4ª SESIÓN EXTRAORDINARIA DEL COMITÉ DE TRANSPARENCIA DE LA PROCURADURÍA DE LA DEFENSA DEL CONTRIBUYENTE

EN LA CIUDAD DE MÉXICO, SIENDO LAS 17:00 HORAS DEL DÍA **03 DE MARZO DE 2020**, SE REUNIERON EN LA SALA DE JUNTAS DEL PISO 6, DE LAS OFICINAS QUE OCUPA LA PROCURADURÍA DE LA DEFENSA DEL CONTRIBUYENTE, UBICADA EN AVENIDA INSURGENTES SUR, NÚMERO 954, COLONIA INSURGENTES SAN BORJA, ALCALDÍA BENITO JUÁREZ, C.P. 03100, LOS INTEGRANTES DEL COMITÉ DE TRANSPARENCIA A QUE HACEN REFERENCIA LOS ARTÍCULOS 43 Y 44, DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA, ASÍ COMO SUS CORRELATIVOS 64 Y 65, DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA: EL CONTADOR PÚBLICO GUILLERMO PULIDO JARAMILLO, DIRECTOR GENERAL DE ADMININTRACIÓN Y RESPONSABLE DEL ÁREA COORDINADORA DE ARCHIVOS; LA LICENCIADA CITLALI MONSERRAT SERRANO GARCÍA, DIRECTORA CONSULTIVA Y DE NORMATIVIDAD Y ENCARGADA DE LA UNIDAD DE TRANSPARENCIA Y, EL LICENCIADO ALFONSO QUIROZ ACOSTA, TITULAR DEL ÓRGANO INTERNO DE CONTROL DESIGNADO POR LA SECRETARÍA DE LA FUNCIÓN PÚBLICA; DE IGUAL FORMA, SE ENCUENTRA PRESENTE EL LICENCIADO GERARDO MARTÍNEZ ACUÑA, EN SU CALIDAD DE SECRETARIO TÉCNICO DEL COMITÉ DE TRANSPARENCIA, PARA EL DESAHOGO DEL SIGUIENTE:

ORDEN DEL DÍA

1.- Lista de asistencia y verificación del Quórum.

2.- Justificación de la Sesión Extraordinaria.

3.- Lectura y aprobación, en su caso, del Orden del Día.

4.- Discusión y en su caso, confirmación, modificación o revocación de la clasificación de la información realizada por la Dirección de Sistemas Sustantivos, relacionada con la solicitud de acceso a la información pública número 0063200003920.

5.- Discusión y en su caso, confirmación, modificación o revocación de la clasificación de la información realizada por la Dirección de Sistemas Sustantivos, relacionada con la solicitud de acceso a la información pública número 0063200004020.

6.- Discusión y en su caso, confirmación, modificación o revocación de la clasificación de la información realizada por la Dirección de Sistemas Sustantivos, relacionada con la solicitud de acceso a la información pública número 0063200004120.

7.- Discusión y en su caso, confirmación, modificación o revocación de la clasificación de la información realizada por la Dirección de Sistemas Sustantivos, relacionada con la solicitud de acceso a la información pública número 0063200004220.

8.- Discusión y en su caso, confirmación, modificación o revocación de la clasificación de la información realizada por la Dirección de Recursos Financieros, relacionada con la solicitud de acceso a la información pública número 0063200004320.

1.- Lista de Asistencia. Una vez verificado por parte del Secretario Técnico del Comité de Transparencia, que se encuentran presentes quienes se enlistan a continuación:

i. C.P. Guillermo Pulido Jaramillo, en su carácter de Responsable del Área Coordinadora de Archivos.

ii. Lic. Citlali Monserrat Serrano García, en su carácter de Encargada de la Unidad de Transparencia.

iii. Lic. Alfonso Quiroz Acosta, en su carácter de Titular del Órgano Interno de Control.

Se hace constar que se cuenta con el Quórum legal para dar inicio a la sesión.

2.- Justificación de la Sesión Extraordinaria. La convocatoria a la sesión extraordinaria se justifica plenamente, tomando en consideración los siguientes motivos:

I. Que de conformidad con lo dispuesto en los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública y 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública, el Comité de Transparencia es quien está facultado para confirmar, modificar o revocar las determinaciones en materia de clasificación de la información que realicen los titulares de las Áreas del Sujeto Obligado; razón por la cual, a efecto de determinar lo que en derecho proceda, se debe verificar la información clasificada por parte de:

a) La Dirección de Sistemas Sustantivos, relacionada con la solicitud de acceso a la información pública con número de folio **0063200003920**.

b) La Dirección de Sistemas Sustantivos, relacionada con la solicitud de acceso a la información pública con número de folio **0063200004020.**

c) La Dirección de Sistemas Sustantivos, relacionada con la solicitud de acceso a la información pública con número de folio **0063200004120**.

d) Dirección de Sistemas Sustantivos, relacionada con la solicitud de acceso a la información pública con número de folio **0063200004220**.

e) La Dirección de Recursos Financieros, relacionada con la solicitud de acceso a la información pública con número de folio **0063200004320**.

3.- Aprobación del orden del día. Se procede a dar lectura del orden del día, el cual es aprobado por los miembros del Comité de Transparencia.

4.- Discusión y en su caso, confirmación, modificación o revocación de la clasificación de la información realizada por la Dirección de Sistemas Sustantivos, relacionada con la solicitud de acceso a la información pública número 0063200003920.

I. El día 06 de febrero de 2020, el peticionario requirió en la solicitud de información pública número **0063200003920**, lo siguiente:

> ***"Se solicita se informe de manera electrónica y proporcione de manera detallada mediante la PNT en archivo de formato de datos abiertos tipo PDF la evidencia de uso de los enlaces de comunicaciones que aparecen en los entregables del contrato PRODECON-SG-DGATI-AD-004-2016 y en los entregables del contrato PRODECON-SG-DGATIC-AD-144-2016. Ambos para el periodo de Febrero 2016 a Diciembre 2016. Hago énfasis en que la información solicitada es pública, no incluye datos personales y está digitalizada. Por lo tanto no es información reservada ni tampoco Ad hoc."***
>
> *[sic]*

II. De conformidad con lo dispuesto en los artículos 45, fracciones II y IV, y 131, de la Ley General de Transparencia y Acceso a la Información

Pública (LGTAIP); 61, fracciones II y IV, 133 y 134, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP), en debido tiempo y forma, y mediante oficio número **PRODECON/SG/DGAJ/DCN/045/2020**, de fecha 07 de febrero de 2020, la Unidad de Transparencia turnó a la **Dirección de Sistemas Sustantivos**, la solicitud de acceso a la información en estudio, al ser la Unidad Administrativa competente para atender la petición.

III. Atento a lo anterior, mediante oficio **PRODECON/SG/DGA/DSS/012/2020**, de fecha 18 de febrero de 2020, y recibido por la Unidad de Transparencia al día siguiente, la **Dirección de Sistemas Sustantivos**, dio respuesta a la solicitud de información que nos ocupa, señalando en la parte que interesa lo siguiente:

> *"[...] En relación a las evidencias de uso de los enlaces de comunicaciones que aparecen de los entregables a los que hace referencia el peticionario, se advierte que cuentan con información reservada, toda vez que:*
>
> *Un **enlace de comunicaciones** es el medio de conexión entre dos lugares con el propósito de **transmitir y recibir información**. Puede hacer referencia a un conjunto de componentes electrónicos, que consisten en un transmisor y un receptor (dos piezas de un equipo terminal de datos) y el circuito de telecomunicación de datos de interconexión. Esto se rige por un protocolo de enlace que permite que los datos digitales puedan ser transferidos desde una fuente de datos a un receptor de datos.*
>
> *Con relación a la difusión de la información de uso de los enlaces de comunicaciones que se advierten en los entregables a los que hace referencia el solicitante, se advierte que representa un riesgo real en tanto que se facilita la identificación de elementos cuyas funciones están encaminadas a preservar la integridad y seguridad de la información, para un hacker es más fácil penetrar en una red si conoce de los elementos básicos que la conforman, como puede ser Tipo de enlace, Proveedor de servicio, intervalos de uso, ya que estos le permiten focalizar los ataques con algoritmos más precisos debido a los elementos conocidos, asimismo, al tener acceso a intervalos máximos o mínimos (picos) de uso diario o mensual de las comunicaciones, permitiría la intrusión de bots para generar tráfico en la red, disfrazando la intrusión de agentes externos a la red, por lo que pasaría desapercibido un ataque de esta naturaleza, lo que ocasionaría la perpetración de actos que tienden a conocer la información de los contribuyentes, misma que pueden trascender a la afectación de su identidad, a partir de la realización de actos perniciosos en su contra o distintos de sus fines; comprometiendo la operación de Prodecon, lo anterior en virtud de que el dar a conocer el uso y capacidad de los enlaces de comunicaciones, aunado a otros componentes, como son; Dirección IP, Dirección MAC, Segmentos de red, nombres de equipo, número de serie, entre otros, puede permitir a los hackers realizar suplantaciones y darles*

facilidades para que intenten acciones de penetración que pongan en riesgo la información de los servidores y de los equipos de cómputo.

Asimismo, permitiría que la persona mal intencionada pueda buscar en la red cualquier vulnerabilidad para realizar afectaciones mayores, por otra parte, puede extraer información sin que se llegue a detectar por meses, aún con los modernos motores de antimalware y rastreo de patrones por Inteligencia Artificial cabe esa posibilidad, el no tener un presupuesto robusto para buscar medios alternativos de defensa, Prodecon intenta con estas reservas mitigar la posibilidad de ocurrencia de las afectaciones que pueden ocasionar pérdidas mayores.

Por lo tanto, es información que se encuentra reservada, ya que representa un riesgo de ataque informático, toda vez que quien posea esta información puede suplantar la identidad de un usuario válido y tener acceso a los sistemas computacionales, situación que comprometería la información contenida en ellos, asimismo el cruce de información con otros elementos, como el número de serie, dirección MAC, protocolos de comunicación, segmentos de red, entre otros, de cada uno de los equipos comprometerían la disponibilidad, confiabilidad, e integridad de la información de la PRODECON, ya que un posible atacante tendría a su alcance todos los elementos necesarios para hacerse pasar por un usuario válido (suplantación de identidad) e ingresar a la red para intentar ataques informáticos que pueden ser desde la extracción de información (por ejemplo: datos personales), denegación de servicio (impedir la operación informática, inhabilitar los servicios), modificación o alteración de información oficial, publicación o divulgación de información, suplantando la identidad de un equipo válido.

En caso de proporcionar dicha información, se pone en riesgo la seguridad informática y la seguridad de la información de conformidad con el siguiente detalle que consta de la solicitud y las razones para reservar cada punto particular. [...]"

[Sic]

Asimismo, acompañó a su respuesta la prueba de daño correspondiente, en cuya motivación se señaló expresamente lo siguiente:

"[...]
Sobre el particular, de conformidad con lo dispuesto en los artículos 44, fracción II, 100, 104, 108 y 114, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, 97, 102, 105 y 111, de la Ley Federal de Transparencia y Acceso a la Información Pública, y los numerales Segundo, fracción XIV y Sexto, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, se informa que dicha información se encuentra reservada por cuanto hace al enlace de comunicaciones, tal y como se señala en el oficio PRODECON/SG/DGA/DSS/012/2020, mediante el cual se da respuesta al solicitante, en términos de lo dispuesto en los artículos 113, fracción VII, de la Ley General de Transparencia y Acceso a la

Información Pública; 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el numeral Vigésimo Sexto, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas; lo anterior, atendiendo a la siguiente:

I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional. *Se advierte que como información reservada podrá clasificarse aquella que obstruya la persecución de los delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión o limitar la capacidad de las autoridades para evitar la comisión de delitos. En atención a lo antes mencionado, proporcionar el dato solicitado limita la capacidad de Prodecon para evitar que personas ajenas alteren y extraigan información que se utiliza en las actividades cotidianas y cumplir con la encomienda de ser la entidad que tiene a su cargo la protección y defensa del contribuyente en materia fiscal.*

La difusión de la información de uso de los enlaces de comunicaciones representa un riesgo real en tanto que se facilita la identificación de elementos cuyas funciones están encaminadas a preservar la integridad y seguridad de la información, para un hacker es más fácil penetrar en una red si conoce de los elementos básicos que la conforman, como puede ser tipo de enlace, nombre del proveedor de servicio, intervalos de uso de la red, sumado a que haya otra(s) solicitud(es) referente(s) a otros componentes, como son; Dirección IP, Dirección MAC, Segmentos de red, nombres de equipo, número de serie, entre otros, lo que potencializaría el riesgo de vulnerar y focalizar los ataques con algoritmos más precisos debido a los elementos conocidos, asimismo al tener acceso a intervalos máximos o mínimos (picos) de uso diario o mensual de las comunicaciones, permitiría la intrusión de bots para generar tráfico en la red, disfrazando la intrusión de agentes externos a la red, por lo que pasaría desapercibido un ataque de esta naturaleza, lo que ocasionaría la perpetración de actos que tienden a conocer la información de los contribuyentes, misma que pueden trascender a la afectación de su identidad, a partir de la realización de actos perniciosos en su contra o distintos de sus fines; comprometiendo la operación de Prodecon, lo anterior en virtud de que el dar a conocer el uso y capacidad de los enlaces de comunicaciones puede permitir a los hackers realizar suplantaciones y darles facilidades para que intenten acciones de penetración que pongan en riesgo la información de los servidores y de los equipos de cómputo.

Asimismo, permitiría que la persona mal intencionada pueda buscar en la red cualquier vulnerabilidad para realizar afectaciones mayores, por otra parte, puede extraer información sin que se llegue a detectar por meses, aún con los modernos motores de antimalware y rastreo de patrones por Inteligencia Artificial cabe esa posibilidad, el no tener un presupuesto robusto para buscar medios alternativos de defensa, Prodecon intenta con estas reservas mitigar la posibilidad de ocurrencia de las afectaciones que pueden ocasionar pérdidas mayores.

II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda. *Al permitir que se identifique el uso de los enlaces de comunicaciones, se estaría vulnerando la operación de la infraestructura tecnológica de Prodecon, así como afectando el ejercicio de los derechos de los contribuyentes a hacer uso de los servicios que brinda Prodecon. Lo anterior ante la probabilidad de que personas con pretensiones delictivas pudieran aprovechar la identificación de vulnerabilidades de la infraestructura tecnológica o generar irregularidades en la operación administrativa y sustantiva y de esta forma perjudicar la reputación de la institución, así como el derecho de los Contribuyentes a recibir justicia fiscal por parte de esta Procuraduría; además, al perpetrar la información que se tiene concentrada de los contribuyentes, la misma quedaría expuesta, propiciando un robo de identidad o mal uso de dicha información, lo que podría ocasionar una afectación a la seguridad, vida e integridad de los Contribuyentes.*

Esto vulnera el interés general, ya que el beneficio se limitaría al derecho del solicitante de obtener información, en donde en todo caso, prevalecería el interés particular sobre el interés público.

