7ª SESIÓN EXTRAORDINARIA DEL COMITÉ DE TRANSPARENCIA DE LA PROCURADURÍA DE LA DEFENSA DEL CONTRIBUYENTE

EN LA CIUDAD DE MÉXICO, SIENDO LAS 11:00 HORAS DEL DÍA **04 DE MAYO 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, C.P. 03100, ALCALDÍA BENITO JUÁREZ, 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, NO SE PRESENTA PERSONA ALGUNA POR PARTE 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 0063200010220.

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 0063200011320.

6.- Discusión y en su caso, confirmación, modificación o revocación de la clasificación de la información realizada por la Dirección General de Administración, relacionada con la solicitud de acceso a la información pública número 0063200012320.

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.

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:

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 **0063200010220.**

b) La Dirección de Sistemas Sustantivos, relacionada con la solicitud de acceso a la información pública con número de folio **0063200011320.**

c) La Dirección General de Administración, relacionada con la solicitud de acceso a la información pública con número de folio **0063200012320**.

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 0063200010220.

I. El día 24 de febrero de 2020, el peticionario requirió en la solicitud de información pública número **0063200010220**, lo siguiente:

> ***"Se solicita se informe mediante la PNT en formato de datos abiertos tipo CSV o XLSX 1. La base de usuarios que hayan utilizado el sistema SICSS (Incluir usuarios vigentes y NO vigentes u obsoletos) 1.1 Para los usuarios que ya NO están vigentes ¿Cual es el procedimiento que se realiza para la depuración de usuarios obsoletos? y ¿Cual es el procedimiento de seguridad de la información que se realiza para garantizar que ya no pueden ingresar al sistema SICSS? Proporcionar evidencia en PDF para ambos procedimientos. 1.2 Para los usuarios que ya NO están vigentes también proporcionar evidencia en PDF de la baja de los usuarios obsoletos. ¿Cuando un usuario de PRODECON es dado de baja de la Institución se realiza algun procedimeinto de borrado seguro en los equipos de cómputo personal? En caso afirmativo proporcionar en un archivo de datos abiertos tipo CSV o XLSX con la relación de los usuarios dados de baja y en PDF la evidencia de los certificados de borrado seguro generados desde febrero del 2016 hasta enero del 2020. En caso negativo ¿cual es el fundamento técnico administrativo por el que no se realiza borrado seguro?"***
>
> *[sic]*

II. De conformidad con lo dispuesto en los artículos 45, fracciones II, IV y XII, 121, 129, 131, 132 y 133, de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 3, 133, 134, 136 y 137 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/128/2020**, de fecha 25 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. Mediante oficio **PRODECON/SG/DGA/DSS/029BIS/2020**, de fecha 10 de marzo de 2020, recibido por la Unidad de Transparencia el 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:

> *"[...] Por lo que hace a la solicitud de **"...incluir usuarios NO vigentes u obsoletos"**, se advierte que puede ser un dato personal, puesto que ya no*

son servidores públicos adscritos a esta Prodecon, se hace de su conocimiento que no se puede proporcionar lo solicitado, toda vez que corresponde información clasificada como confidencial, lo anterior con fundamento en lo dispuesto en los artículos 116, primero párrafo de la Ley General de Transparencia y Acceso a la Información Pública; 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; en relación con los numerales Trigésimo Octavo, fracción I, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas; de ahí que, se solicita a la Unidad de Transparencia que por su conducto sea sometida al Comité de Transparencia.

[...]

***Respuesta:** Se reitera que no se realiza alguna baja de los usuarios obsoletos conforme lo descrito en el numeral anterior. Por lo que hace al procedimiento de borrado seguro de la información del equipo, se informa que **sí se lleva a cabo el procedimiento de borrado seguro en los equipos de cómputo personal**, sin embargo, proporcionar la relación de usuarios dados de baja en un archivo CSV o XLSX no es factible, ya que se advierte que puede ser un dato personal, puesto que ya no son servidores públicos adscritos a esta Prodecon, se hace de su conocimiento que no se puede proporcionar lo solicitado, toda vez que corresponde a información clasificada como confidencial, lo anterior con fundamento en lo dispuesto en los artículos 116, primero párrafo de la Ley General de Transparencia y Acceso a la Información Pública; 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; en relación con los numerales Trigésimo Octavo, fracción I, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas; de ahí que, se solicita a la Unidad de Transparencia que por su conducto sea sometida al Comité de Transparencia.*

*Por otra parte, el proporcionar en PDF la **evidencia de los certificados o informes de borrado seguro generados desde febrero del 2016 hasta enero del 2020**, se hace de su conocimiento que dicho documento contiene nombres de ex servidores públicos que ya no están adscritos a esta Prodecon, por lo que puede ser un dato personal, es por ello que se advierte que corresponde a información clasificada como confidencial, lo anterior con fundamento en lo dispuesto en los artículos 116, primero párrafo de la Ley General de Transparencia y Acceso a la Información Pública; 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; en relación con los numerales Trigésimo Octavo, fracción I, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas; de ahí que, se solicita a la Unidad de Transparencia que por su conducto sea sometida al Comité de Transparencia.*

Por lo que hace al resto de la información contenida en los certificados o informes de borrado seguro, se advierte que representa un riesgo real, ya que cada certificado contiene todos los detalles referentes al hardware del equipo de cómputo, como son: Número de serie de los equipos de cómputo y sus componentes, Adaptadores de red, controladores, características del BIOS, UUID (Universally Unique Identifier), Direcciones

IP, MAC ADDRESS, entre otros, con lo que se potencia la vulnerabilidad de permitir a los hackers realizar ataques a la infraestructura de la Prodecon, poniendo en riesgo la información de los servidores y de los equipos de cómputo.

De tal suerte que, proporcionar la información solicitada a una persona con los medios técnicos, conocimientos y herramientas adecuadas, permitiría el acceso ilícito a un atacante a los equipos de cómputo o Servidores de esta Procuraduría a través de la red y por lo tanto a los sistemas sustantivos y administrativos, pudiendo realizar un atentado en cualquier momento y de manera inadvertida, extrayendo información que las áreas generan y utilizan para el desarrollo de sus actividades o incluso la que los contribuyentes presentan para su atención, lo que traería diversas consecuencias, dependiente del tipo de datos que obtengan. Por lo anterior, se advierte que se cuenta con información reservada, toda vez que:

Al permitir que se conozcan todos los detalles referentes al hardware del equipo de cómputo de esta PRODECON, representa un alto riesgo de ataque a la infraestructura tecnológica, por lo que se estaría vulnerando la operación de la Prodecon, así como afectando el ejercicio de los derechos de los contribuyentes a hacer uso de los servicios que brinda Prodecon.

