

SFP

SECRETARÍA DE
LA FUNCIÓN PÚBLICA



COMITE DE TRANSPARENCIA

Folio: 2700100013516

Ciudad de México, a veintiséis de octubre de dos mil dieciséis.

VISTO: El estado que guarda el procedimiento de acceso a la información, derivado de la solicitud presentada el 13 de septiembre de 2016, a través de la Plataforma Nacional de Transparencia, a la que corresponde el número de folio 2700100013516, y

RESULTANDO

I.- Que mediante la referida solicitud, se requirió la información siguiente:

Modalidad preferente de entrega de información

"Entrega por Internet en la PNT" (sic)

Descripción clara de la solicitud de información

"Se solicita entregar en formato electrónico, copia de los contratos (incluyendo sus anexos técnicos) que haya celebrado la dependencia del 2013 a la fecha, cuyo objeto se encuentre relacionado con las tecnologías de la información (por ejemplo cómputo, impresión, energía, fotocopiado, centros de datos, digitalización, telecomunicaciones, red de datos, etc)" (sic)

II.- Que a través de la resolución de 11 de octubre de 2016, con fundamento en lo dispuesto por los artículos 65, fracción II y 135, de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 44 y 132, de la Ley General de Transparencia y Acceso a la Información Pública, este Comité de Transparencia determinó la ampliación del plazo de respuesta por un periodo hasta por diez días, toda vez que no contaba con los elementos suficientes para su debido pronunciamiento.

III.- Que por oficio No. SPRHySPC/40/2016 de 7 de octubre de 2016, la Dirección General de Administración y Finanzas del Instituto de Administración y Avalúos de Bienes Nacionales informó a este Comité, que pone a disposición del peticionario versión pública de los contratos que atienden lo solicitado, constantes de 366 fojas útiles, en la que se eliminarán los datos confidenciales consistentes en la credencial de elector, pasaporte y cédula profesional, de conformidad con lo dispuesto en los artículos 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 116 de la Ley General de Transparencia y Acceso a la Información Pública.

IV.- Que mediante oficio No. 514/DGRMSG/0798/2016 de 26 de octubre de 2016, la Dirección General de Recursos Materiales y Servicios Generales comunicó a este Comité, que pone a disposición del particular versión pública de 156 contratos que atienden lo solicitado, constante de 6,408 fojas útiles, en la que se eliminarán los datos confidenciales consistentes en el número de cuenta y clave bancaria estandarizada, credencial de elector, teléfono, Registro Federal de Contribuyentes, domicilio y pasaporte, así como los accesos para red (ip), y el dimensionamiento de la infraestructura (propuesta técnica del proveedor), y la propuesta económica del proveedor, de conformidad con lo dispuesto en los artículos 113, fracciones I y II, de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 116 de la Ley General de Transparencia y Acceso a la Información Pública.

Por otra parte, la unidad administrativa señaló la reserva del anexo dos de los contratos DC-119-2015, DC-143-2015, DC-027-2014 y DC-070-2013, que se refieren a la propuesta técnica del proveedor (tales como propuesta de solución); asimismo señaló que el contrato No. OT/039/2013 contiene información reservada relativa al servicio de pruebas de estrés para el aplicativo DeclaraNet plus, y el DC-084-2013 contiene información reservada relacionada con aplicación de evaluaciones, empero, fundamenta dicha reserva en los artículos 113 de la Ley Federal de Transparencia y Acceso a la Información Pública y 116 de la Ley General de Transparencia y Acceso a la Información Pública.

V.- Que a través de oficio No. 511/DGTI/1078/2016 y comunicación electrónica de 26 de octubre, 2016, la Dirección General de Tecnologías de Información informó a este Comité, que de conformidad con el

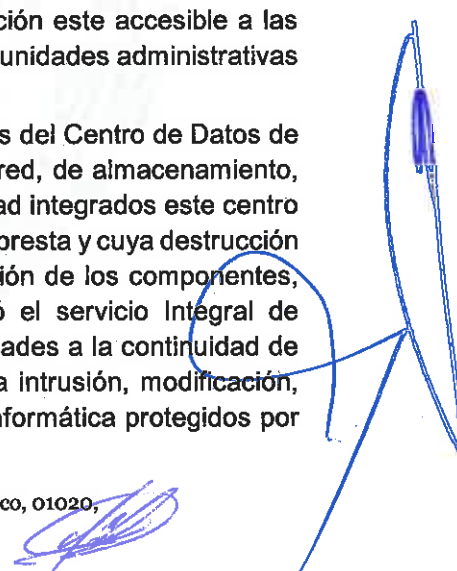
artículo 74, fracción XI, del Reglamento Interior de la Secretaría de la Función Pública derivado de la revisión efectuada a los instrumentos en cuestión, así como de los anexos que forman parte de los mismos, determinó los caos que contienen información clasificada como reservada y confidencial que contienen los mismos, no obstante señaló que la documentación que contiene la información solicitada, es administrada por la Dirección General de Recursos Materiales y Servicios Generales, por lo que será dicha unidad administrativa la que se pronuncie respecto a la forma en que se pondrá a disposición la información.

En este sentido, la unidad administrativa manifestó que los contratos DC-107-2013 – DC-CM-005-2014, denominado “Contrato plurianual de adquisición de bienes y prestación de servicios para el establecimiento y puesta en marcha de un nuevo centro de datos de alta disponibilidad para la Secretaría de la Función Pública y su Convenio Modificatorio”, y DC-087-2014, en sus Anexos Uno y Dos, denominado “Contrato para la adquisición de transformador de pedestal de 500 KVA para el centro de datos de la Secretaría de la Función Pública” de conformidad con los artículos 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, de aplicación supletoria a la Ley Federal, están reservados.

En virtud de la reserva de la información relativa al contrato DC-107-2013 y su anexo modificatorio DC-CM-005-2014 señalada la unidad administrativa indicó que la información contenida en el Anexo Uno “Especificaciones técnicas y alcances del Servicio y sus Anexos A y B” y Anexo Dos consistente en la Propuesta Técnica y Económica del “Proveedor”, así como los cuatro anexos del convenio modificatorio, contienen la descripción de los componentes y mecanismos tecnológicos, así como su ubicación, mediante los cuales se realiza la publicación y operación de los sistemas de información catalogados como críticos, debido a que su correcto funcionamiento contribuye de manera directa al cumplimiento de los objetivos de la Secretaría y al ejercicio de diversas funciones de las dependencias y entidades de la Administración Pública Federal, por lo que con el propósito de garantizar la confidencialidad de los mecanismos, configuraciones, procedimientos y demás recursos de seguridad de las instalaciones de tecnologías de la información y comunicaciones que resguardan la información a través de los cuales esta Secretaría cumple sus metas fiscalizadoras y de rendición de cuentas.

En este contexto, la unidad administrativa señaló que el centro de datos de alta disponibilidad provisto a través de este contrato, fue concebido, equipado y aprovisionado previendo las mejores condiciones operativas posibles para la seguridad de la información con la que operan los sistemas de información críticos, y el cual dispone de elementos de hardware y software, dispuestos tecnológicamente para garantizar en la mayor medida posible que la información este accesible a las personas afines a ella, a través de los medios que la Secretaría a través de sus unidades administrativas han establecido, acorde a la normatividad vigente.

Lo anterior, toda vez que actualmente la Secretaría resguarda a través del Centro de Datos de Alta de disponibilidad, el equipamiento tecnológico, como son los equipos de red, de almacenamiento, de procesamiento, de respaldo, de soporte físico y demás sistemas de seguridad integrados este centro de datos, que son indispensables para la provisión de los servicios públicos que presta y cuya destrucción o inhabilitación resultaría una amenaza, por lo que de no reservar la descripción de los componentes, mecanismos y el entorno tecnológicos mediante los cuales se proporcionó el servicio Integral de Seguridad Informática, podría propiciar la explotación maliciosa de vulnerabilidades a la continuidad de operaciones de la dependencia, toda vez que se pretende prevenir y evitar la intrusión, modificación, pérdida o destrucción de la información contenida en sistemas o equipos de informática protegidos por los mecanismos de seguridad de los equipos a cargo de esta dependencia.





Adicionalmente, el objetivo del proceso de Administración de la Seguridad de la Información previsto en el Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones, y en la de seguridad de la información, consiste en evaluar, diseñar, establecer y vigilar los mecanismos que permitan la administración de la seguridad de la información de la Secretaría, así como disminuir el impacto de eventos adversos que potencialmente puedan afectar el logro de los objetivos institucionales, por lo que de no reservar la información respecto de la descripción de los componentes, mecanismos y el entorno tecnológico mediante los cuales se proporcionó el establecimiento y puesta en marcha de un nuevo centro de datos de alta disponibilidad, permitiría el análisis de potenciales vulnerabilidades a la infraestructura, la información y los procesos que lo sustentan, lo que potencializa la comisión de conductas que son tipificadas por el Código Penal Federal como delitos.