III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar perjuicio. *Resguardar únicamente la información que contenga datos de la infraestructura tecnológica que se provee en los servicios de esta procuraduría, en virtud de que al divulgarse la misma, se pondría en riesgo la operación diaria al ser susceptible de hackeos y con ello vulnerar la información de los contribuyentes, por lo que reservar dicha información representa el medio adecuado para lograr el fin precitado.*

Ahora bien, considerando que la información de la PRODECON contiene información sensible de los contribuyentes, entre otros datos, la DSS solicita, de considerarlo viable, se confirme la reserva dichos datos por cinco años, al estimar que dicha temporalidad es adecuada y proporcional para la protección del interés público, en términos de lo previsto en el artículo-99, de la Ley Federal de Transparencia y Acceso a la Información Pública.

Cabe señalar que dicho plazo se puede ampliar de conformidad con el penúltimo párrafo del artículo 99, de la Ley Federal de Transparencia y Acceso a la Información Pública, mismo que establece: "Excepcionalmente, los sujetos obligados, con la aprobación de su Comité de Transparencia, podrán ampliar el periodo de reserva hasta por un plazo de cinco años adicionales, siempre y cuando justifiquen que subsisten las causa que dieron origen a su clasificación, mediante la aplicación de una prueba de daño".
[...]" *[Sic]*

IV. Atento a la clasificación de la información propuesta por la Dirección de Sistemas Sustantivos; en términos de lo establecido en los artículos 137, de la Ley General de Transparencia y Acceso a la Información

Pública y 140, de la Ley Federal de Transparencia y Acceso a la Información pública, se tiene por recibida en este Comité de Transparencia para los efectos conducentes.

V. En esa tesitura, del análisis a la prueba de daño que acompañó la Unidad Administrativa a su respuesta, se puede observar que reservó la información relativa a la evidencia de uso de los enlaces de comunicaciones que se advierten en los entregables de los contratos PRODECON-SG-DGATI-AD-004-2016 y PRODECON-SG-DGACTIC-AD-144-2016, relativos a los periodos de febrero de 2016 a diciembre de 2016, en términos de lo previsto en los artículos 113 fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública; 110 fracción VII, de la Ley Federal de Transparencia y acceso a la Información Pública; así como el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

Y al respecto, expresó esencialmente los siguientes motivos:

Que un enlace de comunicaciones es el medio de conexión entre dos lugares con el propósito de transmitir y recibir información. Puede hacer referencia a un conjunto de componentes electrónicos, que consisten en un transmisor y un receptor (dos piezas de un equipo terminal de datos) y el circuito de telecomunicación de datos de interconexión. Esto se rige por un protocolo de enlace que permite que los datos digitales pueden ser transferidos desde una fuente de datos a un receptor de datos.

Que con la difusión de la información requerida se limita la capacidad de Prodecon para evitar que personas ajenas alteren y extraigan información que se utiliza en las actividades cotidianas, por lo que conllevaría a un incumplimiento en su encomienda de brindar protección y defensa a los contribuyentes en materia fiscal.

Lo anterior en virtud de que, de proporcionarse la información solicitada, se facilitaría la identificación de elementos cuyas funciones están encaminadas a preservar la integridad y seguridad de la información, toda vez que para un Hacker le es más fácil entrar en una red si conoce los elementos básicos que la conforman, como pueden ser el tipo de enlace, proveedor de servicio, intervalos de uso, sumado a que en otras solicitudes se ha solicitado información relativa a otros componentes; lo que potencializaría el riesgo de vulnerar y focalizar los ataques con algoritmos más precisos debido a los elementos conocidos; asimismo, al tener acceso a intervalos máximos o mínimos

(picos) de uso diario o mensual de las comunicaciones, permitiría la intrusión de bots para generar tráfico en la red, disfrazando la intrusión de agentes externos a la red, por lo que pasaría desapercibido un ataque de esta naturaleza, lo que ocasionaría la perpetración de actos que tienden a conocer la información de los contribuyentes, misma que pueden trascender a la afectación de su identidad, a partir de la realización de actos perniciosos en su contra o distintos de sus fines; comprometiendo la operación de la Entidad, lo anterior en virtud de que el dar a conocer el uso y capacidad de los enlaces de comunicaciones puede permitir a los hackers realizar suplantaciones y darles facilidades para que intenten acciones de penetración que pongan en riesgo la información de los servidores y de los equipos de cómputo.

Aunado a que, de difundirse la información solicitada, permitiría que una persona mal intencionada, pueda buscar en la red cualquier vulnerabilidad para realizar afectaciones, es por ello que, con la reserva propuesta se intenta mitigar la posibilidad de ocasionar pérdidas mayores.

Asimismo, se hace referencia que, al permitir que se identifique el uso de los enlaces de comunicaciones, se estaría vulnerando la operación de la infraestructura tecnológica de Prodecon, lo que podría ocasionar una afectación a la seguridad, vida e integridad de los Contribuyentes; lo que vulnera el interés general, ya que el beneficio se limitaría al derecho del solicitante de obtener información, en donde en todo caso, prevalecería el interés particular sobre el interés público.

VI. En atención a lo anterior, este Comité de Transparencia determina lo siguiente:

Atendiendo la motivación que hizo valer la Dirección de Sistemas Sustantivos, la cual se encuentra encaminada a denotar que con la difusión de la información solicitada se tiene la expectativa razonable de que ocurra un ataque cibernético, toda vez que se facilitaría la identificación de elementos cuyas funciones están encaminadas a preservar la integridad y seguridad de la información, aunado a que, de tener acceso a intervalos máximos o mínimos de uso diario o mensual de las comunicaciones, se permitiría la intrusión de software malicioso para generar tráfico en la red, disfrazando la intrusión de agentes externos a ésta, pasando así desapercibido un ataque de esa naturaleza, lo que ocasionaría la perpetración de actos tendientes a la extracción ilegal de información privilegiada de los contribuyentes y

de la propia Entidad, comprometiendo la operación de la Procuraduría.

Lo anterior, pues el dar a conocer el uso o capacidad de los enlaces de comunicaciones puede permitirse a los hackers realizar suplantaciones y darle facilidades para emprender acciones de penetración indebida que ponga en riesgo la información de los servidores y de los equipos de cómputo de la Procuraduría.

Aunado a que, se podrían identificar vulnerabilidades específicas de los equipos informáticos, así como sus mecanismos de seguridad implementados, con el fin de comprometerlos, poniendo en riesgo la operación diaria de la Entidad, ello agravado por el hecho de que ya se compartieron datos que permitirían ocultar estas actividades.

Por lo anterior, en términos del artículo 140, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública, este Comité de Transparencia estima que la información que nos ocupa actualiza la causal de reserva a que se refieren los artículos 113 fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública; 110 fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con lo preceptuado en el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas; mismos que son de la literalidad siguiente:

> "***Artículo 113.*** *Como información reservada podrá clasificarse aquella cuya publicación:*
>
> *(...)*
>
> ***VII.*** *Obstruya la prevención o persecución de los delitos; (...)"*
>
> *"**Artículo 110.** Conforme a lo dispuesto por el artículo 113 de la Ley General, como información reservada podrá clasificarse aquella cuya publicación:*
> *(...)*
>
> ***VII.*** *Obstruya la prevención o persecución de los delitos; (...)"*
>
> *"**Vigésimo sexto.** De conformidad con el artículo 113, fracción VII de la Ley General, podrá considerarse como información reservada, aquella que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos.*

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

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

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

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

De la citas que preceden, se advierte con meridiana claridad que como información reservada podrá clasificarse aquella cuya publicación obstruya la prevención o persecución de los delitos, siendo de ambas hipótesis la que interesa para el caso que nos atañe la primera, relativa a la prevención de los delitos; lo anterior, en atención a la naturaleza de las manifestaciones de la Dirección de Sistemas Sustantivos, tendientes a exaltar que la difusión de la información podría tener como consecuencia un ataque intrusivo o cibernético, los cuales se encuentran contenidos en el Capítulo II, del Título Noveno del Código Penal Federal.

Por lo anterior, este Comité de Transparencia considera que, con la entrega de la información relativa a los enlaces de comunicaciones de esta Procuraduría se ocasionaría:

I. Un potencial **riesgo real, demostrable e identificable**, toda vez que se colocaría a esta Procuraduría de la Defensa del Contribuyente en un estado de **vulnerabilidad** toda vez que limitaría su capacidad para evitar que personas ajenas a la Institución pudiesen alterar y/o extraer información que se utiliza en sus actividades cotidianas, ello, pues se permitiría el acceso ilícito a sus equipos informáticos e información contenida en estos, facilitando:

- Una posible intervención de sus comunicaciones,
- La suplantación de sus equipos y de la información que almacena en sus servidores;
- El robo de la información que obra en sus archivos digitales,
- El detrimento de sus instalaciones tecnológicas y
- El hackeo de los sistemas informáticos.

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

II. Un **perjuicio significativo al interés público**, pues la Procuraduría de la Defensa del Contribuyente tiene como objeto garantizar el derecho de los contribuyentes a recibir justicia en materia fiscal en el orden federal, a través de la prestación de los servicios gratuitos de asesoría, representación y defensa, velando por el cumplimiento efectivo de sus derechos, para contribuir a propiciar un ambiente favorable en la construcción de una cultura de plena vigencia de los derechos del contribuyente en nuestro país, así como en la recepción de quejas, reclamaciones o emisión de recomendaciones públicas a las autoridades fiscales federales, a efecto de que se lleguen a corregir aquellas prácticas que indebidamente lesionan o les causan molestias excesivas o innecesarias a los contribuyentes; por lo que, de ser vulnerada su infraestructura tecnológica y equipamiento de la misma índole, 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, lo que de ninguna manera puede estar por encima del interés particular del peticionario.

III. 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 de telecomunicaciones 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 y que se encuentran en posesión del sujeto obligado, conociendo con un alto grado de precisión la información técnica referente a sus equipos, los protocolos de seguridad y las características de la infraestructura instalada.

En esa tónica, derivado de la naturaleza 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 Procuraduría, es que se colige que dar a conocer la misma facilitaría que personas expertas en informática **perturben los sistemas de comunicaciones** con los que cuenta la Entidad y ejecuten programas informáticos perjudiciales que modifiquen o destruyan información relevante; situación que pondría en un **estado vulnerable** la información que en ellos se contiene, facilitando la intervención de las comunicaciones.

VII. Ahora bien, en cuanto al periodo de reserva de la información, este Comité de Transparencia estima pertinente reservar la citada información, por un periodo de **cinco años,** ya que, a juicio de este Comité, dicho plazo es proporcional con la naturaleza y al grado de especificidad del tipo de información de que se trata.

En razón de lo antes expuesto, este Comité de Transparencia **CONFIRMA LA CLASIFICACIÓN** como **RESERVADA** de la información relativa a la evidencia de uso de los enlaces de comunicaciones que se advierten en los entregables de los contratos PRODECON-SG-DGATI-AD-004-2016 y PRODECON-SG-DGACTIC-AD-144-2016, relativos a los periodos de febrero de 2016 a diciembre de 2016, contenidos en la prueba de daño que se acompaña a la respuesta de la solicitud de información 0063200003920; lo anterior, de conformidad con lo dispuesto en los artículos 113, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública; 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas; asimismo, se confirma el periodo de cinco años para la reserva que nos ocupa, el cual puede ser ampliado, en términos de lo dispuesto en los artículos 101 y 103 de la Ley General de Transparencia y Acceso a la Información Pública y, 99 y 102 de la Ley Federal de Transparencia y Acceso a la Información Pública.

5.- Discusión y en su caso, confirmación, modificación o revocación de la clasificación de la información realizada por la Dirección de Sistemas Sustantivos, relacionada con la solicitud de acceso a la información pública número 0063200004020.

I. El día 06 de febrero de 2020, el peticionario requirió en la solicitud de información pública número **0063200004020**, lo siguiente:

> ***"Para el periodo de Enero 2017 a Diciembre 2017 se solicita se informe de manera electrónica y proporcione de manera detallada mediante la PNT en archivo de formato de datos abiertos tipo PDF TODA la evidencia que corresponde exclusivamente al uso de los enlaces de comunicaciones y que aparece en los entregables del contrato PRODECON-SG-DGATI-AD-004-2016 y en los entregables del contrato PRODECON-SG-DGATIC-AD-144-2016. Hago énfasis en que la información solicitada es pública, no incluye datos personales y está digitalizada. Por lo tanto no es información reservada ni tampoco Ad hoc"***
>
> *[Sic]*

II. De conformidad con lo dispuesto en los artículos 45, fracciones II y IV, y 131, de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 61, fracciones II y IV, 133 y 134, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP), en debido tiempo y forma, y mediante oficio número **PRODECON/SG/DGAJ/DCN/046/2020**, de fecha 07 de febrero de 2020, la Unidad de Transparencia turnó a la **Dirección de Sistemas Sustantivos**, la solicitud de acceso a la información en estudio, al ser la Unidad Administrativa competente para atender la petición.

III. Atento a lo anterior mediante oficio **PRODECON/SG/DGA/DSS/013/2020**, de fecha 18 de febrero de 2020, y recibido por la Unidad de Transparencia al día siguiente, la **Dirección de Sistemas Sustantivos**, dio respuesta a la solicitud de información que nos ocupa, señalando en la parte que interesa lo siguiente:

> *"[...] En relación a las evidencias de uso de los enlaces de comunicaciones que aparecen de los entregables a los que hace referencia el peticionario, se advierte que cuentan con información reservada, toda vez que:*
>
> *Un **enlace de comunicaciones** es el medio de conexión entre dos lugares con el propósito de **transmitir y recibir información**. Puede hacer referencia a un conjunto de componentes electrónicos, que consisten en un transmisor y un receptor (dos piezas de un equipo terminal de datos) y el circuito de telecomunicación de datos de interconexión. Esto se rige por un protocolo de enlace que permite que los datos digitales puedan ser transferidos desde una fuente de datos a un receptor de datos.*

Con relación a la difusión de la información de uso de los enlaces de comunicaciones que se advierten en los entregables a los que hace referencia el solicitante, se advierte que representa un riesgo real en tanto que se facilita la identificación de elementos cuyas funciones están encaminadas a preservar la integridad y seguridad de la información, para un hacker es más fácil penetrar en una red si conoce de los elementos básicos que la conforman, como puede ser Tipo de enlace, Proveedor de servicio, intervalos de uso, ya que estos le permiten focalizar los ataques con algoritmos más precisos debido a los elementos conocidos, asimismo, al tener acceso a intervalos máximos o mínimos (picos) de uso diario o mensual de las comunicaciones, permitiría la intrusión de bots para generar tráfico en la red, disfrazando la intrusión de agentes externos a la red, por lo que pasaría desapercibido un ataque de esta naturaleza, lo que ocasionaría la perpetración de actos que tienden a conocer la información de los contribuyentes, misma que pueden trascender a la afectación de su identidad, a partir de la realización de actos perniciosos en su contra o distintos de sus fines; comprometiendo la operación de Prodecon, lo anterior en virtud de que el dar a conocer el uso y capacidad de los enlaces de comunicaciones, aunado a otros componentes, como son; Dirección IP, Dirección MAC, Segmentos de red, nombres de equipo, número de serie, entre otros, puede permitir a los hackers realizar suplantaciones y darles facilidades para que intenten acciones de penetración que pongan en riesgo la información de los servidores y de los equipos de cómputo.