En caso de proporcionar dicha información, se pone en riesgo 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 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 a los certificados de borrado seguro, tal y como se señala en el oficio PRODECON/SG/DGA/DSS/029BIS/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:

PRUEBA DE DAÑO

Equipo de cómputo: *es una máquina digital que ejecuta comandos para convertirlos en datos convenientes y útiles que posteriormente se envían a las unidades de salida. Está formado físicamente por numerosos circuitos*

integrados y muchos componentes de apoyo, extensión y accesorios, que en conjunto pueden ejecutar tareas diversas con suma rapidez y bajo el control de un programa (software).

Servidor: *es un equipo informático que forma parte de una red y provee servicios (archivos, correo, base de datos, Web) a otros equipos de cómputo (clientes).*

Número de serie: *identificador de un equipo de cómputo o servidor para la marca que lo fabrica.*

Adaptador de red: *Un adaptador de red, también llamado tarjeta de red, es el interfaz electrónico entre su ordenador (host) y el cable que lo conecta a la red. Su función es que administra el tráfico de información a través de la red para asegurar que la información llegue a su destino.*

Controladores o Drivers de un equipo de cómputo: *Es un software que conecta el sistema operativo directamente con los componentes del hardware de la PC.*

BIOS: *El BIOS (sigla en inglés de basic input/output system; en español "sistema básico de entrada y salida") es un software que localiza y reconoce todos los dispositivos necesarios para cargar el sistema operativo en la memoria RAM.*

UUID (Universal/y Unique Identifier): *Un UUID puede ser usado con un identificador específico "intencionalmente" y ser usado en varias ocasiones para identificar el mismo objeto en diferentes contextos.*

Dirección IP: *(Internet Protocol), la dirección IP es un conjunto de números que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, laptop, teléfono inteligente, Switch, entre otros) que utilice el protocolo o (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP. La dirección IP no debe confundirse con la dirección MAC ADDRESS, que es un identificador de 48 bits expresado en código hexadecimal, para identificar de forma única la tarjeta de red y no depende del protocolo de conexión utilizado en la red.*

MAC ADDRESS: *(media access control address) de un dispositivo, es un identificador único que se les asigna a las interfaces de redes. Las tarjetas de red inalámbrica o las de red Ethernet, los routers, las impresoras, etc., todos tienen un identificador propio de 48 bits que no se repite en todo el mundo, es como su propia huella digital para poder comunicarse.*

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 prevención o 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 información contenida en los certificados o informes de borrado seguro, se advierte que representa un riesgo real, ya que cada certificado contiene todos los detalles referentes al hardware del equipo de cómputo personal o de un servidor (físico o virual), como son: Números de series de equipos de cómputo y sus componentes, Adaptadores de red, controladores, características del BIOS, UUID (Universally Unique Identifier), Direcciones IP, MAC ADDRESS, entre otros, lo que 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 los equipos de cómputo o servidores, referente a los Números de serie, Adaptadores de red, controladores, características del BIOS, UUID (Universally Unique Identifier), Direcciones IP, MAC ADDRESS, 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 o Equipo de cómputo/ Servidor, si conoce de los elementos básicos que la conforman, aunado a que haya otra(s) solicitud(es) referente(s) a otros componentes, como son; Segmentos de red, intervalos de uso de la red, enlaces d comunicación, entre otros, lo que potenciaría el riesgo de vulnerar y focalizar lo ataques.

Al otorgar la información de todo hardware del equipo de cómputo o servidor, incluido en el Certificado o Informe de Borrado Seguro, aunado a que existen herramientas de rastreo de IP que pueden otorgar información a una persona que quiera sacar datos d una dirección en concreto, por lo que se puede generar; la suplantación de identidad del equipo para acceder a la red y a toda la infraestructura tecnológica y de comunicaciones, lo cual permitiría extraer información sensible de la conducción de expedientes de los contribuyentes o procedimientos administrativos, afectando severamente las funciones sustantivas y la propia operación e la Procuraduría, al exponer su capacidad de reacción ante posibles ataques informáticos, en razón de identificar o bien remitir diversa información contenida en los equipos, servidores, equipos de comunicaciones que atentan contra la seguridad y conectividad tecnológica que se tienen implementados. Posibilitando en su conjunto, a cualquier persona calificada el ingreso a los sistemas de comunicación y a la información que por ellos se transporta.

Asimismo, permitiría que la persona mal intencionada pueda buscar en la red cualquier vulnerabilidad para realizar afectaciones mayores, por otra parte, puede extraer información, 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 la información de todo hardware del equipo de cómputo o servidor, incluido en el Certificado o Informe de Borrado Seguro, 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 la información del Certificado o Informe de Borrado Seguro, que contiene la información de todo hardware del equipo de cómputo o servidor, como son; Números de serie de los equipos de cómputo y sus componentes, Adaptadores de red, controladores, características del BIOS, UUID (Universally Unique Identifier). Direcciones IP, MAC ADDRESS, 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 contiene información susceptible de ser clasificada como reservada de los contribuyentes, entre otros, esta Unidad Administrativa 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 clasificación de la información propuesta por la Unidad Administrativa, se puede observar que clasificó como información **confidencial** lo siguiente:

- Los **nombres** de los **usuarios no vigentes u obsoletos** que utilizaron el sistema SICSS, lo anterior en términos de lo previsto en los artículos 116, primer párrafo de la Ley General de Transparencia y Acceso a la Información Pública; 113 fracciones I, de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con los numerales Trigésimo Octavo, fracciones I, de los Lineamientos Generales para la Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas.

- La relación de **usuarios dados de baja** que se advierte del procedimiento de borrado seguro, lo anterior con fundamento en lo dispuesto en los artículos 116, primero párrafo de la Ley General de Transparencia y Acceso a la Información Pública; 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; en relación con los numerales Trigésimo Octavo, fracción I, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas.

- Los **nombres de los ex servidores públicos** que se advierten en los informes de borrado de datos (certificados de borrado seguro) generados desde febrero del 2016 hasta enero del 2020, lo anterior con fundamento en lo dispuesto en los artículos 116, primero párrafo de la Ley General de Transparencia y Acceso a la Información Pública; 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; en relación con los numerales Trigésimo Octavo, fracción I, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas.

Asimismo, del análisis a la clasificación de la información propuesta por la Unidad Administrativa, se puede observar que clasificó como información **reservada** lo siguiente:

- Los **informes de borrado de datos** (certificados de borrado seguro), toda vez que cada certificado contiene todos los detalles referentes al hardware del equipo de cómputo, como son: Número de serie de los equipos de cómputo y sus componentes, Adaptadores de red, controladores, características del BIOS, UUID (Universally Unique Identifier), Direcciones IP, MAC ADDRESS, entre otros; lo anterior 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.

  Y al respecto, expresó esencialmente los siguientes motivos:

  Que, de proporcionar los informes de borrado de datos (certificados de borrado seguro), se tiene la expectativa razonable de que ocurran ataques a la infraestructura de la Procuraduría, poniendo en riesgo la información de los servidores y de los equipos de cómputo.