Asimismo, la Dirección General de Tecnologías de Información señaló que las instalaciones de tecnologías de información y comunicaciones de la Secretaría, como son los equipos de seguridad perimetral, la red de comunicaciones, los elementos de seguridad física y protección a contingencias, consistente en equipos especializados instalados, configurados y operados desde el centro de datos de alta disponibilidad, que son indispensables para la provisión de los servicios públicos que presta y cuya intromisión, modificación, pérdida, destrucción o inhabilitación de forma temporal o definitiva, materializa una amenaza en contra de la información y los sistemas o equipos de informática de la Secretaría de la Función Pública, por lo que aún y cuando los servicios del contrato DC-107-2013, y su Convenio modificatorio DC-CM-005-2014, concluyeron su vigencia, es necesario reservar la información relacionada con la arquitectura tecnológica y el entorno de operación de los elementos operativos del centro de datos de alta disponibilidad que fueron provistos como parte de tales instrumentos.

Por otra parte, en cuanto al contrato DC-087-2014 contiene la descripción de elementos técnicos, así como su ubicación, mediante los cuales se brinda el soporte a la publicación y operación de los sistemas de información catalogados como críticos, debido a que su correcto funcionamiento contribuye de manera directa al cumplimiento de los objetivos de la Secretaría, así como al ejercicio de diversas funciones de las dependencias y entidades de la Administración Pública Federal, por lo que con el propósito de la reserva de las condiciones operativas de tales infraestructuras de soporte que mantienen la disponibilidad de la información a través de los cuales la Secretaría cumple sus metas fiscalizadoras y de rendición de cuentas se actualiza el supuesto de reserva señalado.

Lo anterior, en virtud de que la infraestructura de soporte operativo fue concebido, equipado y aprovisionado previendo las mejores condiciones posibles para la continuidad en su funcionamiento con lo que se brindarían condiciones de seguridad de la información con la que operan los sistemas de información críticos, y el cual dispone de elementos dispuestos tecnológicamente para garantizar en la mayor medida posible que la información este accesible a las personas afines a ella, a través de los medios que la Secretaría a través de sus unidades administrativas han establecido, acorde a la normatividad vigente,

Asimismo debe considerarse que actualmente la Secretaría resguarda a través del Centro de Datos de Alta de disponibilidad, el equipamiento tecnológico, como son los equipos de red, de almacenamiento, de procesamiento, de respaldo, de soporte físico y demás sistemas de seguridad integrados este centro de datos, que son indispensables para la provisión de los servicios públicos que presta y cuya destrucción o inhabilitación resultaría una amenaza, por lo que de no reservar la descripción y localización de los componentes de soporte operativo al señalado centro de datos, podría propiciar la explotación maliciosa de vulnerabilidades a la continuidad de operaciones de la dependencia,

lo cual sustenta la reserva que se presenta, toda vez que se pretende prevenir y evitar la intrusión, modificación, pérdida o destrucción de la información contenida en sistemas o equipos de informática protegidos por elementos de soporte operativo de los equipos a cargo de la Secretaría de la Función Pública que forma parte de uno de los poderes del Estado.

En efecto, las instalaciones que soportan la operación de la infraestructura de tecnologías de información y comunicaciones de la Secretaría, como son los centros de datos, y en específico el de alta disponibilidad, se considera como una infraestructura crítica y estratégica, al resultar indispensables para la provisión de los servicios públicos que presta y cuya intromisión, modificación, pérdida, destrucción o inhabilitación de forma temporal o definitiva, materializa una amenaza en contra de la información y los sistemas o equipos de informática de la Secretaría de la Función Pública, por lo que aún y cuando los bienes y servicios del contrato DC-087-2014, Contrato para la adquisición de transformador de pedestal tipo trifásico TR-1 de 500 KVA para el centro de datos de la Secretaría de la Función Pública, concluyeron su vigencia, es necesario reservar la información relacionada con el entorno de operación de los elementos que sustentan el correcto funcionamiento del centro de datos de alta disponibilidad que fueron provistos.

Con las exposiciones anteriores, la unidad administrativa indicó que la reserva de los contratos señalados se actualiza el daño presente que ocasionaría la difusión de esta información, se traduce en hacer del conocimiento general la ubicación, agentes de riesgo potenciales, existentes y explotables, y en general las condiciones actuales de operación de los equipos del centro de datos y sistemas institucionales, poniendo en riesgo las previsiones y mecanismos que el conjunto de infraestructuras dispuestas alrededor del centro de datos proporciona para preservar la confidencialidad, integridad y disponibilidad de la información, y que al exponerlos a un acceso no autorizado o a un ataque intencionado y dirigido podría derivar en la obtención o la alteración o la pérdida de información sensible para la operación de la Secretaría de la Función Pública y en general de la Administración Pública Federal, como podría ser el caso de un acceso no autorizado a bases de datos con información confidencial de personas identificadas o identificables, impactando en el cumplimiento de las atribuciones de la SFP, el deterioro de la imagen de la Secretaría y el debilitamiento de las instituciones ante la ciudadanía, que al ser sujetos de un análisis dirigido, se podrían explotar posibles vulnerabilidades actuales sobre la operación de los procesos críticos de las tecnologías de información y comunicaciones de la red, equipos y sistemas institucionales aún existentes, pudiendo evadir con ello las previsiones y mecanismos que este servicio proporciona para preservar la confidencialidad, integridad y disponibilidad de la información de la Secretaría, orientados a impedir el acceso ilícito a sistemas y equipos de informática.

Además, hacer pública la información implicaría un daño probable debido a que sería necesario establecer medidas contingentes adicionales para prevenir cualquier situación de riesgo que derive de cualquier posible explotación a las vulnerabilidades expuestas con el conocimiento de configuraciones, capacidades y arquitecturas de las tecnologías que conforman el centro de datos de alta disponibilidad, destinando recursos públicos para un fin al que no están afectos, debido a la necesidad de redefinir o establecer nuevas configuraciones de equipos y planes de servicios, así como nuevos diseños y desarrollos de tecnologías de información, al quedar materialmente vulnerados los vigentes, en perjuicio del logro de los objetivos institucionales y el ejercicio de atribuciones legales.

El daño específico consiste en que la información relativa a la infraestructura del centro de datos de alta disponibilidad de la Secretaría de la Función Pública descrita como parte de las especificaciones técnicas y la propuesta del proveedor adjudicado que podrían ser utilizadas para



perpetrar ataques intencionados mediante la explotación de vulnerabilidades conocidas en las tecnologías y mecanismos de operación existentes, así como el entorno de operación actual, exponiendo con ello la información de carácter personal, relativa a procedimientos de fiscalización, de control del ejercicio público y de obligaciones de transparencia, al robo, alteración y el mal uso, impactando el cumplimiento de las metas de la Secretaría, lo que potencialmente puede afectar el logro de los objetivos institucionales o podrían configurar inclusive, como ha sido expuesto la comisión de conductas sancionadas por el Código Penal Federal como delitos.

Finalmente, la Dirección General de Tecnologías de Información señaló que las características especiales y específicas del Centro de datos de alta disponibilidad con el que opera la Secretaría, se refieren a información de carácter reservada en su ubicación, agentes de riesgo existentes y explotables, y en general las condiciones actuales de operación de los equipos del centro de datos y sistemas institucionales, su configuración, arquitectura, así como la información que detenta, por lo que debe ser reservado por un plazo de 5 años.

VI.- Que a través de oficio No. UGD/DGAENG/DPIGD/409/2176/2016 de 24 de octubre de 2016, la Unidad de Gobierno Digital informó a este Comité, que los contratos y anexos que atienden lo solicitado serán proporcionados por la Dirección General de Recursos Materiales y Servicios Generales.

Ahora bien, respecto a los contratos y anexos que obran en el archivo de la Unidad de Gobierno Digital, la unidad administrativa señaló que dichos instrumentos están clasificados como confidenciales, con fundamento en el artículo 46, fracción XV, de la Ley de Instituciones de Crédito; y 14, fracciones I y II de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental por tratarse de un secreto fiduciario, por un plazo de 12 años por el Banco Nacional de Obras y Servicios Públicos, S. N. C., en su carácter de fiduciario del Fideicomiso Público de Administración e Inversión No. 2058 e-México (Fideicomiso e-México).