Asimismo, permitiría que la persona mal intencionada pueda buscar en la red cualquier vulnerabilidad para realizar afectaciones mayores, por otra parte, puede extraer información sin que se llegue a detectar por meses, aún con los modernos motores de antimalware y rastreo de patrones por Inteligencia Artificial cabe esa posibilidad, el no tener un presupuesto robusto para buscar medios alternativos de defensa, Prodecon intenta con estas reservas mitigar la posibilidad de ocurrencia de las afectaciones que pueden ocasionar pérdidas mayores.

Por lo tanto, es información que se encuentra reservada, ya que representa un riesgo de ataque informático, toda vez que quien posea esta información puede suplantar la identidad de un usuario válido y tener acceso a los sistemas computacionales, situación que comprometería la información contenida en ellos, asimismo el cruce de información con otros elementos, como el número de serie, dirección MAC, protocolos de comunicación, segmentos de red, entre otros, de cada uno de los equipos comprometerían la disponibilidad, confiabilidad, e integridad de la información de la PRODECON, ya que un posible atacante tendría a su alcance todos los elementos necesarios para hacerse pasar por un usuario válido (suplantación de identidad) e ingresar a la red para intentar ataques informáticos que pueden ser desde la extracción de información (por ejemplo: datos personales), denegación de servicio (impedir la operación informática, inhabilitar los servicios), modificación o alteración de información oficial, publicación o divulgación de información, suplantando la identidad de un equipo válido.

En caso de proporcionar dicha información, se pone en riesgo la seguridad informática y la seguridad de la información de conformidad con el siguiente detalle que consta de la solicitud y las razones para reservar cada punto particular. [...]"

[Sic]

Además, acompañó a su respuesta la prueba de daño correspondiente, en cuya motivación se señaló expresamente lo siguiente:

"[...]
Sobre el particular, de conformidad con lo dispuesto en los artículos 44, fracción II,100,104, 108 y 114, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, 97,102,105 y 111, de la Ley Federal de Transparencia y Acceso a la Información Pública, y los numerales Segundo, fracción XIV y Sexto, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, se informa que dicha información se encuentra reservada por cuanto hace al enlace de comunicaciones, tal y como se señala en el oficio PRODECON/SG/DGA/DSS/013/2020, mediante el cual se da respuesta al solicitante, en términos de lo dispuesto en los artículos 113, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública; 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el numeral Vigésimo Sexto, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas; lo anterior, atendiendo a la siguiente:

I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional. *Se advierte que como información reservada podrá clasificarse aquella que obstruya la persecución de los delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión o limitar la capacidad de las autoridades para evitar la comisión de delitos. En atención a lo antes mencionado, proporcionar el dato solicitado limita la capacidad de Prodecon para evitar que personas ajenas alteren y extraigan información que se utiliza en las actividades cotidianas y cumplir con la encomienda de ser la entidad que tiene a su cargo la protección y defensa del contribuyente en materia fiscal.*

La difusión de la información de uso de los enlaces de comunicaciones representa un riesgo real en tanto que se facilita la identificación de elementos cuyas funciones están encaminadas a preservar la integridad y seguridad de la información, para un hacker es más fácil penetrar en una red si conoce de los elementos básicos que la conforman, como puede ser tipo de enlace, nombre del proveedor de servicio, intervalos de uso de la red, sumado a que haya otra(s) solicitud(es) referente(s) a otros componentes, como son; Dirección IP, Dirección MAC, Segmentos de red, nombres de equipo, número de serie, entre otros, lo que potencializaría el

riesgo de vulnerar y focalizar los ataques con algoritmos más precisos debido a los elementos conocidos, asimismo al tener acceso a intervalos máximos o mínimos (picos) de uso diario o mensual de las comunicaciones, permitiría la intrusión de bots para generar tráfico en la red, disfrazando la intrusión de agentes externos a la red, por lo que pasaría desapercibido un ataque de esta naturaleza, lo que ocasionaría la perpetración de actos que tienden a conocer la información de los contribuyentes, misma que pueden trascender a la afectación de su identidad, a partir de la realización de actos perniciosos en su contra o distintos de sus fines; comprometiendo la operación de Prodecon, lo anterior en virtud de que el dar a conocer el uso y capacidad de los enlaces de comunicaciones puede permitir a los hackers realizar suplantaciones y darles facilidades para que intenten acciones de penetración que pongan en riesgo la información de los servidores y de los equipos de cómputo.

Asimismo, permitiría que la persona mal intencionada pueda buscar en la red cualquier vulnerabilidad para realizar afectaciones mayores, por otra parte, puede extraer información sin que se llegue a detectar por meses, aún con los modernos motores de antimalware y rastreo de patrones por Inteligencia Artificial cabe esa posibilidad, el no tener un presupuesto robusto para buscar medios alternativos de defensa, Prodecon intenta con estas reservas mitigar la posibilidad de ocurrencia de las afectaciones que pueden ocasionar pérdidas mayores.

II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda. *Al permitir que se identifique el uso de*

los enlaces de comunicaciones, se estaría vulnerando la operación de la infraestructura tecnológica de Prodecon, así como afectando el ejercicio de los derechos de los contribuyentes a hacer uso de los servicios que brinda Prodecon. Lo anterior ante la probabilidad de que personas con pretensiones delictivas pudieran aprovechar la identificación de vulnerabilidades de la infraestructura tecnológica o generar irregularidades en la operacıon administrativa y sustantiva y de esta forma perjudicar la reputación de la institución, así como el derecho de los Contribuyentes a recibir justicia fiscal por parte de esta Procuraduría; además, al perpetrar la información que se tiene concentrada de los contribuyentes, la misma quedaría expuesta, propiciando un robo de identidad o mal uso de dicha información, lo que podría ocasionar una afectación a la seguridad, vida e integridad de los Contribuyentes.

Esto vulnera el interés general, ya que el beneficio se limitaría al derecho del solicitante de obtener información, en donde en todo caso, prevalecería el interés particular sobre el interés público.

III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar perjuicio. *Resguardar únicamente la información que contenga datos de la infraestructura tecnológica que se provee en los servicios de esta procuraduría, en virtud de que al divulgarse la misma, se pondría en riesgo la operación diaria al ser*

susceptible de hackeos y con ello vulnerar la información de los contribuyentes, por lo que reservar dicha información representa el medio adecuado para lograr el fin precitado.

Ahora bien, considerando que la información de la PRODECON contiene información sensible de los contribuyentes, entre otros datos, la DSS solicita, de considerarlo viable, se confirme la reserva dichos datos por cinco años, al estimar que dicha temporalidad es adecuada y proporcional para la protección del interés público, en términos de lo previsto en el artículo-99, de la Ley Federal de Transparencia y Acceso a la Información Pública.

Cabe señalar que dicho plazo se puede ampliar de conformidad con el penúltimo párrafo del artículo 99, de la Ley Federal de Transparencia y Acceso a la Información Pública, mismo que establece: "Excepcionalmente, los sujetos obligados, con la aprobación de su Comité de Transparencia, podrán ampliar el periodo de reserva hasta por un plazo de cinco años adicionales, siempre y cuando justifiquen que subsisten las causa que dieron origen a su clasificación, mediante la aplicación de una prueba de daño".
[...]"

[Sic]

IV. Atento a la clasificación de la información propuesta por la Dirección de Sistemas Sustantivos; en términos de lo establecido en los artículos 137, de la Ley General de Transparencia y Acceso a la Información Pública y 140, de la Ley Federal de Transparencia y Acceso a la Información pública, se tiene por recibida en este Comité de Transparencia para los efectos conducentes.

V. En esa tesitura, del análisis a la prueba de daño que acompañó la Unidad Administrativa a su respuesta, se puede observar que reservó la información relativa a la evidencia de uso de los enlaces de comunicaciones que se advierten en los entregables de los contratos PRODECON-SG-DGATI-AD-004-2016 y PRODECON-SG-DGACTIC-AD-144-2016, relativos a los periodos de enero de 2017 a diciembre de 2017, en términos de lo previsto en los artículos 113 fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública; 110 fracción VII, de la Ley Federal de Transparencia y acceso a la Información Pública; así como el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

Y al respecto, expresó esencialmente los siguientes motivos:

Que un enlace de comunicaciones es el medio de conexión entre dos lugares con el propósito de transmitir y recibir información. Puede

hacer referencia a un conjunto de componentes electrónicos, que consisten en un transmisor y un receptor (dos piezas de un equipo terminal de datos) y el circuito de telecomunicación de datos de interconexión. Esto se rige por un protocolo de enlace que permite que los datos digitales pueden ser transferidos desde una fuente de datos a un receptor de datos.

Que con la difusión de la información requerida se limita la capacidad de Prodecon para evitar que personas ajenas alteren y extraigan información que se utiliza en las actividades cotidianas, por lo que conllevaría a un incumplimiento en su encomienda de brindar protección y defensa a los contribuyentes en materia fiscal.

Lo anterior en virtud de que, de proporcionarse la información solicitada, se facilitaría la identificación de elementos cuyas funciones están encaminadas a preservar la integridad y seguridad de la información, toda vez que para un Hacker le es más fácil entrar en una red si conoce los elementos básicos que la conforman, como pueden ser el tipo de enlace, proveedor de servicio, intervalos de uso, sumado a que en otras solicitudes se ha solicitado información relativa a otros componentes; lo que potencializaría el riesgo de vulnerar y focalizar los ataques con algoritmos más precisos debido a los elementos conocidos; asimismo, al tener acceso a intervalos máximos o mínimos (picos) de uso diario o mensual de las comunicaciones, permitiría la intrusión de bots para generar tráfico en la red, disfrazando la intrusión de agentes externos a la red, por lo que pasaría desapercibido un ataque de esta naturaleza, lo que ocasionaría la perpetración de actos que tienden a conocer la información de los contribuyentes, misma que pueden trascender a la afectación de su identidad, a partir de la realización de actos perniciosos en su contra o distintos de sus fines; comprometiendo la operación de la Entidad, lo anterior en virtud de que el dar a conocer el uso y capacidad de los enlaces de comunicaciones puede permitir a los hackers realizar suplantaciones y darles facilidades para que intenten acciones de penetración que pongan en riesgo la información de los servidores y de los equipos de cómputo.

Aunado a que, de difundirse la información solicitada, permitiría que una persona mal intencionada, pueda buscar en la red cualquier vulnerabilidad para realizar afectaciones, es por ello que, con la reserva propuesta se intenta mitigar la posibilidad de ocasionar pérdidas mayores.

Asimismo, se hace referencia que, al permitir que se identifique el uso de los enlaces de comunicaciones, se estaría vulnerando la operación de la infraestructura tecnológica de Prodecon, lo que podría ocasionar una afectación a la seguridad, vida e integridad de los Contribuyentes; lo que vulnera el interés general, ya que el beneficio se limitaría al derecho del solicitante de obtener información, en donde en todo caso, prevalecería el interés particular sobre el interés público.

VI. En atención a lo anterior, este Comité de Transparencia determina lo siguiente:

Atendiendo la motivación que hizo valer la Dirección de Sistemas Sustantivos, la cual se encuentra encaminada a denotar que con la difusión de la información solicitada se tiene la expectativa razonable de que ocurra un ataque cibernético, toda vez que se facilitaría la identificación de elementos cuyas funciones están encaminadas a preservar la integridad y seguridad de la información, aunado a que, de tener acceso a intervalos máximos o mínimos de uso diario o mensual de las comunicaciones, se permitiría la intrusión de software malicioso para generar tráfico en la red, disfrazando la intrusión de agentes externos a ésta, pasando así desapercibido un ataque de esa naturaleza, lo que ocasionaría la perpetración de actos tendientes a la extracción ilegal de información privilegiada de los contribuyentes y de la propia Entidad, comprometiendo la operación de la Procuraduría.

Lo anterior, pues el dar a conocer el uso o capacidad de los enlaces de comunicaciones puede permitirse a los hackers realizar suplantaciones y darle facilidades para emprender acciones de penetración indebida que ponga en riesgo la información de los servidores y de los equipos de cómputo de la Procuraduría.

Aunado a que, se podrían identificar vulnerabilidades específicas de los equipos informáticos, así como sus mecanismos de seguridad implementados, con el fin de comprometerlos, poniendo en riesgo la operación diaria de la Entidad, ello agravado por el hecho de que ya se compartieron datos que permitirían ocultar estas actividades.

Por lo anterior, en términos del artículo 140, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública, este Comité de Transparencia estima que la información que nos ocupa actualiza la causal de reserva a que se refieren los artículos 113 fracción

VII, de la Ley General de Transparencia y Acceso a la Información Pública; 110 fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con lo preceptuado en el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas; mismos que son de la literalidad siguiente:

> "***Artículo 113.*** *Como información reservada podrá clasificarse aquella cuya publicación:*
>
> *(...)*
>
> ***VII.*** *Obstruya la prevención o persecución de los delitos; (...)"*
>
> *"**Artículo 110.** Conforme a lo dispuesto por el artículo 113 de la Ley General, como información reservada podrá clasificarse aquella cuya publicación:*
> *(...)*
>
> ***VII.*** *Obstruya la prevención o persecución de los delitos; (...)"*
>
> *"**Vigésimo sexto.** De conformidad con el artículo 113, fracción VII de la Ley General, podrá considerarse como información reservada, aquella que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos.*
>
> *Para que se verifique el supuesto de reserva, cuando se cause un perjuicio a las actividades de persecución de los delitos, deben de actualizarse los siguientes elementos:*
>
> ***I.*** *La existencia de un proceso penal en sustanciación o una carpeta de investigación en trámite;*
>
> ***II.*** *Que se acredite el vínculo que existe entre la información solicitada y la carpeta de investigación, o el proceso penal, según sea el caso, y*
>
> ***III.*** *Que la difusión de la información pueda impedir u obstruir las funciones que ejerce el Ministerio Público o su equivalente durante la etapa de investigación o ante los tribunales judiciales con motivo del ejercicio de la acción penal."*

De las citas que preceden, se advierte con meridiana claridad que como información reservada podrá clasificarse aquella cuya publicación obstruya la prevención o persecución de los delitos, siendo de ambas hipótesis la que interesa para el caso que nos atañe

la primera, relativa a la prevención de los delitos; lo anterior, en atención a la naturaleza de las manifestaciones de la Dirección de Sistemas Sustantivos, tendientes a exaltar que la difusión de la información podría tener como consecuencia un ataque intrusivo o cibernético, los cuales se encuentran contenidos en el Capítulo II, del Título Noveno del Código Penal Federal.