  Asimismo que, la información contenida en los informes de borrado de datos (certificados de borrado seguro), si es obtenida por una persona con los medios técnicos, conocimientos y herramientas adecuadas, permitiría el acceso ilícito a un atacante a los equipos de cómputo o servidores de la Procuraduría a través de la red y por lo tanto a los sistemas sustantivos y administrativos, pudiendo realizar un atentado en cualquier momento y de manera inadvertida, extrayendo información que las áreas generan y utilizan para el desarrollo de sus actividades o incluso la que los contribuyentes presentan para su atención, lo que traería diversas consecuencias dependiendo del tipo de datos que obtengan, vulnerando con ello la operación de la Procuraduría y el ejercicio de los derechos de los contribuyentes a hacer uso de los servicios que brinda la Entidad.

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

a) Clasificación como información confidencial de los nombres de los usuarios no vigentes u obsoletos que utilizaron el sistema SICSS, la relación de usuarios dados de baja que se advierte del procedimiento de borrado seguro y los nombres de los ex servidores públicos que se advierten en los informes de borrado de datos (certificados de borrado seguro) generados desde febrero del 2016 hasta enero del 2020.

Si bien es cierto que, en un principio la información relativa a los servidores públicos tiene el carácter de pública pues su conocimiento favorece la rendición de cuentas, también cierto lo es que, cuando dejan de prestar sus servicios en la dependencia o entidad del sector público en la que se encontraban adscritos y se da por concluida su relación laboral, pierden ese carácter y por ende, su nombre como persona física, es susceptible de clasificarse como confidencial al encontrarse relacionado intrínsecamente con su persona e intimidad, máxime que ya no implica el ejercicio de recursos públicos.

En esa tesitura, toda vez que la información relativa a los nombres de los ex servidores públicos está relacionada con información concerniente a personas identificadas o identificables, por lo que su divulgación puede afectar la intimidad de las personas; se estima procedente su clasificación como confidencial, atento a las siguientes consideraciones:

> **Nombre de persona física (ex servidores públicos).** De conformidad con lo dispuesto en los artículos 116, primer párrafo, de la Ley General de Transparencia y Acceso a la Información Pública y 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública, se considera información confidencial la que contiene datos personales concernientes a una persona identificada o identificable.
>
> En ese sentido, al ser el nombre un atributo de la personalidad, y la manifestación principal del derecho a la identidad, toda vez que por sí mismo permite la identificación plena de una persona física.
>
> Por tanto, el nombre de una persona física debe considerarse como información confidencial por tratarse de un dato personal, con fundamento en lo dispuesto en los artículos 116, primer párrafo, de la Ley General de Transparencia y Acceso a la Información Pública; 113, fracción I, de la Ley Federal de

Transparencia y Acceso a la Información Pública; 3, fracción IX, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; y el numeral Trigésimo Octavo, fracción I, de los Lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

En ese orden de ideas y una vez realizado un análisis minucioso de la clasificación de información, este Comité de Transparencia considera que los **nombres de los usuarios no vigentes u obsoletos que utilizaron el sistema SICSS, la relación de usuarios dados de baja que se advierte del procedimiento de borrado seguro y los nombres de los ex servidores públicos que se advierten en los informes de borrado de datos (certificados de borrado seguro) generados desde febrero del 2016 hasta enero del 2020**, constituyen datos personales concernientes a una persona identificada o identificable, respectivamente; por lo tanto, este Órgano Colegiado estima que se cuentan con los elementos suficientes para confirmar la clasificación de la información con el carácter de confidencial.

En razón de lo antes expuesto, este Comité de Transparencia **CONFIRMA LA CLASIFICACIÓN** como **CONFIDENCIAL** de los datos personales relacionados con la solicitud de acceso a la información pública con número de folio **0063200010220**, relativos a: **los nombres de los usuarios no vigentes u obsoletos que utilizaron el sistema SICSS, la relación de usuarios dados de baja que se advierte del procedimiento de borrado seguro y los nombres de los ex servidores públicos que se advierten en los informes de borrado de datos (certificados de borrado seguro) generados desde febrero del 2016 hasta enero del 2020;** en términos de lo dispuesto en los artículos 116, primer párrafo, de la Ley General de Transparencia y Acceso a la Información Pública; 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; 3, fracción IX, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y el numeral Trigésimo Octavo, fracción I, de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas.

b) Clasificación como información reservada de los informes de borrado de datos (certificados de borrado seguro).

Atendiendo a la motivación que hizo valer la Dirección de Sistemas Sustantivos, la cual se encuentra encaminada a demostrar que de proporcionar la información solicitada se tiene la expectativa razonable de que ocurran ataques a la infraestructura de la Procuraduría, poniendo en riesgo la información de los servidores y de

los equipos de cómputo, ya que cada informe contiene todos los detalles referentes al hardware del equipo de cómputo, como son: **Número de serie de los equipos de cómputo y sus componentes, Adaptadores de red, controladores, características del BIOS, UUID (Universally Unique Identifier), Direcciones IP, MAC ADDRESS, entre otros.**

Maxime que, la información contenida en los certificados o informes de borrado seguro, si es obtenida por una persona con los medios técnicos, conocimientos y herramientas adecuadas, permitiría el acceso ilícito a un atacante a los equipos de cómputo o servidores de esta Procuraduría a través de la red y por lo tanto a los sistemas sustantivos y administrativos, pudiendo realizar un atentado en cualquier momento y de manera inadvertida, extrayendo información que las áreas generan y utilizan para el desarrollo de sus actividades o incluso la que los contribuyentes presentan para su atención, lo que traería diversas consecuencias dependiendo de la información que se extraiga.

Lo anterior, aunado a que ha habido otras solicitudes de información en donde se ha requerido información referente a otros componentes de los equipos, como son: segmentos de red, intervalos de uso, enlaces de comunicación, entre otros, que en conjunto potenciarían el riesgo de focalizar los ataques.

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, en efecto, la información relativa a los **informes de borrado de datos** (certificados de borrado seguro) 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 que ocurran ataques a la infraestructura de la Procuraduría, poniendo en riesgo la información de los servidores y de los equipos de cómputo, ya que cada certificado contiene todos los detalles referentes al hardware del equipo de cómputo, supuestos que 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 **informes de borrado de datos** (certificados de borrado seguro), se ocasionaría:

1. 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 el **acceso ilícito a sistemas y equipos de informática**, que sin duda afectarían severamente el ejercicio de sus labores cotidianas y sustantivas.

2. 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 legal 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 la información requerida 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.

3. 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 relativa a los **informes de borrado de datos** (certificados de borrado seguro) **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.

Asimismo, no sobra exaltar que, lo anteriormente argumentado se robustece con lo resuelto por este mismo Comité de Transparencia en sus sesiones 9ª. Extraordinaria de fecha 18 de septiembre de 2018 y 3ª. Sesión Extraordinaria celebrada el 28 de febrero de 2020 (en donde se reservó el número de serie de los equipos de cómputo); 9ª. Sesión Extraordinaria de fecha 18 de septiembre de 2018 (en donde se reservaron las características del BIOS); 16ª. Sesión Extraordinaria del 29 de octubre de 2018 (en donde se reservó la dirección IP), y en la 4ª. Sesión Ordinaria celebrada el 05 de octubre de 2018 (en donde se reservó la Mac Address).

