo 113 de la Ley General, como información reservada podrá clasificarse aquella cuya publicación: Página 2 de 7 I. Comprometa la seguridad nacional, la seguridad pública, o la defensa nacional y cuente con un propósito genuino y un efecto demostrable; II. Pueda menoscabar la conducción de las negociaciones y relaciones internacionales; III. Se entregue al Estado mexicano expresamente con ese carácter o el de confidencial por otro u otros sujetos de derecho internacional, excepto cuando se trate de violaciones graves

de derechos humanos o delitos de lesa humanidad de conformidad con el derecho internacional; IV. Pueda afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; pueda poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país, pueda comprometer la seguridad en la provisión de moneda nacional al país, o pueda incrementar el costo de operaciones financieras que realicen los sujetos obligados del sector público federal; V. Pueda poner en riesgo la vida, seguridad o salud de una persona física; VI. Obstruya las actividades de verificación, inspección y auditoría relativas al cumplimiento de las leyes o afecte la recaudación de contribuciones; VII. Obstruya la prevención o persecución de los delitos; VIII. La que contenga las opiniones, recomendaciones o puntos de vista que formen parte del proceso deliberativo de los Servidores Públicos, hasta en tanto no sea adoptada la decisión definitiva, la cual deberá estar documentada; IX. Obstruya los procedimientos para fincar responsabilidad a los Servidores Públicos, en tanto no se haya dictado la resolución administrativa; X. Afecte los derechos del debido proceso; XI. Vulnere la conducción de los Expedientes judiciales o de los procedimientos administrativos seguidos en forma de juicio, en tanto no hayan causado estado; XII. Se encuentre contenida dentro de las investigaciones de hechos que la ley señale como delitos y se tramiten ante el Ministerio Público, y XIII. Las que por disposición expresa de una ley tengan tal carácter, siempre que sean acordes con las bases, principios y disposiciones establecidos en la Ley General y esta Ley y no las contravengan; así como las previstas en tratados internacionales. Por otra parte, los artículos 116 de la Ley General y 113 de la Ley Federal establecen que información será considerada como confidencial. LEY GENERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 04-05-2015 Artículo 116. Se considera información confidencial la que contiene datos personales concernientes a una persona identificada o identificable. La información confidencial no estará sujeta a temporalidad alguna y sólo podrán tener acceso a ella los titulares de la misma, sus representantes y los Servidores Públicos facultados para ello. Se considera como información confidencial: los secretos bancario, fiduciario, industrial, comercial, fiscal, bursátil y postal, cuya titularidad corresponda a particulares, sujetos de derecho internacional o a sujetos obligados cuando no involucren el ejercicio de recursos públicos. Asimismo, será información confidencial aquella que presenten los particulares a los sujetos obligados, siempre que tengan el derecho a ello, de conformidad con lo dispuesto por las leyes o los tratados internacionales. LEY FEDERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 09-05-2016 Artículo 113. Se considera información confidencial: I. La que contiene datos personales concernientes a una persona física identificada o identificable; Página 3 de 7 II. Los secretos bancario, fiduciario, industrial, comercial, fiscal, bursátil y postal, cuya titularidad corresponda a