Por lo anterior, este Comité de Transparencia considera que, con la entrega de la información relativa a los enlaces de comunicaciones de esta Procuraduría se ocasionaría:

I. Un potencial **riesgo real, demostrable e identificable**, toda vez que se colocaría a esta Procuraduría de la Defensa del Contribuyente en un estado de **vulnerabilidad** toda vez que limitaría su capacidad para evitar que personas ajenas a la Institución pudiesen alterar y/o extraer información que se utiliza en sus actividades cotidianas, ello, pues se permitiría el acceso ilícito a sus equipos informáticos e información contenida en estos, facilitando:

· Una posible intervención de sus comunicaciones,
· La suplantación de sus equipos y de la información que almacena en sus servidores;
· El robo de la información que obra en sus archivos digitales,
· El detrimento de sus instalaciones tecnológicas y
· El hackeo de los sistemas informáticos.

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

II. Un **perjuicio significativo al interés público**, pues la Procuraduría de la Defensa del Contribuyente tiene como objeto garantizar el derecho de los contribuyentes a recibir justicia en materia fiscal en el orden federal, a través de la prestación de los servicios gratuitos de asesoría, representación y defensa, velando por el cumplimiento efectivo de sus derechos, para contribuir a propiciar un ambiente favorable en la construcción de una cultura de plena vigencia de los derechos del contribuyente en nuestro país, así como en la recepción de quejas, reclamaciones o emisión de recomendaciones públicas a las autoridades fiscales federales, a efecto de que se lleguen a corregir aquellas prácticas que indebidamente lesionan o les causan molestias excesivas o innecesarias a los contribuyentes; por lo que, de ser vulnerada su infraestructura tecnológica y equipamiento de la misma índole, 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, lo que de ninguna manera puede estar por encima del interés particular del peticionario.

III. 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 de telecomunicaciones 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 y que se encuentran en posesión del sujeto obligado, conociendo con un alto grado de precisión la información técnica referente a sus equipos, los protocolos de seguridad y las características de la infraestructura instalada.

En esa tónica, derivado de la naturaleza 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 Procuraduría, es que se colige que dar a conocer la misma facilitaría que personas expertas en informática **perturben los sistemas de comunicaciones** con los que cuenta la Entidad y ejecuten programas informáticos perjudiciales que modifiquen o destruyan información relevante; situación que pondría en un **estado vulnerable** la información que en ellos se contiene, facilitando la intervención de las comunicaciones.

VII. Ahora bien, en cuanto al periodo de reserva de la información, este Comité de Transparencia estima pertinente reservar la citada información, por un periodo de **cinco años,** ya que, a juicio de este Comité, dicho plazo es proporcional con la naturaleza y al grado de especificidad del tipo de información de que se trata.

En razón de lo antes expuesto, este Comité de Transparencia **CONFIRMA LA CLASIFICACIÓN** como **RESERVADA** de la información relativa a la evidencia de uso de los enlaces de comunicaciones que se advierten en los entregables de los contratos PRODECON-SG-DGATI-AD-004-2016 y PRODECON-SG-DGACTIC-AD-144-2016, relativos a los periodos de enero de 2017 a diciembre de 2017, contenidos en la prueba de daño que se acompaña a la respuesta de la solicitud de información 0063200004020; lo anterior, de conformidad con lo dispuesto en los artículos 113, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública; 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas; asimismo, se confirma el periodo de cinco años para la reserva que nos ocupa, el cual puede ser ampliado, en términos de lo dispuesto en los artículos 101 y 103 de la Ley General de Transparencia y Acceso a la Información Pública y, 99 y 102 de la Ley Federal de Transparencia y Acceso a la Información Pública.

6.- Discusión y en su caso, confirmación, modificación o revocación de la clasificación de la información realizada por la Dirección de Sistemas Sustantivos, relacionada con la solicitud de acceso a la información pública número 0063200004120.

I. El día 06 de febrero de 2020, el peticionario requirió en la solicitud de información pública número **0063200004120**, lo siguiente:

> ***"Para el periodo de Enero 2018 a Diciembre 2018 se solicita se informe de manera electrónica y proporcione de manera detallada mediante la PNT en archivo de formato de datos abiertos tipo PDF TODA la evidencia que corresponde exclusivamente al uso de los enlaces de comunicaciones y que aparece en los entregables del contrato PRODECON-SG-DGATI-AD-004-2016 y en los entregables del contrato PRODECON-SG-DGATIC-AD-144-2016. Hago énfasis en que la información solicitada es pública, no incluye datos personales y está digitalizada. Por lo tanto no es información reservada ni tampoco Ad hoc"***
>
> *[Sic]*

II. De conformidad con lo dispuesto en los artículos 45, fracciones II y IV, y 131, de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 61, fracciones II y IV, 133 y 134, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP), en debido tiempo y forma, y mediante oficio número **PRODECON/SG/DGAJ/DCN/047/2020**, de fecha 07 de febrero de 2020, la Unidad de Transparencia turnó a la **Dirección de Sistemas Sustantivos**, la solicitud de acceso a la información en estudio, al ser la Unidad Administrativa competente para atender la petición.

III. Atento a lo anterior, mediante oficio **PRODECON/SG/DGA/DSS/014/2020**, de fecha 18 de febrero de 2020, y recibido por la Unidad de Transparencia al día siguiente, la **Dirección de Sistemas Sustantivos**, dio respuesta a la solicitud de información que nos ocupa, señalando en la parte que interesa lo siguiente:

> *"[...] En relación a las evidencias de uso de los enlaces de comunicaciones que aparecen de los entregables a los que hace referencia el peticionario, se advierte que cuentan con información reservada, toda vez que:*
>
> *Un **enlace de comunicaciones** es el medio de conexión entre dos lugares con el propósito de **transmitir y recibir información**. Puede hacer referencia a un conjunto de componentes electrónicos, que consisten en un transmisor y un receptor (dos piezas de un equipo terminal de datos) y el circuito de telecomunicación de datos de interconexión. Esto se rige por un protocolo de enlace que permite que los datos digitales puedan ser transferidos desde una fuente de datos a un receptor de datos.*
>
> *Con relación a la difusión de la información de uso de los enlaces de comunicaciones que se advierten en los entregables a los que hace referencia el solicitante, se advierte que representa un riesgo real en tanto que se facilita la identificación de elementos cuyas funciones están encaminadas a preservar la integridad y seguridad de la información, para un hacker es más fácil penetrar en una red si conoce de los elementos básicos que la conforman, como puede ser Tipo de enlace, Proveedor de servicio, intervalos de uso, ya que estos le permiten focalizar los ataques con algoritmos más precisos debido a los elementos conocidos, asimismo, al tener acceso a intervalos máximos o mínimos (picos) de uso diario o mensual de las comunicaciones, permitiría la intrusión de bots para generar tráfico en la red, disfrazando la intrusión de agentes externos a la red, por lo que pasaría desapercibido un ataque de esta naturaleza, lo que ocasionaría la perpetración de actos que tienden a conocer la información de los contribuyentes, misma que pueden trascender a la afectación de su identidad, a partir de la realización de actos perniciosos en su contra o distintos de sus fines; comprometiendo la operación de Prodecon, lo anterior en virtud de que el dar a conocer el uso y capacidad de los enlaces de comunicaciones, aunado a otros componentes, como son; Dirección IP, Dirección MAC, Segmentos de red, nombres de equipo, número de serie,*

entre otros, puede permitir a los hackers realizar suplantaciones y darles facilidades para que intenten acciones de penetración que pongan en riesgo la información de los servidores y de los equipos de cómputo.

Asimismo, permitiría que la persona mal intencionada pueda buscar en la red cualquier vulnerabilidad para realizar afectaciones mayores, por otra parte, puede extraer información sin que se llegue a detectar por meses, aún con los modernos motores de antimalware y rastreo de patrones por Inteligencia Artificial cabe esa posibilidad, el no tener un presupuesto robusto para buscar medios alternativos de defensa, Prodecon intenta con estas reservas mitigar la posibilidad de ocurrencia de las afectaciones que pueden ocasionar pérdidas mayores.

Por lo tanto, es información que se encuentra reservada, ya que representa un riesgo de ataque informático, toda vez que quien posea esta información puede suplantar la identidad de un usuario válido y tener acceso a los sistemas computacionales, situación que comprometería la información contenida en ellos, asimismo el cruce de información con otros elementos, como el número de serie, dirección MAC, protocolos de comunicación, segmentos de red, entre otros, de cada uno de los equipos comprometerían la disponibilidad, confiabilidad, e integridad de la información de la PRODECON, ya que un posible atacante tendría a su alcance todos los elementos necesarios para hacerse pasar por un usuario válido (suplantación de identidad) e ingresar a la red para intentar ataques informáticos que pueden ser desde la extracción de información (por ejemplo: datos personales), denegación de servicio (impedir la operación informática, inhabilitar los servicios), modificación o alteración de información oficial, publicación o divulgación de información, suplantando la identidad de un equipo válido.

En caso de proporcionar dicha información, se pone en riesgo la seguridad informática y la seguridad de la información de conformidad con el siguiente detalle que consta de la solicitud y las razones para reservar cada punto particular.
[...]"

[Sic]

Asimismo, acompañó a su respuesta la prueba de daño correspondiente, en cuya motivación se señaló expresamente lo siguiente:

"[...]
Sobre el particular, de conformidad con lo dispuesto en los artículos 44, fracción II,100,104, 108 y 114, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, 97,102,105 y 111, de la Ley Federal de Transparencia y Acceso a la Información Pública, y los numerales Segundo, fracción XIV y Sexto, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, se informa que dicha información se encuentra reservada por cuanto hace al enlace de comunicaciones, tal y como se señala en el oficio PRODECON/SG/DGA/DSS/014/2020, mediante

el cual se da respuesta al solicitante, en términos de lo dispuesto en los artículos 113, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública; 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el numeral Vigésimo Sexto, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas; lo anterior, atendiendo a la siguiente:

I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional. *Se advierte que como información reservada podrá clasificarse aquella que obstruya la persecución de los delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión o limitar la capacidad de las autoridades para evitar la comisión de delitos. En atención a lo antes mencionado, proporcionar el dato solicitado limita la capacidad de Prodecon para evitar que personas ajenas alteren y extraigan información que se utiliza en las actividades cotidianas y cumplir con la encomienda de ser la entidad que tiene a su cargo la protección y defensa del contribuyente en materia fiscal.*

La difusión de la información de uso de los enlaces de comunicaciones representa un riesgo real en tanto que se facilita la identificación de elementos cuyas funciones están encaminadas a preservar la integridad y seguridad de la información, para un hacker es más fácil penetrar en una red si conoce de los elementos básicos que la conforman, como puede ser tipo de enlace, nombre del proveedor de servicio, intervalos de uso de la red, sumado a que haya otra(s) solicitud(es) referente(s) a otros componentes, como son; Dirección IP, Dirección MAC, Segmentos de red, nombres de equipo, número de serie, entre otros, lo que potencializaría el riesgo de vulnerar y focalizar los ataques con algoritmos más precisos debido a los elementos conocidos, asimismo al tener acceso a intervalos máximos o mínimos (picos) de uso diario o mensual de las comunicaciones, permitiría la intrusión de bots para generar tráfico en la red, disfrazando la intrusión de agentes externos a la red, por lo que pasaría desapercibido un ataque de esta naturaleza, lo que ocasionaría la perpetración de actos que tienden a conocer la información de los contribuyentes, misma que pueden trascender a la afectación de su identidad, a partir de la realización de actos perniciosos en su contra o distintos de sus fines; comprometiendo la operación de Prodecon, lo anterior en virtud de que el dar a conocer el uso y capacidad de los enlaces de comunicaciones puede permitir a los hackers realizar suplantaciones y darles facilidades para que intenten acciones de penetración que pongan en riesgo la información de los servidores y de los equipos de cómputo.

Asimismo, permitiría que la persona mal intencionada pueda buscar en la red cualquier vulnerabilidad para realizar afectaciones mayores, por otra parte, puede extraer información sin que se llegue a detectar por meses, aún con los modernos motores de antimalware y rastreo de patrones por Inteligencia Artificial cabe esa posibilidad, el no tener un presupuesto robusto para buscar medios alternativos de defensa, Prodecon intenta con

estas reservas mitigar la posibilidad de ocurrencia de las afectaciones que pueden ocasionar pérdidas mayores.

II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda. *Al permitir que se identifique el uso de los enlaces de comunicaciones, se estaría vulnerando la operación de la infraestructura tecnológica de Prodecon, así como afectando el ejercicio de los derechos de los contribuyentes a hacer uso de los servicios que brinda Prodecon. Lo anterior ante la probabilidad de que personas con pretensiones delictivas pudieran aprovechar la identificación de vulnerabilidades de la infraestructura tecnológica o generar irregularidades en la operac1on administrativa y sustantiva y de esta forma perjudicar la reputación de la institución, así como el derecho de los Contribuyentes a recibir justicia fiscal por parte de esta Procuraduría; además, al perpetrar la información que se tiene concentrada de los contribuyentes, la misma quedaría expuesta, propiciando un robo de identidad o mal uso de dicha información, lo que podría ocasionar una afectación a la seguridad, vida e integridad de los Contribuyentes.*

Esto vulnera el interés general, ya que el beneficio se limitaría al derecho del solicitante de obtener información, en donde en todo caso, prevalecería el interés particular sobre el interés público.

III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar perjuicio. *Resguardar únicamente la información que contenga datos de la infraestructura tecnológica que se provee en los servicios de esta procuraduría, en virtud de que al divulgarse la misma, se pondría en riesgo la operación diaria al ser susceptible de hackeos y con ello vulnerar la información de los contribuyentes, por lo que reservar dicha información representa el medio adecuado para lograr el fin precitado.*

Ahora bien, considerando que la información de la PRODECON contiene información sensible de los contribuyentes, entre otros datos, la DSS solicita, de considerarlo viable, se confirme la reserva dichos datos por cinco años, al estimar que dicha temporalidad es adecuada y proporcional para la protección del interés público, en términos de lo previsto en el artículo 99, de la Ley Federal de Transparencia y Acceso a la Información Pública.

Cabe señalar que dicho plazo se puede ampliar de conformidad con el penúltimo párrafo del artículo 99, de la Ley Federal de Transparencia y Acceso a la Información Pública, mismo que establece: "Excepcionalmente, los sujetos obligados, con la aprobación de su Comité de Transparencia, podrán ampliar el periodo de reserva hasta por un plazo de cinco años adicionales, siempre y cuando justifiquen que subsisten las causa que dieron origen a su clasificación, mediante la aplicación de una prueba de daño".
[...]" *[Sic]*

IV. Atento a la clasificación de la información propuesta por la Dirección de Sistemas Sustantivos; en términos de lo establecido en los artículos 137, de la Ley General de Transparencia y Acceso a la Información Pública y 140, de la Ley Federal de Transparencia y Acceso a la Información pública, se tiene por recibida en este Comité de Transparencia para los efectos conducentes.