Empero, la unidad administrativa indicó que en aras de observar el principio de máxima publicidad, pone a disposición del particular 6 contratos y sus anexos constantes de un total de 2,192 fojas útiles, relativos a los contratos denominados 1) Servicios de Centro de Datos y Aplicativos para la plataforma GOB.MX; 2) Servicios para la instrumentación de la estrategia de crecimiento e institucionalización de procesos en materia de datos abiertos en la Administración Pública Federal; 3) Servicios especializados integrales para el apoyo, análisis y ejecución de proyectos relacionados con el desarrollo de sistemas informáticos en la Administración Pública Federal en materia de datos abiertos, así como de programas de implementación, capacitación, innovación, uso y evaluación de los mismos; 4) Servicios de desarrollo, mantenimiento y soporte a la plataforma y aplicaciones críticas del proyecto de Ventanilla Única Nacional; 5) Adquisición de licenciamiento de software del bus de interoperabilidad, de la herramienta de gestión de procesos, y de identidad y control de accesos, así como la prestación de los servicios de soporte técnicos relacionadas con las mismas; y 6) Servicios de aseguramiento de calidad de la Administración de Proyectos de desarrollo de soluciones tecnológicas integradas a gob.mx, en los que testará los datos confidenciales relativos al secreto comercial, contenidos en los anexos técnicos y económicos presentados por los proveedores, lo anterior, con fundamento en los artículos 113, fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública, y 116 de la Ley General de Transparencia y Acceso a la Información Pública.

En este orden de ideas, la unidad administrativa abundó en que los anexos técnicos y económicos presentados por los proveedores en los contratos que nos ocupan contienen información que reviste los

supuestos previstos en el Cuadragésimo Cuarto de los Lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, como a continuación se señala:

- I. Es información generada con motivo de actividades comerciales del proveedor titular señalado en el contrato y sus anexos, en términos de lo dispuesto en la Ley de Propiedad Industrial;
- II. La información es guardada por la Dirección General Adjunta de Proyectos de Gobierno Digital de la Unidad de Gobierno Digital con carácter de confidencial, adoptando las medidas necesarias para preservarla con dicho carácter.
- III. La información significa obtener o mantener una ventaja competitiva o económica frente a terceros; ya que la misma fue objeto de una evaluación técnica cuyo resultado determinó la designación del proveedor, en concordancia con lo señalado en el artículo 134, párrafo tercero de la Constitución Política de los Estados Unidos Mexicanos.
- IV. La información no es del dominio público ni resulta evidente para un técnico o perito en la materia, con base en la información previamente disponible o la que deba ser divulgada por disposición legal o por orden judicial, ya que no fue publicada en el sistema electrónico denominado Compranet, ni se conoce por algún otro medio.

Finalmente, la unidad administrativa precisó que los anexos técnicos y económicos de los instrumentos de mérito cumplen con los requisitos señalados por el artículo 39 del Acuerdo sobre los aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio, a saber:

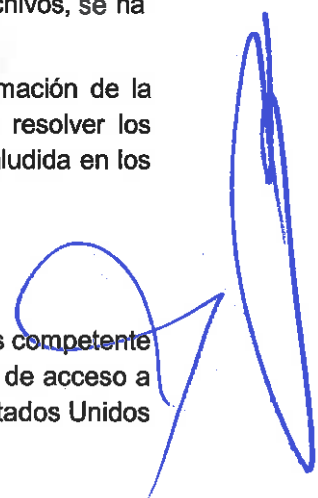
- a) Los contratos y sus anexos son secretos, ya que no son generalmente conocidos ni fácilmente accesibles para personas introducidas en los círculos en que normalmente se utiliza el tipo de información en cuestión; y
- b) Los contratos y sus anexos tienen un valor comercial por ser secretos; y
- c) Los contratos y sus anexos han sido objeto de medidas razonables, en las circunstancias, para mantenerlos secretos, tomadas por la persona que legítimamente la controla; ya que es resguardada por la Dirección General Adjunta de Proyectos de Gobierno Digital de la Unidad de Gobierno Digital con carácter de confidencial, adoptando computadoras con usuario y contraseña para preservarla con dicho carácter.

VII.- Que observando en lo conducente las disposiciones vigentes en materia de Archivos, se ha formado el expediente en que se actúa, con las constancias antes enunciadas.

VIII.- Que de conformidad con lo previsto en el Reglamento del Comité de Información de la Secretaría de la Función Pública, encontrándose en sesión permanente para, entre otros, resolver los procedimientos de su competencia, es de procederse al estudio y análisis de la información aludida en los resultandos precedentes, y

CONSIDERANDO

PRIMERO.- Este Comité de Transparencia de la Secretaría de la Función Pública es competente para conocer, dictar los acuerdos que sean necesarios y resolver el presente procedimiento de acceso a la información, de conformidad con los artículos 6o. y 8o. de la Constitución Política de los Estados Unidos





Mexicanos; 64, 65, fracción II, 103, 108, 110, 113, y 140, de la Ley Federal de Transparencia y Acceso a la Información Pública; 43, 44, fracción II, 104, 111, 113, 116 y 137, de la Ley General de Transparencia y Acceso a la Información Pública; y 6, fracción II, del Reglamento del Comité de Transparencia de la Secretaría de la Función Pública, en relación con el Tercero Transitorio del Decreto por el que se abroga la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y se expide la Ley Federal de Transparencia y Acceso a la Información Pública, publicado en el Diario Oficial de la Federación el 9 de mayo de 2016.

Con independencia de lo anterior, en tratándose de datos personales se estará a lo dispuesto en el Segundo Transitorio de la Ley Federal de Transparencia y Acceso a la Información Pública, y las disposiciones correlativas de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, su Reglamento y disposiciones administrativas que regulan aquéllos.

SEGUNDO.- En el folio que nos ocupa, se requiere obtener la información señalada en el Resultando I, del presente fallo, misma que se tiene por reproducida para los efectos conducentes.

Al respecto, la Dirección de Administración y Finanzas del Instituto de Administración y Avalúos de Bienes Nacionales, la Dirección General de Recursos Materiales y Servicios Generales, y la Unidad de Gobierno Digital, ponen a disposición versión pública de una parte de la información, conforme a lo señalado en los Resultandos III, IV, y VI, de esta resolución.

Previo a continuar con el análisis de los datos confidenciales comunicados por la Dirección General de Recursos Materiales y Servicios Generales, es de precisarse que el dato relativo a los accesos para red (ip), en el presente caso no corresponde a un dato confidencial, toda vez éste no encuadra en ninguno de los supuestos previstos en el artículo 113 de la Ley Federal de Transparencia y Acceso a la Información Pública, por lo que no será testado en la información que se entrega al particular.

Ahora bien, por lo que hace al señalamiento de la Dirección General de Recursos Materiales y Servicios Generales de una parte de la información reservada contenida en los contratos DC-119-2015, DC-143-2015, DC-027-2014, DC-070-2013, OT/039/2013 y DC-084-2013, consistente en la propuesta técnica del proveedor (tales como propuesta de solución) y al servicio de pruebas de estrés para el aplicativo DeclaraNet plus, y la relacionada con aplicación de evaluaciones, destaca que considerando el contenido de los contratos, esta información corresponde a la propuesta técnica del proveedor, por lo que no encuadra en ninguno de los supuestos de reserva previstos en el artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública, sino en el supuesto de confidencialidad previsto en el artículo 113, fracción II, del mismo ordenamiento.

Lo anterior, en atención a que si bien es cierto, uno de los objetivos de la Ley Federal de Transparencia y Acceso a la Información Pública, es permitir que toda persona tenga acceso a la información en poder de los sujetos obligados de conformidad con las facultades que les correspondan; también lo es que en términos de lo previsto en el Título Cuarto de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el Título Sexto de la Ley General de Transparencia y Acceso a la Información Pública, de aplicación supletoria a la ley de la materia, se establece la información que se considera confidencial, misma que en términos del artículo 11, fracción VI, de la Ley Federal de Transparencia y Acceso a la Información Pública, los sujetos obligados deben proteger y resguardar.

Conforme a lo dispuesto por el Quinto, Décimo y Undécimo de los Lineamientos de Protección de Datos Personales, en relación con el Segundo Transitorio del Decreto por el que se abroga la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y se expide la Ley Federal de

Transparencia y Acceso a la Información Pública, publicado en el Diario Oficial de la Federación el 9 de mayo de 2016, los servidores públicos deberán adoptar las medidas necesarias para garantizar el tratamiento, confidencialidad y seguridad de los datos personales concernientes a una persona física, identificada o identificable, que recaben u obtengan en ejercicio de sus atribuciones, mismos que no podrán difundir salvo que medie el consentimiento del titular de dichos datos.