En razón de lo antes expuesto, este Comité de Transparencia **CONFIRMA LA CLASIFICACIÓN** como **RESERVADA** de la información relativa a los **informes de borrado de datos** (certificados de borrado seguro), contenida en la prueba de daño que se acompaña a la respuesta de la solicitud de información **0063200010220**; 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.

VII. Ahora bien, en cuanto al periodo de reserva de la información relativa a los **informes de borrado de datos** (certificados de borrado seguro), 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.

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 0063200011320.

I. El día 24 de febrero de 2020, el peticionario requirió en la solicitud de información pública número **0063200011320**, lo siguiente:

> ***"Se solicita se informe detalladamente mediante la PNT. Para cada liberación en producción del Sistema para control y seguimiento de folios de gobierno de la Procuraduría (SICSS) se requiere conocer a) La matriz de escenarios de prueba realizada en cada liberación para asegurar que el sistema cumplió con las especificaciones de las áreas usuarias en formato de datos abiertos tipo CSV p XLSX. b) Evidencia en PDF del la pruebas unitarias y funcionales exitosas en cada liberación a producción. c) Evidencia PDF de las pruebas estáticas y dinámicas de estrés realizadas en cada liberación para asegurar que el sistema tiene un buen desempeño con alta demanda transaccional. d) Listado de los requisitos de calidad que deben cumplir los sistemas de la Procuraduría antes de ser liberados en producción y evidencia PDF de los certificados de liberación."***
>
> [sic]

II. De conformidad con lo dispuesto en los artículos 45, fracciones II, IV y XII, 121, 129, 131, 132 y 133, de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 3, 133, 134, 136 y 137 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/139/2020**, de fecha 25 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. Mediante oficio **PRODECON/SG/DGA/DSS/039/2020**, de fecha 11 de marzo de 2020, recibido por la Unidad de Transparencia el día de cuenta, 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 al **Documento de Control de Cambios,** se advierte que cuenta parcialmente con información reservada toda vez que:*
>
> ***Servidor:** es un equipo informático que forma parte de una red y provee servicios (archivos, correo, base de datos, Web) a otros equipos de cómputo (clientes).*
>
> ***Nombre de Servidor o de equipo informático:** Un nombre de servidor o de equipo es un nombre único que se le da a un dispositivo conectado a una red informática. Puede ser una computadora, un servidor de archivos, un dispositivo de almacenamiento por red, impresora, etc. En Internet, se trabaja con equipos funcionando como servidores (hosts), en estos casos el equivalente para "nombre de equipo" en ingles seria "hostname". Estos servidores siempre tienen una dirección IP asignada.*
>
> ***Dirección IP:** (Internet Protocol), la dirección I Pes un conjunto de números que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, laptop, teléfono inteligente, Switch, entre otros) que utilice el protocolo o (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP. La dirección IP no debe confundirse con la dirección MAC ADDRESS, que es un identificador de 48 bits expresado en (Código hexadecimal, para identificar de forma única la tarjeta de red y no depende del protocolo de conexión utilizado en la red.*
>
> ***Instancia de Base de datos:** es el conjunto de procesos que se ejecutan en el servidor, así como la memoria reservada asociados a una Base de datos. Una instancia de manera formal es la aplicación de un esquema a un conjunto finito de datos. En palabras no tan técnicas, se puede definir como el contenido de una tabla en un momento dado, pero también es válido referirnos a una instancia cuando trabajamos o mostramos únicamente un subconjunto de la información contenida en una relación o tabla.*
>
> ***Carpeta de Archivos o Directorio de archivos:** es un contenedor virtual en el que se almacenan una agrupación de archivos informáticos y otros subdirectorios, atendiendo a su contenido, a su propósito o a cualquier*

criterio que decida el usuario. Técnicamente, el directorio almacena información acerca de los archivos que contiene: como los atributos de los archivos o dónde se encuentran físicamente en el dispositivo de almacenamiento.

Por lo anterior, el difundir la información de los Nombres de Servidores, Dirección IP y ubicación de carpeta de archivos, Instancia de Base de datos 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 o equipo de cómputo, si conoce de los elementos básicos que la conforman, aunado a que haya otra(s) solicitud(es) referente(s) a otros componentes, como son; Dirección MAC, Segmentos de red, número de serie, intervalos de uso de la red, enlaces de comunicación entre otros, lo que potenciaría el riesgo de vulnerar y focalizar los ataques.

Al otorgar los Nombres de Servidores, Dirección IP, Instancia de Base de datos y ubicación de carpeta de archivos, incluidos en el Documento de Control de Cambios, aunado a que existen herramientas de rastreo de IP que pueden otorgar información a una persona que quiera sacar datos de una dirección en concreto, por lo que se puede generar; Amenazas de suplantación de identidad (spoofing), Amenazas Servidor-Servidor durante las actualizaciones dinámicas de software, en el flujo de información entre un cliente y un servidor master o caché, la Instancia de Base de datos puede facilitar una Inyección SQL, (por sus siglas en inglés Structured Query Language; en español, lenguaje de consulta estructurada, utilizado en programación, diseñado para administrar, y recuperar información de sistemas de gestión de bases de datos) que es un método de infiltración de código intruso que se vale de alguna vulnerabilidad informática para realizar operaciones sobre una base de datos, 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, al poner en riesgo la información que alojan los servidores y los equipos de cómputo. [...]."

[Sic]

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

"[...]Sobre el particular, de conformidad con lo dispuesto en los artículos 44, fracción 11, 100, 104, 108 y 114, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción 11, 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, en cuanto hace al Nombres de Servidores, Dirección IP, Instancia de Base de datos y ubicación de carpeta de archivos, tal y como se señala en el oficio PRODECON/SG/DGA/DSS/039/2020, 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:

Servidor: *es un equipo informático que forma parte de una red y provee servicios (archivos, correo, base de datos, Web) a otros equipos de cómputo (clientes).*

Nombre de Servidor o de equipo informático: *Un nombre de servidor o de equipo es un nombre único que se le da a un dispositivo conectado a una red informática. Puede ser un ordenador, un servidor de ficheros, un dispositivo de almacenamiento por red, impresora, etc. En Internet, se trabaja con equipos funcionando como servidores (hosts), en estos casos el equivalente para "nombre de equipo" en inglés seria "hostname". Estos servidores siempre tienen una dirección I P asignada.*

Dirección IP: *(Internet Protocol), la dirección IP es un conjunto de números que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, laptop, teléfono inteligente, Switch, entre otros) que utilice el protocolo o (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP. La dirección IP no debe confundirse con la dirección MAC ADDRESS, que es un identificador de 48 bits expresado en código hexadecimal, para identificar de forma única la tarjeta de red y no depende del protocolo de conexión utilizado en la red.*