V. En esa tesitura, del análisis a la prueba de daño que acompañó la Unidad Administrativa a su respuesta, se puede observar que reservó la información relativa a la evidencia de uso de los enlaces de comunicaciones que se advierten en los entregables de los contratos PRODECON-SG-DGATI-AD-004-2016 y PRODECON-SG-DGACTIC-AD-144-2016, relativos a los periodos de enero de 2018 a diciembre de 2018, en términos de lo previsto en los artículos 113 fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública; 110 fracción VII, de la Ley Federal de Transparencia y acceso a la Información Pública; así como el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

Y al respecto, expresó esencialmente los siguientes motivos:

Que un enlace de comunicaciones es el medio de conexión entre dos lugares con el propósito de transmitir y recibir información. Puede hacer referencia a un conjunto de componentes electrónicos, que consisten en un transmisor y un receptor (dos piezas de un equipo terminal de datos) y el circuito de telecomunicación de datos de interconexión. Esto se rige por un protocolo de enlace que permite que los datos digitales pueden ser transferidos desde una fuente de datos a un receptor de datos.

Que con la difusión de la información requerida se limita la capacidad de Prodecon para evitar que personas ajenas alteren y extraigan información que se utiliza en las actividades cotidianas, por lo que conllevaría a un incumplimiento en su encomienda de brindar protección y defensa a los contribuyentes en materia fiscal.

Lo anterior en virtud de que, de proporcionarse la información solicitada, se facilitaría la identificación de elementos cuyas funciones están encaminadas a preservar la integridad y seguridad de la información, toda vez que para un Hacker le es más fácil entrar en una red si conoce los elementos básicos que la conforman, como pueden ser el tipo de enlace, proveedor de servicio, intervalos de uso, sumado

a que en otras solicitudes se ha solicitado información relativa a otros componentes; lo que potencializaría el riesgo de vulnerar y focalizar los ataques con algoritmos más precisos debido a los elementos conocidos; asimismo, al tener acceso a intervalos máximos o mínimos (picos) de uso diario o mensual de las comunicaciones, permitiría la intrusión de bots para generar tráfico en la red, disfrazando la intrusión de agentes externos a la red, por lo que pasaría desapercibido un ataque de esta naturaleza, lo que ocasionaría la perpetración de actos que tienden a conocer la información de los contribuyentes, misma que pueden trascender a la afectación de su identidad, a partir de la realización de actos perniciosos en su contra o distintos de sus fines; comprometiendo la operación de la Entidad, lo anterior en virtud de que el dar a conocer el uso y capacidad de los enlaces de comunicaciones puede permitir a los hackers realizar suplantaciones y darles facilidades para que intenten acciones de penetración que pongan en riesgo la información de los servidores y de los equipos de cómputo.

Aunado a que, de difundirse la información solicitada, permitiría que una persona mal intencionada, pueda buscar en la red cualquier vulnerabilidad para realizar afectaciones, es por ello que, con la reserva propuesta se intenta mitigar la posibilidad de ocasionar pérdidas mayores.

Asimismo, se hace referencia que, al permitir que se identifique el uso de los enlaces de comunicaciones, se estaría vulnerando la operación de la infraestructura tecnológica de Prodecon, lo que podría ocasionar una afectación a la seguridad, vida e integridad de los Contribuyentes; lo que vulnera el interés general, ya que el beneficio se limitaría al derecho del solicitante de obtener información, en donde en todo caso, prevalecería el interés particular sobre el interés público.

VI. En atención a lo anterior, este Comité de Transparencia determina lo siguiente:

Atendiendo la motivación que hizo valer la Dirección de Sistemas Sustantivos, la cual se encuentra encaminada a denotar que con la difusión de la información solicitada se tiene la expectativa razonable de que ocurra un ataque cibernético, toda vez que se facilitaría la identificación de elementos cuyas funciones están encaminadas a preservar la integridad y seguridad de la información, aunado a que, de tener acceso a intervalos máximos o mínimos de uso diario o mensual de las comunicaciones, se permitiría la intrusión de software

malicioso para generar tráfico en la red, disfrazando la intrusión de agentes externos a ésta, pasando así desapercibido un ataque de esa naturaleza, lo que ocasionaría la perpetración de actos tendientes a la extracción ilegal de información privilegiada de los contribuyentes y de la propia Entidad, comprometiendo la operación de la Procuraduría.

Lo anterior, pues el dar a conocer el uso o capacidad de los enlaces de comunicaciones puede permitirse a los hackers realizar suplantaciones y darle facilidades para emprender acciones de penetración indebida que ponga en riesgo la información de los servidores y de los equipos de cómputo de la Procuraduría.

Aunado a que, se podrían identificar vulnerabilidades específicas de los equipos informáticos, así como sus mecanismos de seguridad implementados, con el fin de comprometerlos, poniendo en riesgo la operación diaria de la Entidad, ello agravado por el hecho de que ya se compartieron datos que permitirían ocultar estas actividades.

Por lo anterior, en términos del artículo 140, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública, este Comité de Transparencia estima que la información que nos ocupa actualiza la causal de reserva a que se refieren los artículos 113 fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública; 110 fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con lo preceptuado en el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas; mismos que son de la literalidad siguiente:

> "***Artículo 113.*** *Como información reservada podrá clasificarse aquella cuya publicación:*
>
> *(...)*
>
> ***VII.*** *Obstruya la prevención o persecución de los delitos; (...)"*
>
> *"**Artículo 110.** Conforme a lo dispuesto por el artículo 113 de la Ley General, como información reservada podrá clasificarse aquella cuya publicación:*
> *(...)*
>
> ***VII.*** *Obstruya la prevención o persecución de los delitos; (...)"*

*"**Vigésimo sexto.** De conformidad con el artículo 113, fracción VII de la Ley General, podrá considerarse como información reservada, aquella que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos.*

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

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

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

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

De la citas que preceden, se advierte con meridiana claridad que como información reservada podrá clasificarse aquella cuya publicación obstruya la prevención o persecución de los delitos, siendo de ambas hipótesis la que interesa para el caso que nos atañe la primera, relativa a la prevención de los delitos; lo anterior, en atención a la naturaleza de las manifestaciones de la Dirección de Sistemas Sustantivos, tendientes a exaltar que la difusión de la información podría tener como consecuencia un ataque intrusivo o cibernético, los cuales se encuentran contenidos en el Capítulo II, del Título Noveno del Código Penal Federal.

Por lo anterior, este Comité de Transparencia considera que, con la entrega de la información relativa a los enlaces de comunicaciones de esta Procuraduría se ocasionaría:

I. Un potencial **riesgo real, demostrable e identificable**, toda vez que se colocaría a esta Procuraduría de la Defensa del Contribuyente en un estado de **vulnerabilidad** toda vez que limitaría su capacidad para evitar que personas ajenas a la Institución pudiesen alterar y/o extraer información que se utiliza en sus actividades cotidianas, ello, pues se permitiría el acceso ilícito a sus equipos informáticos e información contenida en estos, facilitando:

· Una posible intervención de sus comunicaciones,
· La suplantación de sus equipos y de la información que almacena en sus servidores;
· El robo de la información que obra en sus archivos digitales,
· El detrimento de sus instalaciones tecnológicas y
· El hackeo de los sistemas informáticos.

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

II. Un **perjuicio significativo al interés público**, pues la Procuraduría de la Defensa del Contribuyente tiene como objeto garantizar el derecho de los contribuyentes a recibir justicia en materia fiscal en el orden federal, a través de la prestación de los servicios gratuitos de asesoría, representación y defensa, velando por el cumplimiento efectivo de sus derechos, para contribuir a propiciar un ambiente favorable en la construcción de una cultura de plena vigencia de los derechos del contribuyente en nuestro país, así como en la recepción de quejas, reclamaciones o emisión de recomendaciones públicas a las autoridades fiscales federales, a efecto de que se lleguen a corregir aquellas prácticas que indebidamente lesionan o les causan molestias excesivas o innecesarias a los contribuyentes; por lo que, de ser vulnerada su infraestructura tecnológica y equipamiento de la misma índole, 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, lo que de ninguna manera puede estar por encima del interés particular del peticionario.

III. 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 de telecomunicaciones 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 y que se encuentran en posesión del sujeto obligado, conociendo con un alto grado de precisión la información técnica referente a sus equipos, los protocolos de seguridad y las características de la infraestructura instalada.

En esa tónica, derivado de la naturaleza 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 Procuraduría, es que se colige que dar a conocer la misma facilitaría que personas expertas en informática **perturben los sistemas de comunicaciones** con los que cuenta la Entidad y ejecuten programas informáticos perjudiciales que modifiquen o destruyan información relevante; situación que pondría en un **estado vulnerable** la información que en ellos se contiene, facilitando la intervención de las comunicaciones.

VII. Ahora bien, en cuanto al periodo de reserva de la información, este Comité de Transparencia estima pertinente reservar la citada información, por un periodo de **cinco años,** ya que, a juicio de este Comité, dicho plazo es proporcional con la naturaleza y al grado de especificidad del tipo de información de que se trata.

En razón de lo antes expuesto, este Comité de Transparencia **CONFIRMA LA CLASIFICACIÓN** como **RESERVADA** de la información relativa a la evidencia de uso de los enlaces de comunicaciones que se advierten en los entregables de los contratos PRODECON-SG-DGATI-AD-004-2016 y PRODECON-SG-DGACTIC-AD-144-2016, relativos a los periodos de enero de 2018 a diciembre de 2018, contenidos en la prueba de daño que se acompaña a la respuesta de la solicitud de información 0063200004120; lo anterior, de conformidad con lo dispuesto en los artículos 113, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública; 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y

Desclasificación de la Información, así como para la Elaboración de Versiones Públicas; asimismo, se confirma el periodo de cinco años para la reserva que nos ocupa, el cual puede ser ampliado, en términos de lo dispuesto en los artículos 101 y 103 de la Ley General de Transparencia y Acceso a la Información Pública y, 99 y 102 de la Ley Federal de Transparencia y Acceso a la Información Pública.

7.- Discusión y en su caso, confirmación, modificación o revocación de la clasificación de la información realizada por la Dirección de Sistemas Sustantivos, relacionada con la solicitud de acceso a la información pública número 0063200004220.

I. El día 06 de febrero de 2020, el peticionario requirió en la solicitud de información pública número **0063200004220**, lo siguiente:

> ***"Para el periodo de Enero 2019 a Diciembre 2019 se solicita se informe de manera electrónica y proporcione de manera detallada mediante la PNT en archivo de formato de datos abiertos tipo PDF TODA la evidencia que corresponde exclusivamente al uso de los enlaces de comunicaciones y que aparece en los entregables del contrato PRODECON-SG-DGATI-AD-004-2016 y en los entregables del contrato PRODECON-SG-DGATIC-AD-144-2016. Hago énfasis en que la información solicitada es pública, no incluye datos personales y está digitalizada. Por lo tanto no es información reservada ni tampoco Ad hoc"***
>
> *[Sic]*

II. De conformidad con lo dispuesto en los artículos 45, fracciones II y IV, y 131, de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 61, fracciones II y IV, 133 y 134, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP), en debido tiempo y forma, y mediante oficio número **PRODECON/SG/DGAJ/DCN/048/2020**, de fecha 07 de febrero de 2020, la Unidad de Transparencia turnó a la **Dirección de Sistemas Sustantivos**, la solicitud de acceso a la información en estudio, al ser la Unidad Administrativa competente para atender la petición.

III. Atento a lo anterior, mediante oficio **PRODECON/SG/DGA/DSS/015/2020**, de fecha 18 de febrero de 2020, y recibido por la Unidad de Transparencia al día siguiente, la **Dirección de Sistemas Sustantivos**, dio respuesta a la solicitud de información que nos ocupa, señalando en la parte que interesa lo siguiente:

"[...] En relación a las evidencias de uso de los enlaces de comunicaciones que aparecen de los entregables a los que hace referencia el peticionario, se advierte que cuentan con información reservada, toda vez que:

*Un **enlace de comunicaciones** es el medio de conexión entre dos lugares con el propósito de **transmitir y recibir información**. Puede hacer referencia a un conjunto de componentes electrónicos, que consisten en un transmisor y un receptor (dos piezas de un equipo terminal de datos) y el circuito de telecomunicación de datos de interconexión. Esto se rige por un protocolo de enlace que permite que los datos digitales puedan ser transferidos desde una fuente de datos a un receptor de datos.*

Con relación a la difusión de la información de uso de los enlaces de comunicaciones que se advierten en los entregables a los que hace referencia el solicitante, se advierte que representa un riesgo real en tanto que se facilita la identificación de elementos cuyas funciones están encaminadas a preservar la integridad y seguridad de la información, para un hacker es más fácil penetrar en una red si conoce de los elementos básicos que la conforman, como puede ser Tipo de enlace, Proveedor de servicio, intervalos de uso, ya que estos le permiten focalizar los ataques con algoritmos más precisos debido a los elementos conocidos, asimismo, al tener acceso a intervalos máximos o mínimos (picos) de uso diario o mensual de las comunicaciones, permitiría la intrusión de bots para generar tráfico en la red, disfrazando la intrusión de agentes externos a la red, por lo que pasaría desapercibido un ataque de esta naturaleza, lo que ocasionaría la perpetración de actos que tienden a conocer la información de los contribuyentes, misma que pueden trascender a la afectación de su identidad, a partir de la realización de actos perniciosos en su contra o distintos de sus fines; comprometiendo la operación de Prodecon, lo anterior en virtud de que el dar a conocer el uso y capacidad de los enlaces de comunicaciones, aunado a otros componentes, como son; Dirección IP, Dirección MAC, Segmentos de red, nombres de equipo, número de serie, entre otros, puede permitir a los hackers realizar suplantaciones y darles facilidades para que intenten acciones de penetración que pongan en riesgo la información de los servidores y de los equipos de cómputo.

Asimismo, permitiría que la persona mal intencionada pueda buscar en la red cualquier vulnerabilidad para realizar afectaciones mayores, por otra parte, puede extraer información sin que se llegue a detectar por meses, aún con los modernos motores de antimalware y rastreo de patrones por Inteligencia Artificial cabe esa posibilidad, el no tener un presupuesto robusto para buscar medios alternativos de defensa, Prodecon intenta con estas reservas mitigar la posibilidad de ocurrencia de las afectaciones que pueden ocasionar pérdidas mayores.

Por lo tanto, es información que se encuentra reservada, ya que representa un riesgo de ataque informático, toda vez que quien posea esta información puede suplantar la identidad de un usuario válido y tener acceso a los sistemas computacionales, situación que comprometería la

información contenida en ellos, asimismo el cruce de información con otros elementos, como el número de serie, dirección MAC, protocolos de comunicación, segmentos de red, entre otros, de cada uno de los equipos comprometerían la disponibilidad, confiabilidad, e integridad de la información de la PRODECON, ya que un posible atacante tendría a su alcance todos los elementos necesarios para hacerse pasar por un usuario válido (suplantación de identidad) e ingresar a la red para intentar ataques informáticos que pueden ser desde la extracción de información (por ejemplo: datos personales), denegación de servicio (impedir la operación informática, inhabilitar los servicios), modificación o alteración de información oficial, publicación o divulgación de información, suplantando la identidad de un equipo válido.