particulares, sujetos de derecho internacional o a sujetos obligados cuando no involucren el ejercicio de recursos públicos, y III. Aquella que presenten los particulares a los sujetos obligados, siempre que tengan el derecho a ello, de conformidad con lo dispuesto por las leyes o los tratados internacionales. La información confidencial no estará sujeta a temporalidad alguna y sólo podrán tener acceso a ella los titulares de la misma, sus representantes y los Servidores Públicos facultados para ello. Ahora bien, la información precisada en la solicitud 1816400098118 no actualiza algún supuesto previsto en los cuatro artículos antes transcritos, tal y como lo hace aparentar la clasificación efectuada por el sujeto obligado. Lo anterior, puesto que lo peticionado en la solicitud 1816400098118 se trata de información que de ninguna forma debe comprometer la seguridad nacional o la pública, y menos aún vulnerar o alterar el normal desarrollo de las funciones desempeñadas por el sujeto obligado. Sino por el contrario, respecto de lo peticionado en los incisos a), b), c), e) y f), lo único que permiten es dar cuenta de las especificaciones técnicas y características divulgadas a toda persona en las páginas de soporte técnico de cada fabricante del equipo de cómputo respectivo. Es importante se tenga en consideración que lo solicitado en los incisos a), b), c), e) y f), son datos que por disposición de los artículos 68 de la Ley Federal y 70 fracción XXXIV de la Ley General, se encuentran abiertos a todo el público; ya que estos deben formar parte del inventario de los bienes muebles en posesión o propiedad el sujeto obligado. LEY FEDERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 09-05-2016 Artículo 68. Los sujetos obligados en el ámbito federal deberán cumplir con las obligaciones de transparencia y poner a disposición del público y mantener actualizada, en los respectivos medios electrónicos, de acuerdo con sus facultades, atribuciones, funciones u objeto social, según corresponda, la información, por lo menos, de los temas, Documentos y políticas e información señalados en el Título Quinto de la Ley General. Al respecto, aquella información particular de la referida en el presente artículo que se ubique en alguno de los supuestos de clasificación señalados en los artículos 110 y 113 de la presente Ley no será objeto de la publicación a que se refiere este mismo artículo; salvo que pueda ser elaborada una versión pública. En todo caso se aplicará la prueba de daño a que se refiere el artículo 104 de la Ley General. En sus resoluciones el Instituto podrá señalar a los sujetos obligados que la información que deben proporcionar sea considerada como obligación de transparencia de conformidad con el Capítulo II del Título Quinto de la Ley General y el capítulo I del Título Tercero de esta Ley, atendiendo a la relevancia de la información, la incidencia de las solicitudes sobre la misma y el sentido reiterativo de las resoluciones. LEY GENERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 04-05-2015 Artículo 70. En la Ley Federal y de las Entidades Federativas se contemplará que los sujetos obligados pongan a disposición del público y mantengan actualizada, en los respectivos medios electrónicos, de acuerdo con sus facultades, atribuciones, funciones u objeto social, según corresponda, la información, por lo menos, de los temas, documentos y políticas que a continuación se señalan: (...) XXXIV. El inventario de bienes muebles e inmuebles en posesión y propiedad; (...) En cuanto a lo peticionado en el inciso d) de la solicitud 1816400098118, contrario a lo que

