

SFP

SECRETARÍA DE
LA FUNCIÓN PÚBLICA



COMITE DE TRANSPARENCIA

Folio: 0002700157416

Ciudad de México, a veinticuatro de agosto de dos mil dieciséis.

VISTO: El estado que guarda el procedimiento de acceso a la información, derivado de la solicitud presentada el 30 de junio de 2016, a través de la PNT, Plataforma Nacional de Transparencia, a la que corresponde el número de folio 0002700157416, 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

"Solicito copia del documento firmado y anexo técnico del contrato DC-027-2014 " SERVICIO INTEGRAL DE SEGURIDAD INFORMÁTICA " firmado entre la Secretaria de la Función Pública y la empresa MAINBIT, S.A. DE C.V." (sic)

Otros datos para facilitar su localización

"el contrato se firmó el 28 de enero de 2014" (sic)

II.- Que a través de la resolución de 11 de agosto 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. UGD/DGAENGD/DPIGD/409/1343/2016 de 7 de julio de 2016, la Dirección de Promoción e Integración de Gobierno Digital informó a este Comité que, de conformidad con el artículo 18 del Reglamento Interior de la Secretaría de la Función Pública, no cuenta con atribuciones para el resguardo de los contratos ni de sus anexos que firma la Secretaria de la Función Pública con los diversos proveedores.

IV.- Que a través de oficio No. UPCP/308/317/2016 de 13 de julio de 2016, la Unidad de Política de Contrataciones Públicas comunicó a este Comité, que después de la búsqueda exhaustiva en los expedientes documentales relacionados con la promoción de contrataciones consolidadas y de celebración de contratos que están a cargo de la Dirección General Adjunta de Política de Contrataciones Públicas, así como los relacionados con el seguimiento de las contrataciones públicas a cargo de dicha Dirección General Adjunta y de la Dirección General Adjunta de Contrataciones Electrónicas, que obran en su archivo de trámite, no localizó lo solicitado, por lo que, con fundamento en lo dispuesto en los artículos 141 de la Ley Federal de Transparencia y Acceso a la Información Pública, y 138 de la Ley General de Transparencia y Acceso a la Información Pública, la información es inexistente.

V.- Que mediante oficio No. 511/DGTI/0659/2016 y comunicado electrónico de 15 de julio y 10 de agosto de 2016, la Dirección General de Tecnologías de la Información manifestó a este Comité, que pone a disposición del particular la versión pública del instrumento DC-027-2014 "SERVICIO INTEGRAL DE SEGURIDAD INFORMÁTICA", cuyo anexo técnico se encuentra incorporado a la convocatoria de la Licitación Pública Mixta Nacional No. LA-027000002-N442-0213 que se identifica como Anexo Uno de acuerdo con la Cláusula Segunda del mismo, constante de 138 fojas útiles.



Por otro lado, la unidad administrativa señaló que el Anexo Dos "propuesta de "EL PROVEEDOR" contiene información reservada, que encuadra en el supuesto de reserva previsto en la fracción VII, del artículo 113, de la Ley General de Transparencia y Acceso a la Información Pública y fracción VII, del artículo 110, de la Ley Federal de Transparencia y Acceso a la Información Pública, en concordancia con el Vigésimo Sexto, párrafo primero, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

En ese contexto, la Dirección General citada manifestó que de acuerdo con lo dispuesto por los artículos 103, segundo párrafo y 104, fracción I, de la Ley General de Transparencia y Acceso a la Información Pública, 97, párrafo cuarto, 99, párrafo segundo, 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, solicitó la reserva de la información por un período de cinco años, para lo cual señaló como prueba de daño en la que se motiva su reserva lo siguiente:

La información contenida en el Anexo Dos propuesta de "EL PROVEEDOR" del contrato No. DC-027-2014, correspondiente al Servicio Integral de Seguridad Informática, que se identifica como Anexo 1 de la Convocatoria a la Licitación Pública Mixta Nacional No. LA-027000002-N442-2013 "PROPUESTA TÉCNICA" Descripción de las características técnicas de los servicios ofertados por MAINBIT S.A. de C.V.", contienen información respecto a la descripción de los componentes, mecanismos y el entorno tecnológicos mediante los cuales se proporcionó el servicio Integral de Seguridad Informática, con el propósito de garantizar la confidencialidad de los mecanismos, procedimientos, arquitecturas tecnológicas y demás recursos de seguridad de las instalaciones de tecnologías de información, así como de las comunicaciones que resguardaron en su momento, ya que es a través de éstos que la Secretaría cumple sus metas fiscalizadoras y de rendición de cuentas, además de obstruir la prevención de delitos o ilícitos a sistemas y equipos de informática de la Secretaría de la Función Pública, por lo que dichas especificaciones deberán continuar reservados con fundamento en lo dispuesto por el artículo 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública y 113, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública en relación con el artículo 211 Bis 2, del Código Penal Federal.

En esa tesitura, la Dirección General indicó que actualmente la Secretaría resguarda la seguridad de las instalaciones de tecnologías de información y comunicaciones, a través de una arquitectura con funciones equivalentes a las que en su momento se prestó a través del contrato DC-027-2014 "SERVICIO INTEGRAL DE SEGURIDAD INFORMÁTICA", por lo que dar a conocer 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 red de la dependencia, lo cual sustenta la reserva que presenta, ya que se pretende prevenir y evitar la intromisión, modificación, pérdida o destrucción de información contenida en sistemas o equipos de informática protegidos por los mecanismos de seguridad de los equipos a cargo de la Secretaría de la Función Pública que forma parte de uno de los poderes del Estado.

Adicionalmente, la unidad administrativa manifestó que 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 dar a conocer la información relativa a la descripción de los componentes, mecanismos y el entorno tecnológico mediante los cuales proporcionó el servicio Integral de Seguridad Informática, permitiría el análisis de potenciales vulnerabilidades de la red



institucional y potencializa la comisión de conductas que son tipificadas por el Código Penal Federal como delitos.

Abundo, en que las instalaciones de tecnologías de esta dependencia, como son la red institucional, consistente en sistemas de comunicaciones y de seguridad de la información, 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 protegidos por los mecanismos de seguridad de la Secretaría de la Función Pública, por lo que aún y cuando los servicios del contrato DC-027-2014 "SERVICIO INTEGRAL DE SEGURIDAD INFORMÁTICA" concluyeron, es necesario reservar la información relacionada con la arquitectura tecnológica y el entorno de operación de los mecanismos de seguridad mediante los cuales prestó el servicio.

El riesgo real, identificable y demostrable que ocasionaría la difusión de esta información, se traduce en hacer del conocimiento general elementos del entorno tecnológico actual de la Secretaría, que al ser sujetos de un análisis dirigido, se podrían explotar posibles vulnerabilidades sobre la operación de los procesos críticos de las tecnologías de información y comunicaciones de la red, equipos y sistemas institucionales aun 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, impactando en el cumplimiento de las atribuciones de esta Dependencia.

Además, hacer pública la información implicaría la necesidad inmediata de establecer medidas contingentes para prevenir cualquier situación de riesgo, 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. Lo anterior, ya que como ha sido señalado hacer público el conocimiento del entorno tecnológico en donde se prestó el servicio, potencializa la vulnerabilidad a que están expuestas las instalaciones de tecnologías de información de la Secretaría, inclusive, ante la probabilidad de conductas tipificadas por la Legislación Penal Federal como delitos.

Finalmente, el riesgo se materializaría toda vez que la información del entorno tecnológico con el que se presta a la fecha el servicio de seguridad de la información, en estricto sentido, contiene antecedentes que podrían ser vulnerados, como es el caso de perfiles de uso, mecanismos de frontera de red, especificaciones del monitoreo y acciones de reacción, todos destinados a prevenir y disminuir el impacto de eventos adversos que potencialmente pueden afectar el logro de los objetivos institucionales o constituir una amenaza a la seguridad nacional, y que de darse a conocer, podrían configurar inclusive como lo ha expuesto, la comisión de conductas sancionadas por el Código Penal Federal como delitos.