En caso de proporcionar dicha información, se pone en riesgo la seguridad informática y la seguridad de la información de conformidad con el siguiente detalle que consta de la solicitud y las razones para reservar cada punto particular.
[...]"

[Sic]

Asimismo, acompañó a su respuesta la prueba de daño correspondiente, en cuya motivación se señaló expresamente lo siguiente:

"[...]
Sobre el particular, de conformidad con lo dispuesto en los artículos 44, fracción II,100,104, 108 y 114, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, 97,102,105 y 111, de la Ley Federal de Transparencia y Acceso a la Información Pública, y los numerales Segundo, fracción XIV y Sexto, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, se informa que dicha información se encuentra reservada por cuanto hace al enlace de comunicaciones, tal y como se señala en el oficio PRODECON/SG/DGA/DSS/015/2020, mediante

el cual se da respuesta al solicitante, en términos de lo dispuesto en los artículos 113, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública; 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el numeral Vigésimo Sexto, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas; lo anterior, atendiendo a la siguiente:

I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional. *Se advierte que como información reservada podrá clasificarse aquella que obstruya la persecución de los delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión o limitar la capacidad de las autoridades para evitar la comisión de delitos. En atención a lo antes mencionado, proporcionar el dato solicitado limita la capacidad de Prodecon para evitar que personas ajenas*

alteren y extraigan información que se utiliza en las actividades cotidianas y cumplir con la encomienda de ser la entidad que tiene a su cargo la protección y defensa del contribuyente en materia fiscal.

La difusión de la información de uso de los enlaces de comunicaciones representa un riesgo real en tanto que se facilita la identificación de elementos cuyas funciones están encaminadas a preservar la integridad y seguridad de la información, para un hacker es más fácil penetrar en una red si conoce de los elementos básicos que la conforman, como puede ser tipo de enlace, nombre del proveedor de servicio, intervalos de uso de la red, sumado a que haya otra(s) solicitud(es) referente(s) a otros componentes, como son; Dirección IP, Dirección MAC, Segmentos de red, nombres de equipo, número de serie, entre otros, lo que potencializaría el riesgo de vulnerar y focalizar los ataques con algoritmos más precisos debido a los elementos conocidos, asimismo al tener acceso a intervalos máximos o mínimos (picos) de uso diario o mensual de las comunicaciones, permitiría la intrusión de bots para generar tráfico en la red, disfrazando la intrusión de agentes externos a la red, por lo que pasaría desapercibido un ataque de esta naturaleza, lo que ocasionaría la perpetración de actos que tienden a conocer la información de los contribuyentes, misma que pueden trascender a la afectación de su identidad, a partir de la realización de actos perniciosos en su contra o distintos de sus fines; comprometiendo la operación de Prodecon, lo anterior en virtud de que el dar a conocer el uso y capacidad de los enlaces de comunicaciones puede permitir a los hackers realizar suplantaciones y darles facilidades para que intenten acciones de penetración que pongan en riesgo la información de los servidores y de los equipos de cómputo.

Asimismo, permitiría que la persona mal intencionada pueda buscar en la red cualquier vulnerabilidad para realizar afectaciones mayores, por otra parte, puede extraer información sin que se llegue a detectar por meses, aún con los modernos motores de antimalware y rastreo de patrones por Inteligencia Artificial cabe esa posibilidad, el no tener un presupuesto robusto para buscar medios alternativos de defensa, Prodecon intenta con estas reservas mitigar la posibilidad de ocurrencia de las afectaciones que pueden ocasionar pérdidas mayores.

II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda. *Al permitir que se identifique el uso de los enlaces de comunicaciones, se estaría vulnerando la operación de la infraestructura tecnológica de Prodecon, así como afectando el ejercicio de los derechos de los contribuyentes a hacer uso de los servicios que brinda Prodecon. Lo anterior ante la probabilidad de que personas con pretensiones delictivas pudieran aprovechar la identificación de vulnerabilidades de la infraestructura tecnológica o generar irregularidades en la operación administrativa y sustantiva y de esta forma perjudicar la reputación de la institución, así como el derecho de los Contribuyentes a recibir justicia fiscal por parte de esta Procuraduría; además, al perpetrar la información que se tiene concentrada de los contribuyentes, la misma quedaría expuesta, propiciando un robo de*

identidad o mal uso de dicha información, lo que podría ocasionar una afectación a la seguridad, vida e integridad de los Contribuyentes.

Esto vulnera el interés general, ya que el beneficio se limitaría al derecho del solicitante de obtener información, en donde en todo caso, prevalecería el interés particular sobre el interés público.

III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar perjuicio. *Resguardar únicamente la información que contenga datos de la infraestructura tecnológica que se provee en los servicios de esta procuraduría, en virtud de que al divulgarse la misma, se pondría en riesgo la operación diaria al ser susceptible de hackeos y con ello vulnerar la información de los contribuyentes, por lo que reservar dicha información representa el medio adecuado para lograr el fin precitado.*

Ahora bien, considerando que la información de la PRODECON contiene información sensible de los contribuyentes, entre otros datos, la DSS solicita, de considerarlo viable, se confirme la reserva dichos datos por cinco años, al estimar que dicha temporalidad es adecuada y proporcional para la protección del interés público, en términos de lo previsto en el artículo-99, de la Ley Federal de Transparencia y Acceso a la Información Pública.

Cabe señalar que dicho plazo se puede ampliar de conformidad con el penúltimo párrafo del artículo 99, de la Ley Federal de Transparencia y Acceso a la Información Pública, mismo que establece: "Excepcionalmente, los sujetos obligados, con la aprobación de su Comité de Transparencia, podrán ampliar el periodo de reserva hasta por un plazo de cinco años adicionales, siempre y cuando justifiquen que subsisten las causa que dieron origen a su clasificación, mediante la aplicación de una prueba de daño".[...]"

[Sic]

IV. Atento a la clasificación de la información propuesta por la Dirección de Sistemas Sustantivos; en términos de lo establecido en los artículos 137, de la Ley General de Transparencia y Acceso a la Información Pública y 140, de la Ley Federal de Transparencia y Acceso a la Información pública, se tiene por recibida en este Comité de Transparencia para los efectos conducentes.

V. En esa tesitura, del análisis a la prueba de daño que acompañó la Unidad Administrativa a su respuesta, se puede observar que reservó la información relativa a la evidencia de uso de los enlaces de comunicaciones que se advierten en los entregables de los contratos PRODECON-SG-DGATI-AD-004-2016 y PRODECON-SG-DGACTIC-AD-144-2016, relativos a los periodos de enero de 2019 a diciembre de 2019, en términos de lo previsto en los artículos 113 fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública; 110

fracción VII, de la Ley Federal de Transparencia y acceso a la Información Pública; así como el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

Y al respecto, expresó esencialmente los siguientes motivos:

Que un enlace de comunicaciones es el medio de conexión entre dos lugares con el propósito de transmitir y recibir información. Puede hacer referencia a un conjunto de componentes electrónicos, que consisten en un transmisor y un receptor (dos piezas de un equipo terminal de datos) y el circuito de telecomunicación de datos de interconexión. Esto se rige por un protocolo de enlace que permite que los datos digitales pueden ser transferidos desde una fuente de datos a un receptor de datos.

Que con la difusión de la información requerida se limita la capacidad de Prodecon para evitar que personas ajenas alteren y extraigan información que se utiliza en las actividades cotidianas, por lo que conllevaría a un incumplimiento en su encomienda de brindar protección y defensa a los contribuyentes en materia fiscal.

Lo anterior en virtud de que, de proporcionarse la información solicitada, se facilitaría la identificación de elementos cuyas funciones están encaminadas a preservar la integridad y seguridad de la información, toda vez que para un Hacker le es más fácil entrar en una red si conoce los elementos básicos que la conforman, como pueden ser el tipo de enlace, proveedor de servicio, intervalos de uso, sumado a que en otras solicitudes se ha solicitado información relativa a otros componentes; lo que potencializaría el riesgo de vulnerar y focalizar los ataques con algoritmos más precisos debido a los elementos conocidos; asimismo, al tener acceso a intervalos máximos o mínimos (picos) de uso diario o mensual de las comunicaciones, permitiría la intrusión de bots para generar tráfico en la red, disfrazando la intrusión de agentes externos a la red, por lo que pasaría desapercibido un ataque de esta naturaleza, lo que ocasionaría la perpetración de actos que tienden a conocer la información de los contribuyentes, misma que pueden trascender a la afectación de su identidad, a partir de la realización de actos perniciosos en su contra o distintos de sus fines; comprometiendo la operación de la Entidad, lo anterior en virtud de que el dar a conocer el uso y capacidad de los enlaces de comunicaciones puede permitir a los hackers realizar suplantaciones y darles facilidades para que intenten acciones de penetración que

pongan en riesgo la información de los servidores y de los equipos de cómputo.

Aunado a que, de difundirse la información solicitada, permitiría que una persona mal intencionada, pueda buscar en la red cualquier vulnerabilidad para realizar afectaciones, es por ello que, con la reserva propuesta se intenta mitigar la posibilidad de ocasionar pérdidas mayores.

Asimismo, se hace referencia que, al permitir que se identifique el uso de los enlaces de comunicaciones, se estaría vulnerando la operación de la infraestructura tecnológica de Prodecon, lo que podría ocasionar una afectación a la seguridad, vida e integridad de los Contribuyentes; lo que vulnera el interés general, ya que el beneficio se limitaría al derecho del solicitante de obtener información, en donde en todo caso, prevalecería el interés particular sobre el interés público.

VI. En atención a lo anterior, este Comité de Transparencia determina lo siguiente:

Atendiendo la motivación que hizo valer la Dirección de Sistemas Sustantivos, la cual se encuentra encaminada a denotar que con la difusión de la información solicitada se tiene la expectativa razonable de que ocurra un ataque cibernético, toda vez que se facilitaría la identificación de elementos cuyas funciones están encaminadas a preservar la integridad y seguridad de la información, aunado a que, de tener acceso a intervalos máximos o mínimos de uso diario o mensual de las comunicaciones, se permitiría la intrusión de software malicioso para generar tráfico en la red, disfrazando la intrusión de agentes externos a ésta, pasando así desapercibido un ataque de esa naturaleza, lo que ocasionaría la perpetración de actos tendientes a la extracción ilegal de información privilegiada de los contribuyentes y de la propia Entidad, comprometiendo la operación de la Procuraduría.

Lo anterior, pues el dar a conocer el uso o capacidad de los enlaces de comunicaciones puede permitirse a los hackers realizar suplantaciones y darle facilidades para emprender acciones de penetración indebida que ponga en riesgo la información de los servidores y de los equipos de cómputo de la Procuraduría.

Aunado a que, se podrían identificar vulnerabilidades específicas de los equipos informáticos, así como sus mecanismos de seguridad implementados, con el fin de comprometerlos, poniendo en riesgo la

operación diaria de la Entidad, ello agravado por el hecho de que ya se compartieron datos que permitirían ocultar estas actividades.

Por lo anterior, en términos del artículo 140, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública, este Comité de Transparencia estima que la información que nos ocupa actualiza la causal de reserva a que se refieren los artículos 113 fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública; 110 fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con lo preceptuado en el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas; mismos que son de la literalidad siguiente:

> "***Artículo 113.*** *Como información reservada podrá clasificarse aquella cuya publicación:*
>
> *(...)*
>
> ***VII.*** *Obstruya la prevención o persecución de los delitos; (...)"*
>
> *"**Artículo 110.** Conforme a lo dispuesto por el artículo 113 de la Ley General, como información reservada podrá clasificarse aquella cuya publicación:*
> *(...)*
>
> ***VII.*** *Obstruya la prevención o persecución de los delitos; (...)"*
>
> *"**Vigésimo sexto.** De conformidad con el artículo 113, fracción VII de la Ley General, podrá considerarse como información reservada, aquella que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos.*
>
> *Para que se verifique el supuesto de reserva, cuando se cause un perjuicio a las actividades de persecución de los delitos, deben de actualizarse los siguientes elementos:*
>
> ***I.*** *La existencia de un proceso penal en sustanciación o una carpeta de investigación en trámite;*
>
> ***II.*** *Que se acredite el vínculo que existe entre la información solicitada y la carpeta de investigación, o el proceso penal, según sea el caso, y*

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

De la citas que preceden, se advierte con meridiana claridad que como información reservada podrá clasificarse aquella cuya publicación obstruya la prevención o persecución de los delitos, siendo de ambas hipótesis la que interesa para el caso que nos atañe la primera, relativa a la prevención de los delitos; lo anterior, en atención a la naturaleza de las manifestaciones de la Dirección de Sistemas Sustantivos, tendientes a exaltar que la difusión de la información podría tener como consecuencia un ataque intrusivo o cibernético, los cuales se encuentran contenidos en el Capítulo II, del Título Noveno del Código Penal Federal.

Por lo anterior, este Comité de Transparencia considera que, con la entrega de la información relativa a los enlaces de comunicaciones de esta Procuraduría se ocasionaría:

I. Un potencial **riesgo real, demostrable e identificable**, toda vez que se colocaría a esta Procuraduría de la Defensa del Contribuyente en un estado de **vulnerabilidad** toda vez que limitaría su capacidad para evitar que personas ajenas a la Institución pudiesen alterar y/o extraer información que se utiliza en sus actividades cotidianas, ello, pues se permitiría el acceso ilícito a sus equipos informáticos e información contenida en estos, facilitando:

· Una posible intervención de sus comunicaciones,
· La suplantación de sus equipos y de la información que almacena en sus servidores;
· El robo de la información que obra en sus archivos digitales,
· El detrimento de sus instalaciones tecnológicas y
· El hackeo de los sistemas informáticos.

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

II. Un **perjuicio significativo al interés público**, pues la Procuraduría de la Defensa del Contribuyente tiene como objeto garantizar el derecho de los contribuyentes a recibir justicia en materia fiscal en el orden federal, a través de la prestación de los servicios gratuitos de

asesoría, representación y defensa, velando por el cumplimiento efectivo de sus derechos, para contribuir a propiciar un ambiente favorable en la construcción de una cultura de plena vigencia de los derechos del contribuyente en nuestro país, así como en la recepción de quejas, reclamaciones o emisión de recomendaciones públicas a las autoridades fiscales federales, a efecto de que se lleguen a corregir aquellas prácticas que indebidamente lesionan o les causan molestias excesivas o innecesarias a los contribuyentes; por lo que, de ser vulnerada su infraestructura tecnológica y equipamiento de la misma índole, 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, lo que de ninguna manera puede estar por encima del interés particular del peticionario.

III. 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 de telecomunicaciones 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 y que se encuentran en posesión del sujeto obligado, conociendo con un alto grado de precisión la información técnica referente a sus equipos, los protocolos de seguridad y las características de la infraestructura instalada.