Instancia de Base de datos: *es el conjunto de procesos que se ejecutan en el servidor, así como la memoria reservada asociados a una Base de datos. Una instancia de manera formal es la aplicación de un esquema a un conjunto finito de datos. En palabras no tan técnicas, se puede definir como el contenido de una tabla en un momento dado, pero también es válido referirnos a una instancia cuando trabajamos o mostramos únicamente un subconjunto de la información contenida en una relación o tabla.*

Carpeta de Archivos o Directorio de archivos: *es un contenedor virtual en el que se almacenan una agrupación de archivos informáticos y otros subdirectorios, atendiendo a su contenido, a su propósito o a cualquier criterio que decida el usuario. Técnicamente, el directorio almacena información acerca de los archivos que contiene: como los atributos de los archivos o dónde se encuentran físicamente en el dispositivo de almacenamiento.*

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 prevención o 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 información referente al Nombre del Servidor, Dirección IP, Instancia de Base de datos y ubicación de carpeta de archivos, 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 los Nombres de Servidores, Dirección IP, Instancia de Base de datos, y ubicación de carpeta de archivos, 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 o equipo de cómputo, si conoce de los elementos básicos que la conforman, aunado a que haya otra(s) solicitud(es) referente(s) a otros componentes, como son; Dirección MAC, Segmentos de red, número de serie, intervalos de uso de la red, enlaces de comunicación entre otros, lo que potenciaría el riesgo de vulnerar y focalizar los ataques.

Al otorgar los Nombres de Servidores, Dirección IP, Instancia de Base de datos y ubicación de carpeta de archivos, incluidos en el Documento de Control de Cambios, aunado a que existen herramientas de rastreo de IP que pueden otorgar información a una persona que quiera sacar datos de una dirección en concreto, por lo que se puede generar; Amenazas de suplantación de identidad (spoofing), Amenazas Servidor-Servidor durante las actualizaciones dinámicas de software, en el flujo de información entre un cliente y un servidor master o caché, la Instancia de Base de datos puede facilitar una Inyección SQL, (por sus siglas en inglés Structured Query Language; en español, lenguaje de consulta estructurada, utilizado en programación, diseñado para administrar, y recuperar información de sistemas de gestión de bases de datos) que es un método de infiltración de código intruso que se vale de alguna vulnerabilidad informática para realizar operaciones sobre una base de datos, 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, al poner en riesgo la información que alojan los servidores y los equipos de cómputo.

II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda. *Al permitir que se identifique los Nombres de Servidores, Dirección IP, Instancia de Base de datos y ubicación de carpeta de archivos, 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 parcialmente la información del "Documento de Control de Cambios", que contenga datos de los Nombres de Servidores, Dirección IP, Instancia de Base de datos y ubicación de carpeta de archivos, 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 contiene información susceptible de ser clasificada como reservada de los contribuyentes, entre otros, esta Unidad Administrativa 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 parcialmente la información contenida en la documentación de control de cambios, específicamente la relativa a los nombres de servidores, dirección IP, instancia de base de datos y ubicación de carpeta de archivos; lo anterior, 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, al otorgar los nombres de servidores, dirección IP, instancia de base de datos y ubicación de carpeta de archivos, representa un riesgo real para la integridad y seguridad de la información, en tanto que facilitan la identificación de elementos que cuyas funciones están encaminadas a su reservación; siendo que, para un hacker es más fácil penetrar en una red o equipo de cómputo, so conoce los elementos básicos que la conforman, aunado a que, a través de otras solicitudes de información, se ha solicitado información de otros componentes, lo que potencializa el riesgo de vulnerar y focalizar ataques cibernéticos.

Lo anterior, aunado a que existen herramientas de rastreo de IP que pueden otorgar información a una persona que quiera sacar datos de una dirección en concreto, lo que puede generar amenazas de suplantación de identidad (spoofing), así como amenazas denominadas servidor-servidor, durante las actualizaciones dinámicas de software, en el flujo de información entre un cliente y un servidor master o caché.

Asimismo, la instancia de base de datos puede facilitar una Inyección SQL, lenguaje de consulta estructurada, utilizado en programación, diseñado para recuperar información de sistemas de gestión de bases de datos, el cual es un método de infiltración de código intruso que se vale de alguna vulnerabilidad informática para realizar operaciones sobre una base de datos, 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 Procuraduría, al poner en riesgo la información que alojan los servidores y los equipos de cómputo.

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

Atendiendo a la motivación que hizo valer la Dirección de Sistemas Sustantivos, en lo que respecta a los nombres de servidores, dirección IP, instancia de base de datos y ubicación de carpeta de archivos contenidos en la **documentación de control de cambios**, la cual se

encuentra encaminada a demostrar que de proporcionar los datos descritos 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, puesto que para un hacker es más fácil penetrar en una red o equipo de cómputo, si conoce de los elementos básicos que la conforman.

Aunado a que existen herramientas de rastreo de IP que pueden otorgar información, a una persona que quiera sacar datos de una dirección en concreto, se pueden generar diversas amenazas, como son la suplantación de identidad (spoofing), así como amenazas denominadas servidor-servidor, durante las actualizaciones dinámicas de software, en el flujo de información entre un cliente y un servidor master o caché.

Y que, la instancia de base de datos puede facilitar una Inyección SQL, que es un método de infiltración de código intruso que se vale de alguna vulnerabilidad informática para realizar operaciones sobre una base de datos, 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.

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, en efecto, la información relativa a los nombres de servidores, dirección IP, instancia de base de datos y ubicación de carpeta de archivos actualiza la causal de **reserva parcial** de la **documentación de control de cambios**, 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 que una persona que quiera sacar datos de una dirección en concreto, puede generar amenazas de suplantación de identidad (spoofing) y amenazas servidor-servidor durante las actualizaciones dinámicas de software, en el flujo de información entre un cliente y un servidor master o caché, supuestos que 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 nombres de servidores, dirección IP, instancia de base de datos y ubicación de carpeta de

archivos contenidos en la **documentación de control de cambios**, de esta Procuraduría se ocasionaría:

1. 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 el **acceso ilícito a sistemas y equipos de informática**, que sin duda afectarían severamente el ejercicio de sus labores cotidianas y sustantivas.

2. 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 legal 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.

3. 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 relativa a los nombres de servidores, dirección IP, instancia de base de datos y ubicación de carpeta de archivos contenidos en la documentación de control de cambios, **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 tesitura, 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.

En razón de lo antes expuesto, este Comité de Transparencia **CONFIRMA LA CLASIFICACIÓN** como **RESERVA PARCIAL** de la información contenida en la **documentación de control de cambios**, relativa a los **Nombres de Servidores, Instancia de Base de datos y ubicación de carpeta de archivos**, contenida en la prueba de daño que se acompaña a la respuesta de la solicitud de información **0063200011320**; 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.

Sin que sea óbice precisar, que la información concerniente a la **Dirección IP,** ya fue materia de **reserva** por parte de este Comité de Transparencia, en su 16ª. Sesión Extraordinaria de 2018 celebrada el 29 de octubre de 2018, en donde se reservó por un periodo de **cinco años**.