Así las cosas, y dado lo comunicado por la Dirección de Administración y Finanzas del Instituto de Administración y Avalúos de Bienes Nacionales, la Dirección General de Recursos Materiales y Servicios Generales, y la Unidad de Gobierno Digital, en el sentido de que habría de protegerse datos personales so pena de incurrir en falta a los ordenamientos vigentes en la materia, es de analizarse la procedencia de testar dichos datos a efecto de que no aparezcan en la versión pública que pueda ponerse a disposición del particular, previo el pago de los derechos correspondientes.

De esa guisa, es preciso establecer que la protección de los datos personales se encuentra prevista desde la Constitución Política de los Estados Unidos Mexicanos, estableciendo al efecto lo siguiente:

ARTÍCULO 6. La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado

Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:

[...]

II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

[...]

ARTÍCULO 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.

Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

[...]

De los preceptos constitucionales transcritos, se desprende que la información que se refiere al ámbito privado de las personas, así como los datos personales, debe estar protegida, en los términos y con las excepciones a los principios de tratamiento de datos que por razones de orden público fije la ley, por lo que **toda persona tiene derecho a la protección de sus datos personales.**

En seguimiento con lo anterior, la Ley Federal de Transparencia y Acceso a la Información Pública, como encargada de normar el acceso a los datos personales en posesión de las dependencias y entidades de la Administración Pública Federal, establece lo siguiente:

Artículo 113. Se considera información confidencial:

- I. La que contiene datos personales concernientes a una persona física identificada o identificable;
- II. Los secretos bancario, fiduciario, industrial, comercial, fiscal, bursátil y postal, cuya titularidad corresponda a particulares, sujetos de derecho internacional o a sujetos obligados cuando no involucren el ejercicio de recursos públicos, y



- III. Aquella que presenten los particulares a los sujetos obligados, siempre que tengan el derecho a ello, de conformidad con lo dispuesto por las leyes o los tratados internacionales.

La información confidencial no estará sujeta a temporalidad alguna y sólo podrán tener acceso a ella los titulares de la misma, sus representantes y los Servidores Públicos facultados para ello.

...

TRANSITORIOS

...

SEGUNDO. ...

En tanto no se expidan las leyes generales en materia de datos personales en posesión de sujetos obligados y archivo, permanecerá vigente la normatividad federal en la materia.

...

A su vez, la Ley General de Transparencia y Acceso a la Información Pública, aplicable supletoriamente a la citada Ley Federal, prevé:

Artículo 116. Se considera información confidencial la que contiene datos personales concernientes a una persona identificada o identificable.

La información confidencial no estará sujeta a temporalidad alguna y sólo podrán tener acceso a ella los titulares de la misma, sus representantes y los Servidores Públicos facultados para ello.

Se considera como información confidencial: los secretos bancario, fiduciario, industrial, comercial, fiscal, bursátil y postal, cuya titularidad corresponda a particulares, sujetos de derecho internacional o a sujetos obligados cuando no involucren el ejercicio de recursos públicos.

Asimismo, será información confidencial aquella que presenten los particulares a los sujetos obligados, siempre que tengan el derecho a ello, de conformidad con lo dispuesto por las leyes o los tratados internacionales.

Así las cosas, es necesario analizar cada uno de los datos que se consideran como confidenciales de acuerdo con lo señalado por la Dirección de Administración y Finanzas del Instituto de Administración y Avalúos de Bienes Nacionales, la Dirección General de Recursos Materiales y Servicios Generales, y la Unidad de Gobierno Digital, y en consecuencia resulta necesario proteger, al tenor de lo siguiente:

a) **Cuenta bancaria o número de cuenta bancaria y/o Clave Bancaria Estandarizada (Clabe Interbancaria) de una persona moral**, la clasificación de este dato obedece a lo dispuesto por los artículos 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública, y 116 de la Ley General de Transparencia y Acceso a la Información Pública, de aplicación supletoria a la Ley Federal, atendiendo a que este número está asociado al **patrimonio de la persona moral** entendiendo éste como el conjunto de bienes, derechos y obligaciones que le corresponden, y que constituyen una universalidad jurídica, que se relaciona con su patrimonio y a través del cual el cliente puede acceder a la información relacionada con éste, contenida en las bases de datos de las instituciones bancarias y financieras, en donde se pueden realizar diversas transacciones como son movimientos y consulta de saldos. Por lo anterior, en los casos en que el acceso a documentos conlleve la revelación del número de cuenta bancaria, deberán elaborarse versiones públicas en las que deberá testarse dicho dato, por tratarse de información de carácter patrimonial, cuya difusión no contribuye a la rendición de cuentas.

Ante esa circunstancia, el dato señalado debe protegerse y por ende testarse o eliminarse del documento que pudiera ponerse a disposición del peticionario, para evitar su acceso no autorizado, atento a lo previsto por los artículos 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública,



y 116 de la Ley General de Transparencia y Acceso a la Información Pública, de aplicación supletoria a la Ley Federal.

b) **Credencial de elector** debe referirse que ésta, es el documento indispensable para que los ciudadanos puedan ejercer su derecho de voto, según lo establece el artículo 176 del Código Federal de Instituciones y Procedimientos Electorales, en el tenor siguiente:

"ARTÍCULO 176.

[...]

2. La Credencial para votar es el documento indispensable para que los ciudadanos puedan ejercer su derecho de voto.

[...]"

Ahora bien, respecto de la información contenida en las credenciales para votar, cabe señalar lo dispuesto en el artículo 200 del citado ordenamiento legal:

"ARTÍCULO 200.

1. La credencial para votar deberá contener, cuando menos, los siguientes datos del elector:

- a) Entidad federativa, municipio y localidad que corresponden al domicilio;
- b) Sección electoral en donde deberá votar el ciudadano,
- c) Apellido paterno, apellido materno y nombre completo;
- d) Domicilio;
- e) Sexo;
- f) Edad y año de registro;
- g) Firma, huella digital y fotografía del elector;
- h) Clave de registro; y
- i) Clave Única del Registro de Población.

2. Además tendrá:

- a) Espacios necesarios para marcar año y elección de que se trate;
- b) Firma impresa del secretario ejecutivo del Instituto Federal Electoral;
- c) Año de emisión; y
- d) Año en el que expira su vigencia.

[...]

La credencial para votar contiene diversa información que, en su conjunto, configura el concepto de dato personal previsto en la Ley de la materia, al estar referida a personas físicas identificadas, entre otra: nombre, domicilio, sexo, edad y año de registro, firma autógrafa, huella digital, fotografía del elector, clave de registro y Clave Única del Registro Nacional de Población.

A continuación se ejemplificará el contenido que tienen las credenciales para votar presentadas, expedidas por el entonces Instituto Federal Electoral:



Handwritten signature in blue ink.



Como se observa, la credencial para votar contiene diversa información que, en su conjunto, configura el concepto de dato personal previsto en la Ley de la materia, al estar referida a personas físicas identificadas, entre otra: nombre, domicilio, sexo, edad y año de registro, firma autógrafa, huella digital, fotografía del elector, clave de registro y Clave Única de Registro de Población (CURP), así como el OCR, en razón de lo anterior con excepción hecha al CURP, sexo, edad y domicilio, se analizarán los demás datos restantes, atento a las consideraciones siguientes:

Número Identificador (OCR), éste puede ser de 12 o 13 dígitos, según el año de emisión, los 4 primeros deben coincidir con la clave de la sección de la residencia del ciudadano, los restantes corresponden a un número consecutivo único asignado al momento de conformar la Clave de Elector correspondiente.

En virtud de lo anterior, se considera que dicho número de control, al contener el número de la sección electoral en donde vota el ciudadano titular de dicho documento, constituye un dato personal en razón de que devela información concerniente a una persona física identificada o identificable en función de la información geoelectoral ahí contenida.

Por consiguiente, dicha información se considera confidencial en virtud de tratarse de datos personales, toda vez que es información concerniente a una persona física identificada o identificable, por lo que resulta procedente su protección, tal como lo hizo valer el sujeto obligado.

Fotografía, ésta constituye la reproducción fiel de la imagen de una persona, objeto o cosa, obtenida en papel mediante la impresión en un rollo o placa por medio de una cámara fotográfica, o en formato digital, que constituye la reproducción de las imágenes captadas.

En concordancia con lo anterior, la fotografía constituye el primer elemento de la esfera personal de todo individuo, en tanto funge como un instrumento básico de identificación y proyección exterior, y es un factor imprescindible de reconocimiento como sujeto individual; por lo tanto, es un dato personal en términos de los artículos 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 116, de la Ley General de Transparencia y Acceso a la Información Pública sin importar de que se trate de la credencial de elector de un servidor público, dado que dicho documento no derivó de sus atribuciones como servidor público, por lo que es posible eliminar la fotografía de las credenciales de elector cuya reproducción aparezca en el expediente.