En esa tónica, derivado de la naturaleza 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 Procuraduría, es que se colige que dar a conocer la misma facilitaría que personas expertas en informática **perturben los sistemas de comunicaciones** con los que cuenta la Entidad y ejecuten programas informáticos perjudiciales que modifiquen o destruyan información relevante; situación que pondría en un **estado vulnerable** la información que en ellos se contiene, facilitando la intervención de las comunicaciones.

VII. Ahora bien, en cuanto al periodo de reserva de la información, este Comité de Transparencia estima pertinente reservar la citada información, por un periodo de **cinco años,** ya que, a juicio de este Comité, dicho plazo es proporcional con la naturaleza y al grado de especificidad del tipo de información de que se trata.

En razón de lo antes expuesto, este Comité de Transparencia **CONFIRMA LA CLASIFICACIÓN** como **RESERVADA** de la información relativa a la evidencia de uso de los enlaces de comunicaciones que se advierten en los entregables de los contratos PRODECON-SG-DGATI-AD-004-2016 y PRODECON-SG-DGACTIC-AD-144-2016, relativos a los periodos de enero de 2019 a diciembre de 2019, contenidos en la prueba de daño que se acompaña a la respuesta de la solicitud de información 0063200004220; lo anterior, de conformidad con lo dispuesto en los artículos 113, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública; 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas; asimismo, se confirma el periodo de cinco años para la reserva que nos ocupa, el cual puede ser ampliado, en términos de lo dispuesto en los artículos 101 y 103 de la Ley General de Transparencia y Acceso a la Información Pública y, 99 y 102 de la Ley Federal de Transparencia y Acceso a la Información Pública.

8.- Discusión y en su caso, confirmación, modificación o revocación de la clasificación de la información realizada por la Dirección de Recursos Financieros, relacionada con la solicitud de acceso a la información pública número 0063200004320.

I. El día 06 de febrero de 2020, el peticionario requirió en la solicitud de acceso a la información pública, lo siguiente:

"Se solicita se informe de manera electrónica y proporcione de manera detallada mediante la PNT en archivo de formato de datos abiertos tipo PDF las cuentas pagadas a la empresa BERLITZ DE MEXICO y la empresa ANGLO MEXICAN por servicios de capacitación desde Enero 2015 hasta Abril 2019. También se requiere que proporcione evidencia de la búsqueda exhaustiva realizada en los registros electrónicos y expedientes físicos de finanzas. Hago énfasis en que la información solicitada es pública,

debe existir en el GRP Gubernamental y no incluye datos personales. Por lo tanto no es información reservada ni tampoco Ad hoc. En caso de que la información contenga accidentalmente algún dato personal, favor de elaborar y proporcionar la versión pública."

[Sic]

II. De conformidad con lo dispuesto en los artículos 45, fracciones II y IV, y 131, de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 61, fracciones II y IV, 133 y 134, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP), en debido tiempo y forma, y mediante oficio número **PRODECON/SG/DGAJ/DCN/049/2020**, de fecha 07 de febrero de 2020, la Unidad de Transparencia turnó a la **Dirección de Recursos Financieros**, la solicitud de acceso a la información en estudio, por tratarse de un asunto de su competencia.

III. A través del oficio **PRODECON/SG/DGA/DRF/018/2020**, de fecha 19 de febrero de 2020, y recibido por la Unidad de Transparencia el mismo día, la Unidad Administrativa mencionada en el numeral que antecede, dio respuesta a la solicitud de información que nos ocupa, señalando en la parte que interesa lo siguiente:

"[...] De la búsqueda minuciosa y exhaustiva realizada a las bases de datos y controles internos con los que cuenta esta Dirección, se adjunta (...) así como la versión pública de la factura número 19448 y 19483 ambas facturas con un importe total de $23,999.82 (Veintitrés mil novecientos noventa y nueve 82/100. M.N) las cuales corresponden al servicio mencionado por él peticionario.

Cabe precisar, que se solicita se someta a consideración del Comité de Transparencia de esta Entidad la versión pública de la factura referida en el párrafo que antecede.
[...]"

[Sic]

Además, tal y como lo manifestó, acompañó a su respuesta las versiones públicas de las referidas facturas, en cuya motivación se señaló expresamente lo siguiente:

Factura con número de folio	Motivación
DELF19448	"Se eliminan 6 palabras relativas a Folio Fiscal, CSD del Emisor, CSD del SAT, Cadena Original del Timbre, Sello Digital del Emisor, Sello Digital del SAT y 1 Código Bidimensional. Lo anterior por considerarse información confidencial, que de difundirse vulneraría la intimidad de las personas. Por lo tanto, de conformidad con lo dispuesto en los artículos 116, último párrafo de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 113, fracción III, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP), y los Numerales Trigésimo Octavo, fracción II, y Cuadragésimo, de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, esta información se clasifica como **CONFIDENCIAL**, lo que prohíbe su publicidad."

Factura con número de folio	Motivación
DELF19483	"Se eliminan 6 palabras relativas a Folio Fiscal, CSD del Emisor, CSD del SAT, Cadena Original del Timbre, Sello Digital del Emisor, Sello Digital del SAT y 1 Código Bidimensional. Lo anterior por considerarse información confidencial, que de difundirse vulneraría la intimidad de las personas. Por lo tanto, de conformidad con lo dispuesto en los artículos 116, último párrafo de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 113, fracción III, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP), y los Numerales Trigésimo Octavo, fracción II, y Cuadragésimo, de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, esta información se clasifica como **CONFIDENCIAL**, lo que prohíbe su publicidad."

IV. Atento a lo anterior, en términos de lo establecido en los artículos 137, de la Ley General de Transparencia y Acceso a la Información Pública y 140, de la Ley Federal de Transparencia y Acceso a la Información Pública, se tiene por recibida en este Comité de Transparencia la clasificación de la información realizada en las versiones públicas elaboradas por la Dirección de Recursos Financieros, para los efectos conducentes.

Ahora bien, del análisis a las versiones públicas de trato, se advierte que la clasificación de la información se realizó en términos de lo dispuesto en los artículos 116, último párrafo, de la Ley General de Transparencia y Acceso a la Información Pública; 113, fracción III, de la Ley Federal de Transparencia y Acceso a la Información Pública, así como en los

numerales Trigésimo Octavo, fracción II y Cuadragésimo, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas, al considerarse confidencial.

V. En atención a lo anterior, este Comité de Transparencia determina lo siguiente:

Los datos omitidos en las versiones públicas de mérito están relacionados con la información confidencial que a continuación se describe, por lo que su divulgación podría afectar la intimidad de las personas; de ahí, que sea procedente su clasificación, atento a las siguientes consideraciones:

a. Número de Folio Fiscal, CSD del Emisor, CDS del SAT, Cadena Original del Timbre, Sello Digital del Emisor, Sello Digital el SAT y Código Bidimensional del SAT (Código QR).

A fin de esclarecer la clasificación que nos ocupa, conviene traer a colación los siguientes elementos:

Rubros I.A, I.B, I.D y I.E, del "ANEXO 20 de la Resolución Miscelánea Fiscal para 2017, publicada el 23 de diciembre de 2016" el cual fue publicado en el Diario Oficial de la Federación de fecha 10 de enero de 2017 y su última modificación publicada en el Diario Oficial de la Federación el 28 de julio de 2017, que a la letra establecen:

"I. Del Comprobante fiscal digital por Internet
A. Estándar de comprobante fiscal digital por Internet.

(...)

Descripción	
Nodo requerido para precisar la información de los comprobantes relacionados.	
Atributos	
UUID	
Descripción	*Atributo opcional para registrar el folio fiscal (UUID) de un CFDI relacionado con el presente comprobante, por ejemplo: Si el CFDI relacionado es un comprobante de traslado que sirve para registrar el movimiento de la mercancía. Si este comprobante se usa como nota de crédito o nota de débito del comprobante relacionado. Si este comprobante es una devolución sobre el comprobante relacionado. Si éste sustituye a una factura cancelada.*
Uso	*requerido*
Tipo Base	*xs:string*

Longitud	*36*
Espacio en Blanco	***en*** *Colapsar*
Patrón	*[a-f0-9A-F]{8}-[a-f0-9A-F]{4}-[a-f0-9A-F]{4}-[a-f0-9A-F]{4}-[a-f0-9A-F]{12}*

(...)

B. Generación de sellos digitales para Comprobantes Fiscales Digitales por Internet.

Elementos utilizados en la generación de Sellos Digitales:

- *Cadena Original del elemento a sellar.*
- *Certificado de Sello Digital y su correspondiente clave privada.*
- *Algoritmos de criptografía de clave pública para firma electrónica avanzada.*
- *Especificaciones de conversión de la firma electrónica avanzada a Base 64.*

Para la generación de sellos digitales se utiliza criptografía de clave pública aplicada a una cadena original.

Criptografía de la Clave Pública.

La criptografía de Clave Pública se basa en la generación de una pareja de números muy grandes relacionados entre sí, de tal manera que una operación de encripción sobre un mensaje tomando como clave de encripción a uno de los dos números, produce un mensaje alterado en su significado que sólo puede ser devuelto a su estado original mediante la operación de desencripción correspondiente tomando como clave de desencripción al otro número de la pareja.

Uno de estos dos números, expresado en una estructura de datos que contiene un módulo y un exponente, se conserva secreta y se le denomina "clave privada", mientras que el otro número llamado "clave pública", en formato binario y acompañado de información de identificación del emisor, además de una calificación de validez por parte de un tercero confiable, se incorpora a un archivo denominado "certificado de firma electrónica avanzada" o "certificado para sellos digitales" en adelante Certificado.

El Certificado puede distribuirse libremente para efectos de intercambio seguro de información y para ofrecer pruebas de autoría de archivos electrónicos o confirmación de estar de acuerdo con su contenido, ambos mediante el proceso denominado "firmado electrónico avanzado", que consiste en una característica observable de un mensaje, verificable por cualquiera con acceso al certificado digital del emisor, que sirve para implementar servicios de seguridad para garantizar:

- *La integridad (facilidad para detectar si un mensaje firmado ha sido alterado),*
- *La autenticidad,*
- *Certidumbre de origen (facilidad para determinar qué persona es el autor de la firma que valida el contenido del mensaje) y*
- *No repudiación del mensaje firmado (capacidad de impedir que le autor de la firma niegue haber firmado el mensaje)*

Estos servicios de seguridad proporcionan las siguientes características a un mensaje con firma electrónica avanzada:

- *Es infalsificable.*

- *La firma electrónica avanzada no es reciclable (es única por mensaje).*
- *Un mensaje con firma electrónica avanzada alterado, es detectable.*
- *Un mensaje con firma electrónica avanzada, no puede ser repudiado.*

Los certificados de sello digital se generan de manera idéntica a los certificados de e.firma y al igual que las firmas electrónicas avanzadas el propósito del sello digital es emitir comprobantes fiscales con autenticidad, integridad, verificables y no repudiables por el emisor. Para ello basta tener acceso al mensaje original o cadena original, al sello digital y al certificado de sello digital del emisor.

Al ser el certificado de sello digital idéntico en su generación a un certificado de e.firma, proporciona los mismos servicios de seguridad y hereda las características de las firmas digitales. Por consecuencia un comprobante fiscal digital firmado digitalmente por el contribuyente tiene las características señaladas previamente.

Los algoritmos utilizados en la generación de un sello digital son los siguientes:

- *SHA-2 256, que es una función hash de un solo sentido tal que para cualquier entrada produce una salida compleja de 256 bits (32 bytes) denominada "digestión".*
- *RSAPrivateEncrypt, que utiliza la clave privada del emisor para encriptar la digestión del mensaje.*
- *RSAPublicDecrypt, que utiliza la clave pública del emisor para desencriptar la digestión del mensaje.*

A manera de referencia y para obtener información adicional, se recomienda consultar el sitio de comprobantes fiscales digitales que se encuentran dentro del portal del SAT: www.sat.gob.mx

Cadena Original

Se entiende como cadena original, a la secuencia de datos formada con la información contenida dentro del comprobante fiscal digital por Internet, establecida en el Rubro I.A. de este anexo, construida aplicando las siguientes reglas.

Reglas Generales:

1. Ninguno de los atributos que conforman al comprobante fiscal digital por Internet debe contener el carácter | (pleca) debido a que éste es utilizado como carácter de control en la formación de la cadena original.

2. El inicio de la cadena original se encuentra marcado mediante una secuencia de caracteres || (doble pleca).

3. Se expresa únicamente la información del dato sin expresar el atributo al que hace referencia. Esto es, si el valor de un campo es "A" y el nombre del campo es "Concepto", sólo se expresa |A| y nunca |Concepto A|.

4. Cada dato individual se debe separar de su dato subsiguiente, en caso de existir, mediante un carácter | (pleca sencilla).

5. Los espacios en blanco que se presenten dentro de la cadena original son tratados de la siguiente manera:

a. Se deben reemplazar todos los tabuladores, retornos de carro y saltos de línea por el carácter espacio (ASCII 32).

b. Acto seguido se elimina cualquier espacio al principio y al final de cada separador | (pleca).

c. *Finalmente, toda secuencia de caracteres en blanco se sustituye por un único carácter espacio (ASCII 32).*

6. Los datos opcionales no expresados, no aparecen en la cadena original y no tienen delimitador alguno.

7. El final de la cadena original se expresa mediante una cadena de caracteres || (doble pleca).

8. Toda la cadena original se expresa en el formato de codificación UTF-8.

9. El nodo o nodos adicionales <ComplementoConcepto> se integran a la cadena original como se indica en la secuencia de formación en su numeral 10, respetando la secuencia de formación y número de orden del ComplementoConcepto.

10. El nodo o nodos adicionales <Complemento> se integra al final de la cadena original respetando la secuencia de formación para cada complemento y número de orden del Complemento.

11. El nodo Timbre Fiscal Digital del SAT se integra posterior a la validación realizada por un proveedor autorizado por el SAT que forma parte de la Certificación Digital del SAT. Dicho nodo no se integra a la formación de la cadena original del CFDI, las reglas de conformación de la cadena original del nodo se describen en el Rubro III.B. del presente anexo.

Secuencia de Formación:

La secuencia de formación siempre se registra en el orden que se expresa en el apartado correspondiente a cada uno de los comprobantes fiscales, complementos y del timbre fiscal digital del SAT, tomando en cuenta las reglas generales expresadas en el párrafo anterior.

Generación del Sello Digital

Para toda cadena original a ser sellada digitalmente, la secuencia de algoritmos a aplicar es la siguiente:

I. Aplicar el método de digestión SHA-2 256 a la cadena original a sellar incluyendo los nodos Complementarios. Este procedimiento genera una salida de 256 bits (32 bytes) para todo mensaje. La posibilidad de encontrar dos mensajes distintos que produzcan una misma salida es de 1 en 2^{256}, y por lo tanto en esta posibilidad se basa la inalterabilidad del sello, así como su no reutilización. Es de hecho una medida de la integridad del mensaje sellado, pues toda alteración del mismo provoca una digestión totalmente diferente, por lo que no se debe reconocer como válido el mensaje.

a. *SHA-2 256 no requiere semilla alguna. El algoritmo cambia su estado de bloque en bloque de acuerdo con la entrada previa.*

II. Con la clave privada correspondiente al certificado digital del firmante del mensaje, encriptar la digestión del mensaje obtenida en el paso I utilizando para ello el algoritmo de encripción RSA.