Asimismo, no se omite indicar que, de la revisión a la documentación de control de cambios que nos ocupa, se advirtió que consta de un peso electrónico aproximado de 52.9 MB, por lo que **se instruye** a la Unidad de Transparencia para que notifique al solicitante los costos por la reproducción de la información requerida, toda vez que sobrepasa la capacidad permitida por la Plataforma Nacional de Transparencia, así como todas las modalidades de acceso; asimismo, **se instruye** a la Dirección de Servicios Sustantivos, a que elaboren las versiones públicas de la documentación materia de la presente solicitud, una vez cubierto el pago de derechos que al respecto haya realizado el requirente, para su posterior entrega por parte de la Unidad de Transparencia.

VII. Ahora bien, en cuanto al periodo de reserva de la información relativa los nombres de servidores, instancia de base de datos y ubicación de carpeta de archivos contenidos en la **documentación de control de cambios**, 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.

6.- Discusión y en su caso, confirmación, modificación o revocación de la clasificación de la información realizada por la Dirección General de Administración, relacionada con la solicitud de acceso a la información pública número 0063200012320.

I. El día 24 de febrero de 2020, el peticionario requirió en la solicitud de información pública número **0063200012320**, lo siguiente:

> ***"Para el contrato de Outsourcing PRODECON-SG-DRH-LP-004-2019 realizado entre la Procuraduría de la Defensa del Contribuyente y la persona moral denominada Gestión del Agua y Medio Ambiente, Sociedad Civil, la cual durante el 2019 otorgó el SERVICIO ESPECIALIZADO de administración de personal de apoyo a la PRODECON para sus áreas sustantivas, con un monto máximo total de 18,000,000.00 pesos, se solicita informe detalladamente mediante la PNT. 1. ¿Cuales fueron las funciones específicas del personal de apoyo en las áreas sustantivas? 2.***

¿Por qué si la PRODECON tiene plazas de estructura y plazas eventuales aprobadas por la SHCP, necesita más personal de apoyo para realizar su mandato (facultades establecidas en el Art. 5 de la Ley Orgánica) y dar servicio a los contribuyentes? 2.1 ¿Cuales son la facultades que no pueden realizar y por que requieren personal especializado de apoyo? 2.1 ¿Cuál fue el estudio realizado por PRODECON para determinar que necesita personal especializado de apoyo? 2.2 ¿Cuál fue el estudio realizado por PRODECON para determinar el número de recursos (personal especializado de apoyo) y determinar el costo máximo total de 18,000,000.00 de pesos? Proporcionar evidencia en PDF y en caso de no contar con ella, explicar ¿Por qué? 2.3 ¿Cuál fue la metodología utilizada por PRODECON para definir cada uno de los perfiles de este contrato y aclarar a que se refiere los acrónimos NAE1, NAE2, NAE3 y NAE4? Proporcionar evidencia en PDF y en caso de no contar con ella, explicar ¿Por qué? 2.4 ¿Cuál fue el estudio realizado por PRODECON para estimar los sueldos relativos a cada perfil? Proporcionar evidencia en PDF y en caso de no contar con ella, explicar ¿Por qué? 3. Según la exposición del Titular en Funciones el Lic. Luis Placencia durante el Simposio Reforma Fiscal 2020 efectuado el 19 de Febrero del 2020 en el TFJA, la Subcontratación Laboral se justifica por su carácter especializado. Entonces ¿Cuál es la especialización del personal de apoyo contratado con el contrato PRODECON-SG-DRH-LP-004-2019 y qué valor agregado añade que no tenga el personal de estructura y el personal eventual de PRODECON? 3.1 ¿Cuales fueron las funciones aprovechadas por el contratante? 3.2 ¿Cual es la evidencia que garantiza la ejecución de actividades del personal de apoyo contratado? 3.3 ¿Como demuestran que los servicios del personal de apoyo contratado se realizaron correctamente? 4.. ¿Por que no deben considerarse los pagos de este contrato como injustificados o indebidos? y ¿Cual es el fundamento legal, normativo y administrativo en el que PRODECON y la Entidades Fiscalizadoras respaldan su argumento? 4.1 Explicar ¿Por qué el contrato PRODECON-SG-DRH-AD-004-2019 NO debe ser considerado una compra disfrazada? ya que el objeto del contrato sugiere que se trata de un Servicio Especializado de administración de personal de apoyo especialmente diseñado para mantener una nomina de amigos e incondicionales. 5.1 ¿Por que no fueron observados por los entes fiscalizadores (SFP, ASF y OIC de PRODECON) en la revisión de la cuenta pública 2019? 5.2 ¿Por que el Órgano de Gobierno consideró que este tipo de contratos son buenos para el desempeño de la Procuraduría? 6. Detallar los derechos y prestaciones que tuvo el personal contratado en este contrato. Para este punto se solicita un archivo en formato de datos abiertos de tipo CSV o XLSX con los siguientes campos a) Nombre del trabajador contratado b) Número de contrato asociado c) Fecha de inicio de la contratación del empleado d) Fecha de fin de contratación del empleado e) Tipo de especialista f) Cargo equivalente al personal de PRODECON g) Descripción de los servicios h) Sueldo bruto i) Carga social j) Comisión k) Total mensual facturado por empleado l) Derechos del trabajador m) Prestaciones del trabajador 6.1 ¿Como hizo PRODECON para validar el desempeño y los servicios proporcionados por el personal de Outsourcing? ¿Cual es la evidencia? Proporcionar evidencia en formato PDF."

[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 oficios número **PRODECON/SG/138/2020** y **PRODECON/SG/139/2020**, de fecha 25 de febrero de 2020, la Unidad de Transparencia turnó a la **Dirección General de Administración** y a la **Secretaría Técnica**, la solicitud de acceso a la información en estudio, al ser las Unidades Administrativas competentes para atender la petición.

III. A través del oficio **PRODECON/CTN/ST/029/2020**, de fecha 28 de febrero del año en curso, la Secretaria Técnica de esta Procuraduría, dio respuesta a la solicitud de información que nos ocupa.

IV. Mediante oficio **PRODECON/SG/DGA/041/2020**, de fecha 04 de marzo de 2020 y recibido por la Unidad de Transparencia el día 20 siguiente, la **Dirección General de Administración**, dio respuesta a la solicitud de información que nos ocupa, señalando en la parte que interesa lo siguiente:

> *"[...] **6.1 ¿Como hizo PRODECON para validar el desempeño y los servicios proporcionados por el personal de Outsourcing? ¿Cual es la evidencia? Proporcionar evidencia en formato PDF."***
>
> *En relación con este punto, se hace de su conocimiento que la información relativa a verificar el desempeño de los servicios proporcionados se advierte de los entregables que hicieron llegar en su momento dicho personal haciendo de su conocimiento que la información consta 4297 fojas por lo que se solicita a la Unidad de Transparencia que notifique los costos de reproducción correspondientes.*
>
> *De la información referida en el párrafo que antecede se hace de su conocimiento que de una revisión a la misma se advirtió información susceptible de ser clasificada como confidencial con fundamento en los artículos 116, primer párrafo de la LGTAIP; 113, fracción I, de la LFTAIP, y el Numeral Trigésimo Octavo, fracción I, y los cuales se relacionan a continuación*

RFC
CURP
NUMERO DE SEGURIDAD SOCIAL
FIRMA
HUELLA

> *Es por lo anterior se solicita a esa Unidad de Transparencia que por su conducto, se somete a aprobación del Comité de Transparencia de la Institución. [...]"*
>
> *[Sic]*

V. Atento a la clasificación de la información propuesta por la Dirección General de Administración; 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.