No obstante lo anterior, la fotografía no podrá testarse o eliminarse de la reproducción de las credenciales de elector, cuando esta corresponda a un servidor público o ex servidor público, toda vez que la reproducción gráfica del servidor público resulta idónea para que se tenga certeza de que la persona actuante corresponde a la que aparece en dicho medio de identificación.

Número de folio, de la credencial de elector, atento a lo que señala el "Acuerdo que aprueba el modelo de la credencial para votar", publicado en el Diario Oficial de la Federación el 10 de enero de 1991, se indica lo siguiente:

CONSIDERANDOS

[..]

3. *La política fundamental bajo la cual se desarrollaron las tareas para el diseño de la credencial para votar fue la consulta permanente con los representantes de los partidos políticos, mediante sesiones de trabajo para la obtención de criterios y recomendaciones.*

Estos coincidieron en que la credencial contara con una clave única de elector y con un número de folio que permitiera un estricto control de la misma y facilitara la rastreabilidad de la información para llegar al documento fuente.

[..]

7. Para llegar al modelo que se propone, la dirección ejecutiva del Registro Federal de Electores diseñó un proyecto que fue puesto a consideración y análisis de los partidos políticos quienes aportaron sus recomendaciones en la forma y contenido.

[...]

Descripción:

Anverso.

En esta cara de la credencial los datos se encuentran distribuidos en tres bloques horizontales: ...

El segundo bloque lo constituyen los datos personales del elector, clave de registro, número de folio y el logotipo del padrón electoral 1991.

[...]

El número de folio es el de la solicitud de inscripción al padrón que presentó el ciudadano, el cual se incluye en la credencial para permitir la auditabilidad de los servicios del Registro Federal de Electores.

[...]

8. La Dirección Ejecutiva del Registro Federal de Electores y la Comisión Nacional de Vigilancia, apoyados por sus respectivos cuadros técnicos, han realizado el mayor esfuerzo para plasmar un modelo de credencial para votar, que cumple con los requisitos jurídicos y de índole técnica consignados en el Código Federal de Instituciones y Procedimientos Electorales.

Cabe resaltar el pleno acuerdo sobre la totalidad de los elementos del modelo que se presenta como quedó plasmado en las reuniones del grupo de asesores técnicos de los partidos políticos el 23 de octubre de 1990 y de la Comisión Nacional de Vigilancia el 30 de noviembre del mismo año, en ellas se solicitó que la credencial para votar, cuente con un número de folio que permita un estricto control de la misma y facilite la rastreabilidad de la información para llegar al documento fuente, elemento que ha quedado integrado en el modelo que se presenta.

De lo anterior, se colige que el folio de la credencial de elector corresponde al número de la solicitud de inscripción al Padrón Electoral que presentó el ciudadano, el cual se incluye para permitir la auditabilidad de los servicios de tal Registro Federal de Electores. Asimismo, el número de folio permite un estricto control de la credencial de elector y facilita la rastreabilidad de la información para llegar al documento fuente.

De este modo, el número de folio de la credencial de elector no se genera a raíz de datos personales ni tampoco es reflejo de los mismos, pues en términos de lo dispuesto en el acuerdo citado, dicha cifra sólo sirve para tener un control de la credencial de elector y facilitar el rastreo en caso de búsqueda del documento fuente, es decir, a la solicitud del "Padrón del Registro Federal de Electores"

[Énfasis añadido]

"C. Nivel alto

Los sistemas de datos personales que contengan alguno de los datos que se enlistan a continuación, además de cumplir con las medidas de seguridad de nivel básico y medio, deberán observar las marcadas con nivel alto.

- **Datos Ideológicos:** ...
- **Datos de Salud:** ...
- **Características personales:** Tipo de sangre, ADN, huella digital, u otros análogos.

[Énfasis añadido]

En virtud de lo anterior, se considera que la huella digital es un dato personal susceptible de clasificarse como confidencial, en términos de lo dispuesto por los artículos 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 116, de la Ley General de Transparencia y Acceso a la Información Pública.

Clave de elector, ésta se compone de 18 caracteres, mismos que hacen identificable a una persona física, toda vez que se conforma por las primeras letras de los apellidos, año, mes, día, sexo, clave del estado en donde nació su titular, así como una homoclave interna de registro. Por tanto, al ser datos que constituyen información que hace identificable a una persona física, resulta procedente su clasificación atento a lo dispuesto por los artículos 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 116, de la Ley General de Transparencia y Acceso a la Información Pública.





Año de registro y vigencia, se considera que dichos datos son considerados datos personales con el carácter de confidencial, cuya difusión permite conocer el año en que un individuo se convirtió en elector y la fecha en que deja de tener validez su credencial.

Así las cosas, tal información es un dato personal de carácter confidencial que amerita sea clasificado, según lo dispuesto en el dispositivo legal apenas invocado.

Espacios necesarios para marcar el año y elección. Constituyen información personal, porque permite conocer cuando una determinada persona ejerció su derecho al voto, por lo que debe ser protegida mediante su clasificación como confidencial.

Estado, Municipio, localidad y sección, estos datos corresponden a la circunscripción territorial donde un ciudadano debe ejercer el voto, por lo que al estar referida a un aspecto personal del titular de dicho documento, se considera que actualiza la confidencialidad prevista en la Ley de la materia.

Firma, se trata de un dato personal confidencial en tanto que hace identificable al titular, por lo que reviste el carácter de confidencial; en términos de los artículos 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 116, de la Ley General de Transparencia y Acceso a la Información Pública, por lo que, si bien se trata de un servidor público, se hace evidente que la rúbrica contenida en la credencial para votar no la plasmó en el ejercicio de sus atribuciones como funcionario, por lo que es de protegerse dicho dato personal.

Ante esa circunstancia, los datos confidenciales anteriormente citados deberán ser protegidos y por ende testarse o eliminarse del documento que pudiera ponerse a disposición del peticionario, para evitar su acceso no autorizado, atento a lo previsto en los artículos 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 116, de la Ley General de Transparencia y Acceso a la Información Pública.

c) **Registro Federal de Contribuyentes (RFC)** otorgado por el Servicio de Administración Tributaria (SAT) al titular de ésta, vinculado al nombre de su propio titular, permite identificar, entre otros datos, la edad de la persona, así como su homoclave, siendo esta última única e irrepetible.

Al efecto, es de recordar que la clave del Registro Federal de Contribuyentes, se conforma en el caso de las personas físicas, que tiene derecho u obligación a declarar impuestos; en donde, por ejemplo de la clave VECJ880326 XXX, se desprende que:

VE es la primera letra del apellido paterno más la primera vocal interna del apellido paterno.

C es la inicial del apellido materno. De no existir un apellido materno se utiliza una (X).

J es la inicial del primer nombre.

88 son los dos últimos dígitos del año de nacimiento.

03 es el mes de nacimiento.

26 es el día de nacimiento. Por lo tanto, en este caso puede deducirse que la persona nació el veintiséis de marzo de 1988.

XXX es la homoclave, designada por el SAT a través de papel oficial ya designado, y depende de algunos factores que realiza el SAT por medio de un software alfanumérico.

Por tanto, se concluye que éste es un dato personal, toda vez que la clave de Registro Federal de Contribuyentes, al vincularse o relacionarse con el nombre de su titular, permite identificar, entre otros datos, la edad de la persona, en el caso, de proporcionar acceso a ésta, al conocerse su homoclave, siendo esta última única e irrepetible, se incrementa la posibilidad de identificar plenamente a su titular. En consecuencia procede su clasificación y por ende testar o eliminar del documento en términos de los artículos 113, fracción I, de la Ley



Federal de Transparencia y Acceso a la Información Pública, y 116 de la Ley General de Transparencia y Acceso a la Información Pública, de aplicación supletoria a la Ley Federal.