indica el sujeto obligado, permite corroborar si realmente se emplean mecanismos tendientes a robustecer la seguridad nacional. Página 4 de 7 Por último, lo requerido en el inciso g) simplemente es un criterio para una mejor sistematización de la información requerida en los otros incisos; además dicha información es pública por mandato de los artículos 68 de la Ley Federal y 70 fracción II de la Ley General. LEY GENERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 04-05-2015 Artículo 70. En la Ley Federal y de las Entidades Federativas se contemplará que los sujetos obligados pongan a disposición del público y mantengan actualizada, en los respectivos medios electrónicos, de acuerdo con sus facultades, atribuciones, funciones u objeto social, según corresponda, la información, por lo menos, de los temas, documentos y políticas que a continuación se señalan: (...) II. Su estructura orgánica completa, en un formato que permita vincular cada parte de la estructura, las atribuciones y responsabilidades que le corresponden a cada servidor público, prestador de servicios profesionales o miembro de los sujetos obligados, de conformidad con las disposiciones aplicables; (...) Inclusive, si alguno de los datos requeridos en la solicitud 1816400098118 pusieran en riesgo las actividades desempeñadas por los servidores públicos del sujeto obligado, el Instituto Mexicano del Seguro Social (IMSS), este Instituto (INAI), la Comisión Nacional del Sistema de Ahorro para el Retiro (CON SAR), la Sociedad Hipotecaria Federal (SIF) y el Banco Nacional de Obras y Servicios Públicos (BANOBRAS), la Secretaría Jurídica del Ejecutivo Federal, las Secretarías de Comunicaciones y Transportes, de la Defensa Nacional, de Gobernación, de Marina y de Relaciones Exteriores, no hubiesen entregado datos equivalentes, en respuesta a las solicitudes de información pública: 0064100554418, 0673800063618, 0612100007418, 0682000003618, 0632000009318, 0220000003218, 0000900061918, 0000700046818, 0000400060318, 0001300022218 y 0000500043718, respectivamente; mismas que con fundamento en el penúltimo párrafo del artículo 149 de la Ley Federal, someto a consideración de este Instituto. En suma, la clasificación efectuada por el sujeto obligado resulta violatoria del principio de máxima publicidad, y en última instancia del derecho fundamental de acceso a la información reconocido constitucional y convencionalmente en beneficio del hoy recurrente; ya que como se argumentó en líneas anteriores, lo requerido en la solicitud 1816400098118 no actualiza algún supuesto de reservada previsto en la Ley Federal o en la Ley General. AGRAVIO SEGUNDO.- Falta de notificación de la Resolución del Comité de Transparencia, por la cual se clasificó la información requerida. ARTÍCULOS TRANSGREDIDOS: 137, EN RELACIÓN CON EL 132 DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA, 140 EN RELACIÓN CON EL 135 DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. Por disposición del artículo 140 de la Ley Federal y 137 de la Ley General, los sujetos obligados deben seguir el siguiente procedimiento cuando consideren que los Documentos o la información requerida deban ser clasificados. LEY FEDERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 09-05-2016 Artículo 140. En caso de que los sujetos obligados consideren que los Documentos o la información requerida deban ser clasificados, deberá seguirse el procedimiento previsto en el Capítulo I del Título Séptimo de la Ley General, atendiendo además a las siguientes disposiciones: I. El Área deberá remitir la solicitud, así como un escrito en el que funde y motive la clasificación al Comité de Transparencia, mismo que deberá resolver para: Página 5 de 7 I. Confirmar la clasificación; II. Modificar la clasificación y otorgar total o parcialmente el acceso a la información, y III. Revocar la clasificación y conceder el acceso a la información. El Comité de Transparencia podrá tener acceso a la información que esté en poder del Área correspondiente, de la cual se haya solicitado su clasificación. La resolución del Comité de Transparencia será notificada al interesado en el plazo de respuesta a la solicitud que establece el artículo 135 de la presente Ley. LEY GENERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 04-05-2015 Artículo 137. En caso de que los sujetos obligados consideren que los Documentos o la información deba ser clasificada, se sujetará a lo siguiente: El Área deberá remitir la solicitud, así como un escrito en el que funde y motive la clasificación al Comité de Transparencia, mismo que deberá resolver para: a) Confirmar la clasificación; b) Modificar la clasificación y otorgar total o parcialmente el acceso a la información, y c) Revocar la clasificación y conceder el acceso a la información. El Comité de Transparencia podrá tener acceso a la información que esté en poder del Área correspondiente, de la cual se haya solicitado su clasificación. La resolución del Comité de Transparencia será notificada al interesado en el plazo de respuesta a la solicitud que establece el artículo 132 de la presente Ley. Ahora bien, en contravención a los preceptos jurídicos antes citados, el sujeto obligado omite notificarme la resolución del Comité de Transparencia a través de la cual se clasificó la información requerida en la solicitud 1816400098118. PRUEBAS A. Con fundamento en el artículo 20 de la Ley General, de aplicación supletoria a la Ley Federal, atentamente solicito se aplique la reversión de la carga de la prueba al sujeto obligado, es decir, se le requiera para que pruebe la reserva de la información precisada en la solicitud de información pública número 1816400098118. LEY FEDERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 09-05-2016 Artículo 7. A falta de disposición expresa en esta Ley, se aplicarán de manera supletoria y en el siguiente orden de prelación, las disposiciones de la Ley General y de la Ley Federal de Procedimiento Administrativo. LEY GENERAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 04-05-2015 Artículo 20. Ante la negativa del acceso a la información o su inexistencia, el sujeto obligado deberá demostrar que la información solicitada está prevista en alguna de las excepciones contenidas en esta Ley o, en su caso, demostrar que la información no se refiere a alguna de sus facultades, competencias o funciones. B. La instrumental de actuaciones y la presuncional en su doble aspecto, en todo lo que me favorezca. Página 6 de 7 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. En sesión del 11 de julio de 2018, el Pleno del INAI instruyó:

(Transcripción original) "...este Instituto considera procedente **MODIFICAR** la respuesta de la Comisión Federal de Electricidad e **instruirle** a efecto de que, a través de su Comité de Transparencia, confirme la reserva de la información relativa a los números de serie y de parte; la versión de la BIOS; la marca; si se cuenta con contraseña para acceder a la configuración de la BIOS; el procesador; la capacidad de almacenamiento en el Disco Duro; y, conforme al organigrama estructural, la unidad, área u órgano que hace uso del equipo de cómputo, de la que disponga cada equipo de cómputo en su posesión, 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, debiendo cumplir con la debida fundamentación, motivación y prueba de daño.

No es óbice precisar que toda vez que en la solicitud de acceso se señaló como modalidad preferente "Entrega por internet en la PNT" y, por el momento procesal en que se encuentra el recurso de revisión ello ya no es posible, el sujeto obligado deberá entregar el Acta de resolución correspondiente a la dirección que el particular proporcionó para tales efectos, o ponerla a su disposición en un sitio de internet, y comunicar a éste los datos que le permitan acceder a la misma. Lo anterior, de conformidad con lo establecido en el artículo 132 de la Ley Federal de Transparencia y Acceso a la Información Pública." (Sic)

Ante lo que: la Dirección General, la Coordinación de Comunicación Corporativa, Auditoría Interna, la Dirección Corporativa de Operaciones, la Dirección Corporativa de Negocios Comerciales, la Subdirección Corporativa de Estrategia y Regulación, la Oficina del Abogado General, la Dirección Corporativa de Administración, la Dirección Corporativa de Finanzas, la Dirección Corporativa de Ingeniería y Proyectos de Infraestructura, el Programa de Ahorro de Energía del Sector Eléctrico (PAESE), la Subsidiaria Distribución, la Subsidiaria Transmisión, la Subsidiaria Suministrador de Servicios Básicos, la Subsidiaria Generación I, la Subsidiaria Generación II, la Subsidiaria Generación III, la Subsidiaria Generación IV, la Subsidiaria Generación V y la Subsidiaria Generación VI, informaron:

(Transcripción original) "Se solicita la clasificación como reservada de la información relativa a los números de serie y de parte; la versión de la BIOS; la marca; si se cuenta con contraseña para acceder a la configuración de la BIOS; el procesador; la capacidad de almacenamiento en el Disco Duro; y, conforme al organigrama estructural, la unidad, área u órgano que hace uso del equipo de cómputo, de la que disponga cada equipo de cómputo en su posesión, 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 total 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 y **no la clasificación aludida por el sujeto obligado en la respuesta a la solicitud de acceso a la información.**

Por lo anterior informado, se concluye que la información relativa a: los números de serie y de parte; la versión de la BIOS; la marca; si se cuenta con contraseña para acceder a la configuración de la BIOS; el procesador; la capacidad de almacenamiento en el Disco Duro; y, conforme al organigrama estructural, la unidad, área u órgano que hace uso del equipo de cómputo, de la que disponga cada equipo de cómputo en su posesión, 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

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.

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 "...los números de serie y de parte; la versión de la BIOS; la marca; si se cuenta con contraseña para acceder a la configuración de la BIOS; el procesador; la capacidad de almacenamiento en el Disco Duro; y, conforme al organigrama estructural, la unidad, área u órgano que hace uso del equipo de cómputo, de la que disponga cada equipo de cómputo en su posesión" 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 General, la Coordinación de Comunicación Corporativa, Auditoría Interna, la Dirección Corporativa de Operaciones, la Dirección Corporativa de Negocios Comerciales, la Subdirección Corporativa de Estrategia y Regulación, la Oficina del Abogado General, la Dirección Corporativa de Administración, la Dirección Corporativa de Finanzas, la Dirección Corporativa de Ingeniería y Proyectos de Infraestructura, el Programa de Ahorro de Energía del Sector Eléctrico (PAESE), la Subsidiaria Distribución, la Subsidiaria Transmisión, la Subsidiaria Suministrador de Servicios Básicos, la Subsidiaria Generación I, la Subsidiaria Generación II, la Subsidiaria Generación III, la Subsidiaria Generación IV, la Subsidiaria Generación V y la Subsidiaria Generación VI.

No habiendo otro asunto que tratar, se dio por terminada la reunión, siendo las doce horas con treinta 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. Jesús Manuel Ponce Salas**

Por instrucciones del Mtro. Diódoro J. Siller Argüello, Coordinador de Proyectos Especiales y Racionalización de Activos de CFE,

**Mtra. Gabriela Alejandra Baca Pérez de Tejada**

Titular de la Unidad de Transparencia

**C. Carlos Alberto Peña Álvarez**

Responsable del Área Coordinadora de Archivos.