VI. Ahora bien, del análisis a la respuesta proporcionada por la Unidad Administrativa, se advierte que clasificó diversa información como confidencial, en términos de lo dispuesto en los artículos 116, primer párrafo, de la Ley General de Transparencia y Acceso a la Información Pública; 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; y el numeral Trigésimo Octavo, fracción I, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

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

Los datos personales que refiere la Unidad Administrativa 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) Registro Federal de Contribuyentes (RFC) de personas físicas. El RFC es una clave alfanumérica que se compone de 13 caracteres. Los dos primeros, generalmente corresponden al apellido paterno, el tercero a la inicial del apellido materno y el cuarto al primer nombre. Le sigue el año de nacimiento, mes y día; los tres últimos dígitos son la homoclave que es asignada por el Servicio de Administración Tributaria y tiene la característica de ser única e irrepetible.[1]

Al respecto, se debe indicar que para su obtención se requiere acreditar previamente mediante documentos oficiales -pasaporte, acta de nacimiento, CURP, etc.-, la identidad de la persona, su fecha y lugar de nacimiento, entre otra información.

Ahora bien, de acuerdo con la legislación tributaria, las personas físicas tramitan su inscripción al RFC, con el único propósito de

[1] Moreno, M. *Registro Federal de Contribuyentes*. 21/06/2019, de CONDUSEF Sitio web: https://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/servicios-financieros/392-registro-federal-de-contribuyentes

realizar mediante esa clave de identificación, operaciones o actividades de naturaleza tributaria. En ese sentido, el artículo 79, fracción IV del Código Fiscal de la Federación prevé que la utilización de una clave de registro no asignada por la autoridad constituye una infracción en materia fiscal.

Por lo antes apuntado, es incuestionable que el Registro Federal de Contribuyentes se encuentra vinculado al nombre de su titular, permite identificar la edad de la persona, así como su homoclave, siendo esta última única e irrepetible. De ahí, que sea un dato personal y, por tanto, información confidencial que debe protegerse.

Corrobora lo anterior, lo señalado en el Criterio 19/17, emitido por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el cual señala lo siguiente:

> ***"Registro Federal de Contribuyentes (RFC) de personas físicas.***
> *El RFC es una clave de carácter fiscal, única e irrepetible, que permite identificar al titular, su edad y fecha de nacimiento, por lo que es un dato personal de carácter confidencial."*

De acuerdo con lo anterior, resulta procedente la clasificación como confidencial del RFC al ser un dato personal, con fundamento en los artículos 116, primer párrafo, de la Ley General de Transparencia y Acceso a la Información Pública; 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; 3, fracción IX, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y el numeral Trigésimo Octavo, fracción I, de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

b) Clave Única de Registro de Población (CURP). Es un instrumento de registro que se asigna a todas las personas que viven en el territorio nacional, así como a los mexicanos que residen en el extranjero; el Registro Nacional de Población es la instancia responsable de asignar la CURP y de expedir la Constancia respectiva[2].

[2] El Registro Nacional de Población-Curp. México <<https://www.consultas.curp.gob.mx/CurpSP/html/informacionecurpPS.html>>

Lo anterior de conformidad con los artículos 86 y 91 de la Ley General de Población que a la letra disponen:

> ***"Artículo 86.-*** *El Registro Nacional de Población tiene como finalidad registrar a cada una de las personas que integran la población del país, con los datos que permitan certificar y acreditar fehacientemente su identidad; (...)"*
>
> ***"Artículo 91.-*** *Al incorporar a una persona en el Registro Nacional de Población, se le asignará una clave que se denominará Clave Única de Registro de Población. Esta servirá para registrarla e identificarla en forma individual; (...)"*

Además, consta de dieciocho elementos, representados por letras y números, que se generan a partir de los datos contenidos en el documento probatorio de la identidad (acta de nacimiento, carta de naturalización o documento migratorio), y que se refieren a:

- El primero y segundo apellidos, así como al nombre de pila.
- La fecha de nacimiento.
- El sexo.
- La entidad federativa de nacimiento.

Los dos últimos elementos de la CURP evitan la duplicidad de la Clave y garantizan su correcta integración, por lo que la Clave identifica individualmente en los registros de personas a cargo de las instituciones públicas.

En ese orden de ideas, es incuestionable que la Clave Única de Registro de Población permite identificar a la persona, así como conocer su edad y el lugar de su nacimiento, toda vez que es única e irrepetible para cada persona, por lo que es posible concluir que constituye un dato personal y, por tanto, información confidencial.

Corrobora lo anterior, lo señalado en el Criterio 18/17, emitido por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el cual señala lo siguiente:

> ***"Clave Única de Registro de Población (CURP).*** *La Clave Única de Registro de Población se integra por datos personales que sólo conciernen al particular titular de la misma, como lo son su nombre, apellidos, fecha de nacimiento, lugar de nacimiento y sexo. Dichos datos, constituyen información que distingue plenamente a una persona física del resto de los habitantes del*

país, por lo que la CURP está considerada como información confidencial."

Por lo expuesto, resulta procedente la clasificación de la CURP al ser un dato personal, con fundamento en los artículos 116, párrafo primero de la Ley General de Transparencia y Acceso a la Información Pública; 113, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública; 3, fracción IX, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y el numeral Trigésimo Octavo, fracción I de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

c) **Número de seguridad social.** Es un número compuesto por once dígitos con el cual los trabajadores que cotizan ante el Instituto respectivo son identificados por dicho organismo desde el mismo momento de su afiliación. Es de carácter personal, permanente y único. Su secuencia de números se compone de los siguientes elementos:

- **Primeros dos dígitos:** Se refiere a la subdelegación en el que fue afiliado.
- **Segundos dos dígitos:** Corresponde al año de afiliación.
- **Terceros dos dígitos:** Refiere a la fecha de nacimiento del afiliado.
- **Cuartos cuatro dígitos:** Números asignados por el Instituto al trabajador para su identificación.
- **Último dígito:** Es el número de verificación del trabajador ante el Instituto.

Además, el número de seguridad social tiene tres funciones principales que son las siguientes:

- Es el número de identificación con el cual los afiliados hacen uso de los servicios del Instituto.
- Permite consultar y monitorear periódicamente el reporte de semanas cotizadas.
- Es condición necesaria para gestionar créditos hipotecarios[3].