Al efecto, se deben tener presente el criterio 9/09, que sobre el particular estableció el Instituto Federal de Acceso a la Información y Protección de Datos, mismo que se reproduce para su pronta referencia:

Registro Federal de Contribuyentes (RFC) de las personas físicas es un dato personal confidencial. De conformidad con lo establecido en el artículo 18, fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental se considera información confidencial los datos personales que requieren el consentimiento de los individuos para su difusión, distribución o comercialización en los términos de esta Ley. Por su parte, según dispone el artículo 3, fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, dato personal es toda aquella información concerniente a una persona física identificada o identificable. Para obtener el RFC es necesario acreditar previamente mediante documentos oficiales (pasaporte, acta de nacimiento, etc.) la identidad de la persona, su fecha y lugar de nacimiento, entre otros. De acuerdo con la legislación tributaria, las personas físicas tramitan su inscripción en el Registro Federal de Contribuyentes con el único propósito de realizar mediante esa clave de identificación, operaciones o actividades de naturaleza tributaria. En este sentido, el artículo 79 del Código Fiscal de la Federación prevé que la utilización de una clave de registro no asignada por la autoridad constituye como una infracción en materia fiscal. De acuerdo con lo antes apuntado, el RFC vinculado al nombre de su titular, permite identificar la edad de la persona, así como su homoclave, siendo esta última única e irreplicable, por lo que es posible concluir que el RFC constituye un dato personal y, por tanto, información confidencial, de conformidad con lo previsto en el artículo 18, fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

d) **Pasaporte**, es un documento con validez internacional, que identifica a su titular (en ciertos países también a sus descendientes directos e incluso a sus cónyuges) expedido por las autoridades de su respectivo país, que acredita un permiso o autorización legal para que salga o ingrese del mismo, por los puertos o aeropuertos internacionales, siempre y cuando las autoridades de esos países lo autoricen, mediante el otorgamiento de un visado.

El pasaporte incluye información del portador relacionada a su nombre, nacionalidad, fecha de nacimiento, sexo, lugar de nacimiento, entre otros, información que en términos de lo expuestos se considera como confidencial en términos de lo dispuesto en los artículos 113, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública y 116 de la Ley General de Transparencia y Acceso a la Información Pública, de aplicación supletoria a la Ley Federal.



El número de pasaporte es un número distintivo y único que separa un pasaporte de cada otro que haya sido expedido, por lo que, se considera información confidencial, en términos de lo expuestos se considera como confidencial en términos de lo dispuesto en los artículos 113, fracción I de la Ley Federal

de Transparencia y Acceso a la Información Pública y 116 de la Ley General de Transparencia y Acceso a la Información Pública.

e) **Domicilio de particulares**, es de señalarse que el domicilio, al ser el lugar en donde reside habitualmente una persona física, tal y como se define por el artículo 29 del Código Civil Federal, constituye un dato personal y, por ende, confidencial, ya que su difusión podría afectar la esfera privada de la misma, en este sentido, las referencias al estado, municipio, localidad, sección, Delegación, código postal, que hagan identificada o identificable a una persona, corresponde al ámbito personal de un individuo.

En razón de lo anterior, es que conforme a lo dispuesto en los artículos 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 116, de la Ley General de Transparencia y Acceso a la Información Pública, se considera que se trata de un dato confidencial, mismo que no es factible hacerlo del carácter público, sin que previamente pudiese existir un consentimiento implícito para su divulgación.

f) **Número de teléfono, como lo es la telefonía fija y la celular**, se refiere al dato numérico asignado para la prestación del servicio de telefonía fija o celular asignado por empresa o compañía que lo proporciona, atento a una concesión del Estado, y que corresponde al uso en forma particular, personal y privada, con independencia de que éste se proporcione para un determinado fin o propósito a terceras personas, incluidas autoridades o prestadores de servicio.

Así el número de teléfono particular, tendrá el carácter de dato personal, cuando a través de éste sea posible identificar o hacer identificable al titular o usuario del mismo, cuando hubiere sido entregada a los sujetos obligados para un determinado propósito (principio de finalidad) o hubieren sido obtenidos en ejercicio de sus funciones.

Ante esa circunstancia debe protegerse y por ende testarse o eliminarse del documento que pudiera ponerse a disposición del peticionario, para evitar su acceso no autorizado, atento a lo previsto en los artículos 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública, y 116 de la Ley General de Transparencia y Acceso a la Información Pública, de aplicación supletoria a la Ley Federal.

g) **Cédula profesional**, en este documento se puede encontrar la Clave Única de Registro de Población y la firma del titular, datos que se consideran confidenciales en términos de los artículos 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública, y 116 de la Ley General de Transparencia y Acceso a la Información Pública, de aplicación supletoria a la Ley Federal.

No obstante, el número de cédula profesional es un dato de naturaleza pública, en virtud de que se trata de un número que autoriza el ejercicio de actividades profesionales, lo que implica a su vez, que los profesionistas deben exhibir la cédula profesional y el número de registro de la misma al momento de prestar sus servicios.

Inclusive, en el criterio 02-10 emitido por el Pleno del Instituto Federal de Acceso a la Información y Protección de Datos, se establece que la cédula profesional de servidores públicos es un documento susceptible de versión pública, tomando en consideración que es un documento que tiene como objeto acreditar que una persona cuenta con la autorización para ejercer la profesión indicada en la misma; a través del conocimiento de algunos de los datos ahí contenidos se puede corroborar la idoneidad del servidor público para ocupar el empleo, cargo o comisión encomendada.

Además, el número de cédula profesional puede ser consultado en el Registro Nacional de Profesionistas que se localiza en la página electrónica de la Secretaría de Educación Pública y en su equivalente en las entidades federativas de la República Mexicana, es decir, este dato se localiza en un registro público.

Derivado de lo anterior, el dato relativo al número de cédula profesional no puede ser considerado un dato personal, de conformidad con lo dispuesto en el artículo 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública.

h) En cuanto a la información confidencial contenida en los anexos técnicos y económicos de los contratos que obran en el archivo de la Unidad de Gobierno Digital y de la Dirección General de Recursos Materiales y Servicios Generales (propuesta de solución, dimensionamiento de la infraestructura, servicio de pruebas de estrés para el aplicativo DeclaraNet plus y la relacionada con aplicación de evaluaciones es de señalar que el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales en el proyecto de resolución al RDA 2533/16, expuso que el secreto comercial es la información que encuadra en lo señalado por la Organización Mundial de la Propiedad Intelectual (OMPI), de la cual México forma parte por medio del *Tratado de la OMPI sobre Derecho de Autor*, del 20 de diciembre de 1996, en la que se considera que el secreto comercial refiere a "*toda aquella información comercial confidencial que confiera a una empresa una ventaja competitiva*".

En este mismo sentido, el secreto comercial es la información restringida en la comercialización, distribución y venta de los productos industriales o servicios a través de usos sistematizados de medios de difusión y comunicación, además de técnicas, estadísticas, de encuesta y de mercadeo que le signifique a la empresa mantener una ventaja competitiva respecto a otras, se relaciona con el sector puramente comercial de la empresa, y sólo tiene lugar cuando concurre el interés de mantener la información en secreto, es decir no es de conocimiento público.

El secreto comercial se relaciona con el sector puramente comercial de la empresa; tales como la lista de clientes, lista de proveedores, cálculos de precios, la creación de sistemas de ventas, la creación de campañas de publicidad, las condiciones de pago, los precios especiales que los proveedores hacen a una empresa, los documentos de cálculo, los informes del viajante de una empresa.

Adicional a lo anterior, el artículo 39 del "Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio", establece como requisitos del secreto comercial, los siguientes:

- La información debe ser secreta (en el sentido de que no sea generalmente conocida ni fácilmente accesible para personas introducidas en los círculos en que normalmente se utiliza el tipo de información en cuestión).
- Debe tener un valor comercial por ser secreta.
- Debe haber sido objeto de medidas razonables para mantenerla secreta.

En este sentido, el secreto comercial contempla información que le permite a su titular obtener o mantener una ventaja competitiva o económica frente a terceros en la realización de actividades económicas.

Ahora bien, a fin de acreditar los supuestos señalados, la Unidad de Gobierno Digital indica que el anexo técnico y económico (propuesta técnico-económica) presentada por el prestador de servicios, se relaciona con lo siguiente:



- a. Los anexos técnicos y económicos contienen información de carácter confidencial, ya que no son generalmente conocidos ni fácilmente accesibles para personas introducidas en los círculos en que normalmente se utiliza el tipo de información en cuestión; y
- b. Los anexos técnicos y económicos contienen información que reviste el carácter de comercial, en tanto que por los beneficios que ofreció el proveedor, es estimó que se contratara con éste.
- c. La información confidencial contenida en los anexos técnicos y económicos ha sido objeto de medidas razonables, para mantener en sigilo la información confidencial, tomadas por la persona que legítimamente la controla; ya que es resguardada por la Dirección General Adjunta de Proyectos de Gobierno Digital de la Unidad de Gobierno Digital, adoptando las medidas pertinentes.

La información no es del dominio público ni resulta evidente para un técnico o perito en la materia, con base en la información previamente disponible o la que deba ser divulgada por disposición legal o por orden judicial, ya que no fue publicada en el sistema electrónico denominado Compranet, ni se conoce por algún otro medio, máxime cuando dicha información representa la ventaja competitiva y comercial que el proveedor ofrece a esta dependencia.