***Nota**: La mayor parte del software comercial podría generar los pasos I y II invocando una sola función y especificando una constante simbólica. En el SAT este procedimiento se hace en pasos separados, lo cual es totalmente equivalente. Es importante resaltar que prácticamente todo el software criptográfico comercial incluye APIs o expone métodos en sus productos que permiten implementar la secuencia de algoritmos aquí descrita. La clave privada sólo debe mantenerse en memoria durante la llamada a la función de encripción; inmediatamente después de su uso debe ser eliminada de su registro de memoria mediante la sobrescritura de secuencias binarias alternadas de "unos" y "ceros".*

III. El resultado es una cadena binaria que no necesariamente consta de caracteres imprimibles, por lo que debe traducirse a una cadena que sí conste solamente de tales caracteres. Para ello se utiliza el modo de expresión de secuencias de bytes denominado "Base 64", que consiste en la asociación de cada 6 bits de la secuencia a un elemento de un "alfabeto"

que consta de 64 caracteres imprimibles. Puesto que con 6 bits se pueden expresar los números del 0 al 63, si a cada uno de estos valores se le asocia un elemento del alfabeto se garantiza que todo byte de la secuencia original puede ser mapeado a un elemento del alfabeto Base 64, y los dos bits restantes forman parte del siguiente elemento a mapear. Este mecanismo de expresión de cadenas binarias produce un incremento de 33% en el tamaño de las cadenas imprimibles respecto de la original.

(...)

D. Especificación técnica del código de barras bidimensional a incorporar en la representación impresa.

Las representaciones impresas de los dos tipos de comprobantes fiscales digitales por Internet deben incluir un código de barras bidimensional conforme al formato de QR Code (Quick Response Code), usando la capacidad de corrección de error con nivel mínimo M, descrito en el estándar ISO/IEC18004, con base en los siguientes lineamientos.

a) Debe contener los siguientes datos en la siguiente secuencia:

1. La URL del acceso al servicio que pueda mostrar los datos de la versión pública del comprobante.

2. Número de folio fiscal del comprobante (UUID).

3. RFC del emisor.

4. RFC del receptor.

5. Total del comprobante.

3. Ocho últimos caracteres del sello digital del emisor del comprobante.

Donde se manejan / caracteres conformados de la siguiente manera:

Prefijo	***Datos***	***Caracteres***
	La URL del acceso al servicio que pueda mostrar los datos del comprobante https://verificacfdi.facturaelectronica.sat.gob.mx/default.aspx	--
Id	*UUID del comprobante, precedido por el texto "&id="*	*40*
re	*RFC del Emisor, a 12/13 posiciones, precedido por el texto "&re="*	*16/21*
rr	*RFC del Receptor, a 12/13 posiciones, precedido por el texto "&rr=", para el comprobante de retenciones se usa el dato que esté registrado en el RFC del receptor o el NumRegIdTrib (son excluyentes).*	*16/84*
tt	*Total del comprobante máximo a 25 posiciones (18 para los enteros, 1 para carácter ".", 6 para los decimales), se deben omitir los ceros no significativos, precedido por el texto "&tt="*	*07/29*
fe	*Ocho últimos caracteres del sello digital del emisor del comprobante, precedido por el texto "&fe="*	*12/24*
Total de caracteres		*198*

De esta manera se generan los datos válidos para realizar una consulta de un CFDI por medio de su expresión impresa.

Ejemplo:

https://verificacfdi.facturaelectronica.sat.gob.mx/default.aspx?id=5803EB8D-81CD-4557-8719-26632D2FA434&re=XOCD720319T86&rr=CARR861127SB0&tt=0000014300.000000&fe=rH8/bw==

El código de barras bidimensional debe ser impreso en un cuadrado con lados no menores a 2.75 centímetros. Ejemplo:

2.75 cm

E. Secuencia de formación para generar la cadena original para comprobantes fiscales digitales por Internet

Secuencia de Formación:

La secuencia de formación siempre se registra en el orden que se expresa a continuación,

1. *Información del nodo Comprobante*
   a. *Version*
   b. *Serie*
   c. *Folio*
   d. *Fecha*
   e. *FormaPago*
   f. *NoCertificado*
   g. *CondicionesDePago*
   h. *Subtotal*
   i. *Descuento*
   j. *Moneda*
   k. *TipoCambio*
   l. *Total*
   m. *TipoDeComprobante*
   n. *MetodoPago*
   o. *LugarExpedicion*
   p. *Confirmacion*
2. *Información del nodo CFDIRelacionados*
   a. *TipoRelacion*
   b. *Información de cada nodo CFDIRelacionado nota: esta secuencia debe ser repetida por cada nodo*
      a. *UUID*
3. *Información del nodo Emisor*
   a. *Rfc*
   b. *Nombre*
   c. *RegimenFiscal*
4. *Información del nodo Receptor*

a. *Rfc*
b. *Nombre*
c. *ResidenciaFiscal*
d. *NumRegIdTrib*
e. *UsoCFDI*

5. *Información de cada nodo Concepto*
nota: esta secuencia debe ser repetida por cada nodo Concepto relacionado
a. *ClaveProdServ*
b. *NoIdentificacion*
c. *Cantidad*
d. *ClaveUnidad*
e. *Unidad*
f. *Descripcion*
g. *ValorUnitario*
h. *Importe*
i. *Descuento*
j. *Impuestos Traslado nota: esta secuencia debe ser repetida por cada nodo Impuesto*
    a. *Base*
    b. *Impuesto*
    c. *TipoFactor*
    d. *TasaOCuota*
    e. *Importe*

k. *Impuesto Retencion nota: esta secuencia debe ser repetida por cada nodo Impuesto*
a. *Base*
b. *Impuesto*
c. *TipoFactor*
d. *TasaOCuota*
e. *Importe*

l. *InformacionAduanera nota: esta secuencia debe ser repetida por cada nodo InformacionAduanera*
a. *NumeroPedimento*

j. *Información del nodo CuentaPredial*
a. *Numero*

k. *Información del nodo ComplementoConcepto de acuerdo con lo expresado en el Rubro III.C.*

l. *Información de cada nodo Parte*
nota: esta secuencia debe ser repetida por cada nodo Parte relacionado
a. *ClaveProdServ*
b. *NoIdentificacion*
c. *Cantidad*
d. *Unidad*
e. *Descripcion*
f. *ValorUnitario*
g. *Importe*
h. *InformacionAduanera nota: esta secuencia debe ser repetida por cada nodo InformacionAduanera*

a. *NumeroPedimento*

6. *Información de cada nodo Impuestos:Retencion*
nota: esta secuencia debe ser repetida por cada nodo Retención relacionado
a. *Impuesto*

b. Importe
7. Información del nodo Impuestos.
a. TotalImpuestosRetenidos
8. Información de cada nodo Traslado
nota: esta secuencia debe ser repetida por cada nodo Traslado relacionado.
a. Impuesto
b. TipoFactor
b. TasaOCuota
c. Importe
9. Información del nodo Impuestos.
a. TotalImpuestosTrasladados
10. El nodo o nodos adicionales <Complemento> se integran al final de la cadena original respetando la secuencia de formación para cada complemento y número de orden del Complemento.
11. El nodo Timbre Fiscal Digital del SAT se integra posterior a la validación realizada por un proveedor autorizado por el SAT que forma parte de la Certificación Digital del SAT. Dicho nodo no se integra a la formación de la cadena original del CFDI, las reglas de conformación de la cadena original del nodo se describen en el Rubro III.B. del presente anexo.
12. Información del nodo Complemento de acuerdo con lo expresado en el Rubro III.C. (...)"

De la cita que precede se puede observar que el Folio Fiscal, CSD del Emisor, CSD del SAT, Cadena Original del timbre, Sello Digital del Emisor, Sello Digital del SAT, así como el Código Bidimensional del SAT (Código QR), que se encuentran plasmados en las facturas que nos ocupan, se encuentran directamente relacionados con la integridad, autenticidad y certidumbre de origen de éstos.

Y que dichas series alfa-numéricas y/o algoritmos se encuentran conformados por diversos elementos propios del emisor y el receptor, lo que los hace identificados o identificables; de ahí, que resulta procedente la clasificación de los referidos datos como información confidencial, con fundamento en los artículos 116, último párrafo, de la Ley General de Transparencia y Acceso a la Información Pública; 113, fracción III, de la Ley Federal de Transparencia y Acceso a la Información Pública, así como los Numerales Trigésimo Octavo, fracción II y Cuadragésimo, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

En ese sentido y una vez realizado un análisis minucioso de la clasificación de información propuesta por la Dirección de Recursos Financieros, responsable de la elaboración de las versiones públicas que nos ocupan, este Comité de Transparencia considera que las partes testadas por dicha Unidad Administrativa estuvieron debidamente realizadas y apegadas a lo que establece la normatividad que regula la elaboración de las mismas, en virtud que, los datos testados constituyen información confidencial, puesto que se trata de información que fue presentada por un particular con dicho carácter y que su divulgación puede trastocar la intimidad de las personas; por lo tanto, este Comité de Transparencia estima que se cuentan con los

elementos suficientes para confirmar la clasificación de la información como el carácter de confidencial.

En razón de lo antes expuesto, este Comité de Transparencia **CONFIRMA LA CLASIFICACIÓN** como **CONFIDENCIAL** de los datos omitidos en las versiones públicas que se acompañan a las respuestas a la solicitud de información antes referida, relativos al Folio Fiscal, CSD del Emisor, CSD del SAT, Cadena Original del Timbre, Sello Digital del Emisor, Sello Digital del SAT y Código Bidimensional (Código QR), en términos de lo dispuesto en los artículos 116, último párrafo, de la Ley General de Transparencia y Acceso a la Información Pública; 113, fracción III, de la Ley Federal de Transparencia y Acceso a la Información Pública, así como los Numerales Trigésimo Octavo, fracción II y Cuadragésimo, de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

Debido a lo antes expuesto, este Comité de Transparencia emite los siguientes puntos:

RESOLUTIVOS

PRIMERO.- Se **CONFIRMA POR UNANIMIDAD** la **CLASIFICACIÓN** como **RESERVADA** de la información relativa a la evidencia de uso de los enlaces de comunicaciones que se advierten en los entregables de los contratos PRODECON-SG-DGATI-AD-004-2016 y PRODECON-SG-DGACTIC-AD-144-2016, relativos a los periodos de febrero de 2016 a diciembre de 2016, contenidos en la prueba de daño que se acompaña a la respuesta de la solicitud de información **0063200003920**; lo anterior de conformidad con lo dispuesto en los artículos 113, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública; 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, por un periodo de **cinco años**, en los términos expuestos en la presente Acta, por tratarse de información que, de proporcionarse, obstruiría la prevención de delitos.

SEGUNDO.- Se **CONFIRMA POR UNANIMIDAD** la **CLASIFICACIÓN** como **RESERVADA** de la información relativa a la evidencia de uso de los enlaces de comunicaciones que se advierten en los entregables de los contratos PRODECON-SG-DGATI-AD-004-2016 y PRODECON-SG-DGACTIC-AD-144-2016, relativos a los periodos de enero de 2017 a diciembre de 2017, contenidos en la prueba de daño que se acompaña a la respuesta de la solicitud de información **0063200004020**; lo anterior de conformidad con lo dispuesto en

los artículos 113, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública; 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, por un periodo de **cinco años**, en los términos expuestos en la presente Acta, por tratarse de información que, de proporcionarse, obstruiría la prevención de delitos.

TERCERO.- Se **CONFIRMA POR UNANIMIDAD** la **CLASIFICACIÓN** como **RESERVADA** de la información relativa a la evidencia de uso de los enlaces de comunicaciones que se advierten en los entregables de los contratos PRODECON-SG-DGATI-AD-004-2016 y PRODECON-SG-DGACTIC-AD-144-2016, relativos a los periodos de enero de 2018 a diciembre de 2018, contenidos en la prueba de daño que se acompaña a la respuesta de la solicitud de información **0063200004120**; lo anterior de conformidad con lo dispuesto en los artículos 113, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública; 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, por un periodo de **cinco años**, en los términos expuestos en la presente Acta, por tratarse de información que, de proporcionarse, obstruiría la prevención de delitos.

CUARTO.- Se **CONFIRMA POR UNANIMIDAD** la **CLASIFICACIÓN** como **RESERVADA** de la información relativa a la evidencia de uso de los enlaces de comunicaciones que se advierten en los entregables de los contratos PRODECON-SG-DGATI-AD-004-2016 y PRODECON-SG-DGACTIC-AD-144-2016, relativos a los periodos de enero de 2019 a diciembre de 2019, contenidos en la prueba de daño que se acompaña a la respuesta de la solicitud de información **0063200004220**; lo anterior de conformidad con lo dispuesto en los artículos 113, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública; 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, por un periodo de **cinco años**, en los términos expuestos en la presente Acta, por tratarse de información que, de proporcionarse, obstruiría la prevención de delitos.

QUINTO.- Se **CONFIRMA POR UNANIMIDAD** la **CLASIFICACIÓN** de **confidencialidad** de la información relativa al Folio Fiscal, CSD del Emisor,

CSD del SAT, Cadena Original del Timbre, Sello Digital del Emisor, Sello Digital del SAT y Código Bidimensional (Código QR), que se advierten en las facturas relacionadas con la solicitud de acceso a la información pública número **0063200004320**, en términos de lo dispuesto en los artículos 116, último párrafo, de la Ley General de Transparencia y Acceso a la Información Pública; 113, fracción III, de la Ley Federal de Transparencia y Acceso a la Información Pública, así como los Numerales Trigésimo Octavo, fracción II, y Cuadragésimo, de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

SEXTO.- Se **APRUEBAN LAS VERSIONES PÚBLICAS** elaboradas por la Dirección de Recursos Financieros, omitiendo la información confidencial contenida en la misma.

Así lo ordenaron y firman para constancia los miembros del Comité de Transparencia de la Procuraduría de la Defensa del Contribuyente.

No habiendo más que manifestar, siendo las 18:00 horas del día en que se actúa, los miembros del Comité de Transparencia así lo reconocen y autorizan, para hacer constancia, así como para los efectos legales a que haya lugar.

COMITÉ DE TRANSPARENCIA

C.P. Guillermo Pulido Jaramillo
Director General de Administración y Responsable del Área Coordinadora de Archivos.

Lic. Citlali Monserrat Serrano García.
Directora Consultiva y de Normatividad y Encargada de la Unidad de Transparencia.

Lic. Alfonso Quiroz Acosta.
Titular del Órgano Interno de Control en la PRODECON.

Elaboró: **Lic. Gerardo Martínez Acuña.- Secretario Técnico del Comité de Transparencia.**