[3] Afiliación y Vigencia de Derechos Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado <<https://www.gob.mx/issste/acciones-y-programas/afiliacion-y-vigencia-de-derechos>>

En esa virtud, resulta procedente la clasificación del número de seguridad social como un dato personal confidencial, toda vez que permite identificar a la persona a través de su fecha de nacimiento, así como el inicio de su relación laboral, además de que, de proporcionarlo, existiría vulnerabilidad de su situación económica y patrimonial.

Lo anterior, de conformidad con lo dispuesto en los artículos 116, párrafo primero de la Ley General de Transparencia y Acceso a la Información Pública; 113, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública; 3, fracción IX, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y el numeral Trigésimo Octavo, fracción I de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

d) Firma. La firma se define como el *"rasgo o conjunto de rasgos, realizados siempre de la misma manera, que identifican a una persona y sustituyen a su nombre y apellidos para aprobar o dar autenticidad a un documento."*

Como se puede observar, el gráfico es una insignia de la personalidad, en virtud de que es una imagen que nos representa ante los demás y que posee el fin de identificar, asegurar o autentificar la identidad de su autor.

En ese sentido, al ser la firma un rasgo a través del cual se puede identificar a su autor y permite autentificar el contenido de un documento suscrito por aquel, dichas razones son suficientes para considerar a este dato como confidencial en términos de lo dispuesto por los artículos 116, párrafo primero de la Ley General de Transparencia y Acceso a la Información Pública; 113, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública; 3, fracción IX, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y numeral Trigésimo Octavo, fracción I, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

e) Huella Digital/Dactilar. Al respecto, es importante precisar que, para la Agencia Española de Protección de Datos, los datos biométricos, son *"aquellos aspectos físicos que, mediante un análisis técnico, permiten distinguir las singularidades que*

concurren respecto de dichos aspectos en un sujeto y que, resultando que es imposible la coincidencia de tales aspectos en dos individuos, una vez procesados, permiten servir para identificar al individuo en cuestión. Así se emplean para tales fines las huellas digitales, el iris del ojo, la voz, etc".[4]

Cabe señalar que la huella dactilar al ser un dato biométrico estático, es decir, que se encuentra invariable a lo largo de la vida de su titular, permite la identificación plena del mismo.

En ese sentido, la información referente a la huella digital/huella dactilar, se encuentra clasificada como confidencial, en términos de los artículos 116, párrafo primero de la Ley General de Transparencia y Acceso a la Información Pública; 113, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública; 3, fracción IX, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y el numeral Trigésimo Octavo, fracción I de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

En ese orden de ideas y una vez realizado un análisis minucioso de la clasificación de información, este Comité de Transparencia considera que el **RFC, CURP, Número de Seguridad Social, Firma** y la **Huella Dactilar/Digital**, constituyen datos personales concernientes a una persona física identificada o identificable, respectivamente; por lo tanto, estima que se cuenta con los elementos suficientes para confirmar la clasificación de la información con el carácter de confidencial.

En razón de lo antes expuesto, este Comité de Transparencia **CONFIRMA LA CLASIFICACIÓN** como **CONFIDENCIAL** de los datos personales que se advierten en la información a la cual pretende tener acceso el peticionario (entregables), relacionada con la solicitud de acceso a la información pública número **0063200012320**, relativos al **RFC, CURP, Número de Seguridad Social**, **Firma** y **Huella Dactilar/Digital;** en términos de lo dispuesto en los artículos 116, párrafo primero de la Ley General de Transparencia y Acceso a la Información Pública; 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; 3, fracción IX, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y el numeral

[4]. Informe 0392/2011 de la Agencia Española de Protección de Datos. Disponible para consulta en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/calidad/common/pdfs/2011-0392_Reconocimiento-facial-en-acceso-a-clases.pdf

Trigésimo Octavo, fracción I, 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 mayoría LA CLASIFICACIÓN** como **CONFIDENCIAL** de los datos personales materia de la solicitud de información **0063200010220**, relativos a los: **nombres de los usuarios no vigentes u obsoletos que utilizaron el sistema SICSS, la relación de usuarios dados de baja que se advierte del procedimiento de borrado seguro y los nombres de los ex servidores públicos que se advierten en los informes de borrado de datos (certificados de borrado seguro) generados desde febrero del 2016 hasta enero del 2020;** en términos de lo dispuesto en los artículos 116, primer párrafo, de la Ley General de Transparencia y Acceso a la Información Pública; 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; 3, fracción IX, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y el numeral Trigésimo Octavo, fracción I, de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas.

SEGUNDO.- Se **CONFIRMA por mayoría LA CLASIFICACIÓN** como **RESERVADA** de la información relativa a los **informes de borrado de datos** (certificados de borrado seguro), contenida en la prueba de daño que se acompaña a la respuesta de la solicitud de información **0063200010220**; 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 mayoría LA CLASIFICACIÓN** como **RESERVA PARCIAL** de la información contenida en la **documentación de control de cambios**, relativa a los **Nombres de Servidores, Instancia de Base de datos y ubicación de carpeta de archivos**, contenida en la prueba de daño que se acompaña a la respuesta de la solicitud de información **0063200011320**; 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 **INSTRUYE** a la Unidad de Transparencia, a efecto de que notifique al solicitante los costos por la reproducción de la información relativa a la **documentación de control de cambios**; así como todas las modalidades de acceso previstas en la ley de la materia.

QUINTO.- Se **INSTRUYE** a la Dirección de Sistemas Sustantivos, a que elabore las versiones públicas de la **documentación de control de cambios**, a que se refiere en su respuesta, para su posterior entrega por parte de la Unidad de Transparencia al solicitante, una vez que se hayan cubierto los costos de reproducción.

SEXTO.- Se **CONFIRMA por mayoría LA CLASIFICACIÓN** como **CONFIDENCIAL** de los datos contenidos en la información que pretende tener acceso el peticionario (entregables), relativos al **RFC, CURP, Número de Seguridad Social, Firma** y **Huella Dactilar/Digital,** materia de la solicitud de información 0063200012320; en términos de lo dispuesto en los artículos 116, párrafo primero de la Ley General de Transparencia y Acceso a la Información Pública; 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; 3, fracción IX, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; y el numeral Trigésimo Octavo, fracción I, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

SÉPTIMO.- Se **INSTRUYE** a la Unidad de Transparencia, a efecto de que notifique al solicitante los costos por la reproducción de la información, relacionada con la solicitud de acceso número **0063200012320**; así como todas las modalidades de acceso previstas en la ley de la materia.

OCTAVO.- Se **INSTRUYE** a la Dirección General de Administración, a que elabore las versiones públicas de la información a la que pretende tener acceso el peticionario, una vez cubierto el pago de derechos que al respecto haya realizado el requirente, para su posterior entrega por parte de la Unidad de Transparencia.

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 12:30 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.

Sin representación
Órgano Interno de Control en la PRODECON.

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