En términos de los razonamientos expuestos, y toda vez que quedaron acreditados los supuestos que constituyen que los anexos técnicos y económicos de los contratos que obran en el archivo de la Unidad de Gobierno Digital revisten el carácter de confidencial al configurarse la hipótesis del secreto comercial, toda vez que no es pública y representa una ventaja comercial para los proveedores, en consecuencia procede su clasificación y por ende, en la información que se entregue al particular esta parte de la información deberá ser testada o eliminada, en términos de los artículos 113, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública, y 116, de la Ley General de Transparencia y Acceso a la Información Pública, de aplicación supletoria a la Ley Federal.

En virtud de lo anterior, con fundamento en lo dispuesto por los artículos 140, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública, y 137, inciso a), de la Ley General de Transparencia y Acceso a la Información Pública, de aplicación supletoria, este Comité de Transparencia modifica la clasificación de datos confidenciales comunicada por la Dirección de Administración y Finanzas del Instituto de Administración y Avalúos de Bienes Nacionales, la Dirección General de Recursos Materiales y Servicios Generales, y la Unidad de Gobierno Digital, en los términos señalados en la presente resolución, asimismo, de conformidad con lo señalado en el diverso 113, último párrafo de la Ley Federal de Transparencia y Acceso a la Información Pública, es de señalarse que la citada clasificación e impedimento para acceder a ella, no está sujeta a temporalidad alguna y sólo podrá tener acceso a ella los titulares de la misma, o sus representantes legales.

Cabe señalar que para dar acceso a la información requerida, si bien el peticionario del folio que nos ocupa solicitó la entrega de la información por internet en la PNT, esto es, a través de la Plataforma Nacional de Transparencia, de conformidad con el artículo 136 de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 133, de la Ley General de Transparencia y Acceso a la Información Pública, de aplicación supletoria, la información requerida no puede entregarse ni enviarse en dicha modalidad, toda vez que para que ello ocurriera, la unidad administrativa responsable de contar con la información, debe disponer de una versión electrónica de la misma, circunstancia que acreditó no poseer, en tanto que la misma obra de forma impresa en su archivo.

No se omite señalar que considerando lo previsto en el Quincuagésimo Noveno de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como la elaboración de versiones públicas, publicados en el Diario Oficial de la Federación el 15 de abril de 2016, al tratarse de información que obra impresa en el archivo de la unidad administrativa, para elaborar la versión pública deberá fotocopiar y sobre ésta testar las palabras, párrafos o renglones clasificados, por lo que, tampoco es posible poner a disposición del peticionario la información en consulta directa, toda vez que por el formato en que se encuentra el expediente solicitado, no sería posible implementar las medidas necesarias a fin de que los servidores públicos garanticen el resguardo de la información confidencial.

Consecuentemente, atento a lo previsto en los citados numerales, se pone a disposición del particular la versión pública de la información solicitada, en copia simple o certificada constante de un total 8,966 fojas útiles, previa constancia de haber realizado el pago del costo de su reproducción o de los derechos respectivos. La versión pública será elaborada por cada una de las unidades administrativas responsables de contar con la información, en este caso, la Dirección General de Administración y Finanzas del Instituto de Administración y Avalúos de Bienes Nacionales, la Dirección General de Recursos Materiales y Servicios Generales y la Unidad de Gobierno Digital, las cuales contarán con un plazo de hasta 6 días hábiles contados a partir de la fecha en que se le comunique el pago señalado, para acudir ante la Unidad de Transparencia con el original de las constancias y la versión pública, para su cotejo, amén de verificar la protección de la información confidencial señalada. El solicitante podrá recabar la información en la Unidad de Transparencia de esta Secretaría previa cita que realice en el domicilio ubicado en Avenida Insurgentes Sur No. 1735, Col. Guadalupe Inn, C.P. 01020, Delegación Álvaro Obregón, Ciudad de México, al teléfono 2000-3000, extensión 2136, o bien, recibir por correo certificado, si al efecto cubre el costo del envío, según lo dispuesto por los artículos 137, 138 y 145, de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con los diversos 133, 134 y 141 de la Ley General de Transparencia y Acceso a la Información Pública.

De lo anterior, resulta inconcuso que esta dependencia cumple con la obligación de dar acceso a la información solicitada en la forma en que ésta lo permite, no obstante, los costos de reproducción y envío sólo obedecen a los derechos, aprovechamientos o productos que deben ser cobrados, conforme a lo indicado, máxime cuando la información solicitada rebasa en número al de 20 fojas señalado en el 145, de la Ley Federal de Transparencia y Acceso a la Información Pública, por lo que no es posible exceptuar el pago de reproducción y envío.

TERCERO.- Finalmente, la Dirección General de Tecnologías de Información señala la reserva del contrato DC-107-2013, y su Convenio modificatorio DC-CM-005-2014, conforme a lo señalado en el Resultando V, de esta resolución.

Lo anterior en virtud que el contrato DC-107-2013 – DC-CM-005-2014, denominado "Contrato plurianual de adquisición de bienes y prestación de servicios para el establecimiento y puesta en marcha de un nuevo centro de datos de alta disponibilidad para la Secretaría de la Función Pública y su Convenio Modificatorio", de conformidad con los artículos 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, de aplicación supletoria a la Ley Federal, en relación con artículo 211 Bis del Código Penal Federal está reservado.

Al efecto, es de señalar que la información contenida en el Anexo Uno "Especificaciones técnicas y alcances del Servicio y sus Anexos A y B" y Anexo Dos consistente en la Propuesta Técnica y Económica del "Proveedor", así como los cuatro anexos del convenio modificatorio, contienen la descripción de los componentes y mecanismos tecnológicos, así como su ubicación, mediante los cuales se realiza la publicación y operación de los sistemas de información catalogados como críticos, debido



a que su correcto funcionamiento contribuye de manera directa al cumplimiento de los objetivos de la Secretaría y al ejercicio de diversas funciones de las dependencias y entidades de la Administración Pública Federal, por lo que con el propósito de garantizar la confidencialidad de los mecanismos, configuraciones, procedimientos y demás recursos de seguridad de las instalaciones de tecnologías de la información y comunicaciones que resguardan la información a través de los cuales esta Secretaría cumple sus metas fiscalizadoras y de rendición de cuentas.

En este contexto, la unidad administrativa señaló que el centro de datos de alta disponibilidad provisto a través de este contrato, fue concebido, equipado y aprovisionado previendo las mejores condiciones operativas posibles para la seguridad de la información con la que operan los sistemas de información críticos, y el cual dispone de elementos de hardware y software, dispuestos tecnológicamente para garantizar en la mayor medida posible que la información este accesible a las personas afines a ella, a través de los medios que la Secretaría a través de sus unidades administrativas han establecido, acorde a la normatividad vigente.

Adicionalmente, el objetivo del proceso de Administración de la Seguridad de la Información previsto en el Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones, y en la de seguridad de la información, consiste en evaluar, diseñar, establecer y vigilar los mecanismos que permitan la administración de la seguridad de la información de la Secretaría, así como disminuir el impacto de eventos adversos que potencialmente puedan afectar el logro de los objetivos institucionales, por lo que de no reservar la información respecto de la descripción de los componentes, mecanismos y el entorno tecnológico mediante los cuales se proporcionó el establecimiento y puesta en marcha de un nuevo centro de datos de alta disponibilidad, permitiría el análisis de potenciales vulnerabilidades a la infraestructura, la información y los procesos que lo sustentan, lo que potencializa la comisión de conductas que son tipificadas por el Código Penal Federal como delitos.

Asimismo, la Dirección General de Tecnologías de Información señaló que las instalaciones de tecnologías de información y comunicaciones de la Secretaría, como son los equipos de seguridad perimetral, la red de comunicaciones, los elementos de seguridad física y protección a contingencias, consistente en equipos especializados instalados, configurados y operados desde el centro de datos de alta disponibilidad, que son indispensables para la provisión de los servicios públicos que presta y cuya intromisión, modificación, pérdida, destrucción o inhabilitación de forma temporal o definitiva, materializa una amenaza en contra de la información y los sistemas o equipos de informática de la Secretaría de la Función Pública, por lo que aún y cuando los servicios del contrato DC-107-2013, y su Convenio modificatorio DC-CM-005-2014, concluyeron su vigencia, es necesario reservar la información relacionada con la arquitectura tecnológica y el entorno de operación de los elementos operativos del centro de datos de alta disponibilidad que fueron provistos como parte de tales instrumentos.

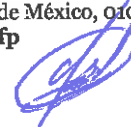
Por otra parte, en cuanto al contrato DC-087-2014 y los anexos uno y dos contiene la descripción de elementos técnicos, así como su ubicación, mediante los cuales se brinda el soporte a la publicación y operación de los sistemas de información catalogados como críticos, debido a que su correcto funcionamiento contribuye de manera directa al cumplimiento de los objetivos de la Secretaría, así como al ejercicio de diversas funciones de las dependencias y entidades de la Administración Pública Federal, por lo que con el propósito de la reserva de las condiciones operativas de tales infraestructuras

de soporte que mantienen la disponibilidad de la información a través de los cuales la Secretaría cumple sus metas fiscalizadoras y de rendición de cuentas se actualiza el supuesto de reserva señalado.

En efecto, las instalaciones que soportan la operación de la infraestructura de tecnologías de información y comunicaciones de la Secretaría, como son los centros de datos, y en específico el de alta disponibilidad, se considera como una infraestructura crítica y estratégica, al resultar indispensables para la provisión de los servicios públicos que presta y cuya intromisión, modificación, pérdida, destrucción o inhabilitación de forma temporal o definitiva, materializa una amenaza en contra de la información y los sistemas o equipos de informática de la Secretaría de la Función Pública, por lo que aún y cuando los bienes y servicios del contrato DC-087-2014, Contrato para la adquisición de transformador de pedestal tipo trifásico TR-1 de 500 KVA para el centro de datos de la Secretaría de la Función Pública, concluyeron su vigencia, es necesario reservar la información relacionada con el entorno de operación de los elementos que sustentan el correcto funcionamiento del centro de datos de alta disponibilidad que fueron provistos.

Con la exposición anterior, es de señalar que en términos del Vigésimo Sexto, primer párrafo, y Trigésimo Tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, se debe señalar que la información está reservada en virtud de que ponerla a disposición difundiría la ubicación, agentes de riesgo potenciales, existentes y explotables, y en general las condiciones actuales de operación de los equipos del centro de datos y sistemas institucionales, poniendo en riesgo las previsiones y mecanismos que el conjunto de infraestructuras dispuestas alrededor del centro de datos proporciona para preservar la confidencialidad, integridad y disponibilidad de la información, y que al exponerlos a un acceso no autorizado o a un ataque intencionado y dirigido podría derivar en la obtención o la alteración o la pérdida de información sensible para la operación de la Secretaría de la Función Pública y en general de la Administración Pública Federal, como podría ser el caso de un acceso no autorizado a bases de datos con información confidencial de personas identificadas o identificables, impactando en el cumplimiento de las atribuciones de la SFP, el deterioro de la imagen de la Secretaría y el debilitamiento de las instituciones ante la ciudadanía, que al ser sujetos de un análisis dirigido, se podrían explotar posibles vulnerabilidades actuales sobre la operación de los procesos críticos de las tecnologías de información y comunicaciones de la red, equipos y sistemas institucionales aún existentes, pudiendo evadir con ello las previsiones y mecanismos que este servicio proporciona para preservar la confidencialidad, integridad y disponibilidad de la información de la Secretaría, orientados a impedir el acceso ilícito a sistemas y equipos de informática.

El riesgo real, identificable y demostrable que ocasionaría la difusión de esta información, se traduce en hacer del conocimiento general elementos del entorno tecnológico que ha utilizado la Secretaría, lo que impediría prevenir cualquier situación de riesgo que derive de cualquier posible explotación a las vulnerabilidades expuestas con el conocimiento de configuraciones, capacidades y arquitecturas de las tecnologías que conforman el centro de datos de alta disponibilidad, destinando recursos públicos para un fin al que no están afectos, debido a la necesidad de redefinir o establecer nuevas configuraciones de equipos y planes de servicios, así como nuevos diseños y desarrollos de tecnologías de información, al quedar materialmente vulnerados los vigentes, en perjuicio del logro de los objetivos institucionales y el ejercicio de atribuciones legales.





Asimismo, esta información podría ser utilizada para perpetrar ataques intencionados mediante la explotación de vulnerabilidades conocidas en las tecnologías y mecanismos de operación existentes, así como el entorno de operación actual, exponiendo con ello la información de carácter personal, relativa a procedimientos de fiscalización, de control del ejercicio público y de obligaciones de transparencia, al robo, alteración y el mal uso, impactando el cumplimiento de las metas de la Secretaría, lo que potencialmente puede afectar el logro de los objetivos institucionales o podrían configurar inclusive, como ha sido expuesto la comisión de conductas sancionadas por el Código Penal Federal como delitos.

En este contexto, para demostrar que el riesgo de perjuicio que supone divulgar la información supera el interés público, es de señalar que en términos de lo dispuesto en el artículo 211 bis 2 del Código Penal Federal está tipificado como delito a quien "... sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad..." por lo que, resulta inconcuso que difundir el contrato que nos ocupa y su convenio modificatorio pondría en riesgo las previsiones y mecanismos que el conjunto de infraestructuras dispuestas alrededor del centro de datos proporciona para preservar la confidencialidad, integridad y disponibilidad de la información.

Finalmente, la reserva de la información se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar perjuicio al interés público para que este sujeto obligado cumpla con las obligaciones a su cargo, consistente en las características especiales y específicas del Centro de datos de alta disponibilidad con el que opera la Secretaría, la ubicación, los agentes de riesgo existentes y explotables, y en general las condiciones actuales de operación de los equipos del centro de datos y sistemas institucionales, su configuración, arquitectura, así como la información que detenta, debe permanecer reservada por un plazo de 5 años.

Siguiendo este orden de ideas, con fundamento en lo dispuesto en los artículos 140, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública, y 137, inciso a) de la Ley General de Transparencia y Acceso a la Información Pública, de aplicación supletoria, este Comité de Transparencia confirma la reserva del contrato DC-107-2013, y su Convenio modificatorio DC-CM-005-2014, así como del contrato DC-087-2014 y sus anexos, comunicada por la Dirección General de Tecnologías de la Información, por un plazo de 5 años en los términos señalados en la presente resolución.

No se omite señalar que de conformidad con lo dispuesto en los artículos 99 de la Ley Federal de Transparencia y Acceso a la Información Pública, y 101 de la Ley General de Transparencia y Acceso a la Información Pública, la clasificación de la información señalada será desclasificada y por tanto pública, cuando se extingan las causas que le dieron origen a la clasificación, o fenezca el plazo de reserva, lo que ocurra primero.

Por lo expuesto y fundado, es de resolver y se

RESUELVE

PRIMERO.- Se modifica la clasificación de datos confidenciales comunicados por la Dirección General de Administración y Finanzas del Instituto de Administración y Avalúos de Bienes Nacionales, la Dirección General de Recursos Materiales y Servicios Generales, y la Unidad de Gobierno Digital, por lo que se pone a disposición del peticionario versión pública de una parte de la información solicitada, en la forma y términos señalados en el Considerando Segundo de esta determinación.



SEGUNDO.- Por otro lado, se confirma la reserva del contrato DC-107-2013, y su Convenio modificatorio DC-CM-005-2014, comunicada por la Dirección General de Tecnologías de Información, en la forma y términos señalados en el Considerando Tercero de esta resolución.

TERCERO.- El solicitante podrá interponer por sí o a través de su representante, el recurso de revisión previsto por los artículos 147, de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 142, de la Ley General de Transparencia y Acceso a la Información Pública, ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, sito en Av. Insurgentes Sur No. 3211, Col. Insurgentes Cuicuilco; Delegación Coyoacán, en esta Ciudad de México, o ante la Unidad de Transparencia de la Secretaría de la Función Pública.

Debe referirse que ese órgano garante ha puesto a disposición de los solicitantes de acceso a la información el Sistema de Gestión de Medios de Impugnación, inserto en la denominada Plataforma Nacional de Transparencia disponible en la dirección <http://www.plataformadetransparencia.org.mx/>, en donde podrá presentar el señalado recurso de revisión.

CUARTO.- Notifíquese por conducto de la Unidad de Transparencia de esta Secretaría de la Función Pública al solicitante, así como a las unidades administrativas responsables señaladas en esta resolución.

Así, por unanimidad de votos lo acordaron los integrantes del Comité de Transparencia de la Secretaría de la Función Pública, Claudia Sánchez Ramos, Coordinadora del Centro de Información y Documentación y Responsable del Área Coordinadora de Archivos; Alejandro Durán Zárate, Director General Adjunto de Procedimientos y Servicios Legales y Titular de la Unidad de Transparencia, y Roberto Carlos Corral Veale, Director General Adjunto de Control y Evaluación, como suplente del Contralor Interno y Miembro de este Comité, de acuerdo con los oficios de designación correspondientes.



Claudia Sánchez Ramos



Alejandro Durán Zárate



Roberto Carlos Corral Veale

Elaboró: Lic. Ivonne Guerra Basulto



Revisó: Lic. Lilliana Olvera Cruz