Adicionalmente, la unidad administrativa señaló que las características especiales y específicas del equipo de propiedad de la empresa Mainbit con el que en su momento prestó el servicio integral de seguridad informática, se refiere a información de carácter patrimonial que es necesario que se reserve, ya que dicha empresa no ha otorgado autorización para que la misma se haga pública.

VI.- Que mediante oficio No. 514/DGRMSG/527/2016 de 05 de agosto de 2016, la Dirección General de Recursos Materiales y Servicios Generales comunicó a este Comité que pone a disposición del peticionario versión pública del contrato DC-027-2014 y su Anexo Uno, en el que omitirá los datos

confidenciales consistentes en el número de cuenta y cuenta CLABE, de conformidad con lo dispuesto en el artículo 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública.

Por otro lado, la unidad administrativa manifestó que por lo que refiere a la propuesta técnica, contenida en el Anexo Dos del contrato, no se encuentra en posibilidad de ponerlo a disposición en razón de que el mismo contiene información reservada de conformidad con lo establecido en el artículo 113, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública, así como en lo ordenado por el artículo 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública.

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, 110, fracción VI, 113, fracción I, 140 y 143 de la Ley Federal de Transparencia y Acceso a la Información Pública; 43, 44, fracciones II y III, 111, 116, y 137 de la Ley General de Transparencia y Acceso a la Información Pública; y 6, fracción II, del Reglamento del Comité de Información 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 General de Tecnologías de la Información y la Dirección General de Recursos Materiales y Servicios Generales, ponen a disposición la versión pública de la información, conforme a lo señalado en los Resultandos V y VI, de esta resolución.

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 General de Recursos Materiales y Servicios Generales, 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 General de Recursos Materiales y Servicios Generales, y en consecuencia resulta necesario proteger, al tenor de lo siguiente:

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.

Por otro lado, la Dirección General de Tecnologías de la Información y la Dirección General de Recursos Materiales y Servicios Generales, comunican la imposibilidad de proporcionar copia del Anexo Dos "propuesta de "EL PROVEEDOR", en razón de que contienen información respecto a la descripción de los componentes, mecanismos y el entorno tecnológicos mediante los cuales se proporcionó el servicio Integral de Seguridad Informática, con el propósito de garantizar la confidencialidad de los mecanismos, procedimientos, arquitecturas tecnológicas y demás recursos de seguridad de las instalaciones de tecnologías de información, así como de las comunicaciones que resguardaron en su momento, ya que es a través de éstos que la Secretaría cumple sus metas fiscalizadoras y de rendición de cuentas, además de obstruir la prevención de delitos o ilícitos a sistemas y equipos de informática de la Secretaría de la Función Pública, por lo que se encuentran clasificadas como reservadas, conforme a lo indicado en el resultando V, párrafos segundo a décimo primero, de este fallo, por el plazo de 5 años, de conformidad con el artículo 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública y 113, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública en relación con el artículo 211 Bis 2, del Código Penal Federal.

En ese sentido, a fin de acreditar cada uno de los elementos previstos en el artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, en relación con los Vigésimo Sexto, párrafo primero y Trigésimo Tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas (en adelante Lineamientos Generales), que prevén que para considerar como reservada la información se deberá señalar:

De la Ley General de Transparencia y Acceso a la Información Pública

Artículo 104. En la aplicación de la prueba de daño, el sujeto obligado deberá justificar que:

- I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional;
- II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda, y
- III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio.

De los Lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas

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.

...

...

Trigésimo tercero. Para la aplicación de la prueba de daño a la que hace referencia el artículo 104 de la Ley General, los sujetos obligados atenderán lo siguiente:

- I. Se deberá citar la fracción y, en su caso, la causal aplicable del artículo 113 de la Ley General, vinculándola con el Lineamiento específico del presente ordenamiento y, cuando corresponda, el supuesto normativo que expresamente le otorga el carácter de información reservada;
- II. Mediante la ponderación de los intereses en conflicto, los sujetos obligados deberán demostrar que la publicidad de la información solicitada generaría un riesgo de perjuicio y por lo tanto, tendrán que acreditar que este último rebasa el interés público protegido por la reserva;
- III. Se debe de acreditar el vínculo entre la difusión de la información y la afectación del interés jurídico tutelado de que se trate;
- IV. Precisar las razones objetivas por las que la apertura de la información generaría una afectación, a través de los elementos de un riesgo real, demostrable e identificable;
- V. En la motivación de la clasificación, el sujeto obligado deberá acreditar las circunstancias de modo, tiempo y lugar del daño, y
- VI. Deberán elegir la opción de excepción al acceso a la información que menos lo restrinja, la cual será adecuada y proporcional para la protección del interés público, y deberá interferir lo menos posible en el ejercicio efectivo del derecho de acceso a la información.

A fin de acreditar los requisitos previstos en el Vigésimo Sexto, párrafo primero de los Lineamientos Generales para determinar la reserva del el Anexo Dos "propuesta de "EL PROVEEDOR", del contrato No. DC-027-2014, correspondiente al Servicio Integral de Seguridad Informática, que se identifica como Anexo 1 de la Convocatoria a la Licitación Pública Mixta Nacional No. LA-027000002-N442-2013 "PROPUESTA TÉCNICA" Descripción de las características técnicas de los servicios ofertados por MAINBIT S.A. de C.V.", contienen información respecto a la descripción de los componentes, mecanismos y el entorno tecnológicos mediante los cuales se proporcionó el servicio Integral de Seguridad Informática, con el propósito de garantizar la confidencialidad de los mecanismos, procedimientos, arquitecturas tecnológicas y demás recursos de seguridad de las instalaciones de tecnologías de información, así como de las comunicaciones que resguardaron en su momento, ya que es a través de éstos que la Secretaría cumple sus metas fiscalizadoras y de rendición de cuentas, además de obstruir la prevención de delitos o ilícitos a sistemas y equipos de informática de la Secretaría de la Función Pública, se actualiza el Vigésimo Sexto, párrafo primero del multicitado lineamiento.

Por otro lado a fin de acreditar los supuestos previstos en el Trigésimo Tercero de los Lineamientos Generales, la fracción y causal aplicable a la reserva de los hechos denunciados que originaron las investigaciones, éstos supuestos son el artículo 113, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública, y el 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación Vigésimo Sexto de los Lineamientos Generales.

La información contenida en el Anexo Dos propuesta de "EL PROVEEDOR" del contrato No. DC-027-2014, correspondiente al Servicio Integral de Seguridad Informática, que se identifica como Anexo 1 de la Convocatoria a la Licitación Pública Mixta Nacional No. LA-027000002-N442-2013 "PROPUESTA TÉCNICA" Descripción de las características técnicas de los servicios ofertados por MAINBIT S.A. de C.V.", contienen información respecto a la descripción de los componentes, mecanismos y el entorno tecnológicos

mediante los cuales se proporcionó el servicio Integral de Seguridad Informática, con el propósito de garantizar la confidencialidad de los mecanismos, procedimientos, arquitecturas tecnológicas y demás recursos de seguridad de las instalaciones de tecnologías de información, así como de las comunicaciones que resguardaron en su momento, ya que es a través de éstos que la Secretaría cumple sus metas fiscalizadoras y de rendición de cuentas, además de obstruir la prevención de delitos o ilícitos a sistemas y equipos de informática de la Secretaría de la Función Pública, por lo que dichas especificaciones deberán continuar reservados con fundamento en lo dispuesto por el artículo 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública y 113, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública en relación con el artículo 211 Bis 2, del Código Penal Federal.

En esa tesitura, la Dirección General indicó que actualmente la Secretaría resguarda la seguridad de las instalaciones de tecnologías de información y comunicaciones, a través de una arquitectura con funciones equivalentes a las que en su momento se prestó a través del contrato DC-027-2014 "SERVICIO INTEGRAL DE SEGURIDAD INFORMÁTICA", por lo que dar a conocer 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 red de la dependencia, lo cual sustenta la reserva que presenta, ya que se pretende prevenir y evitar la intromisión, modificación, pérdida o destrucción de información contenida en sistemas o equipos de informática protegidos por los mecanismos de seguridad de los equipos a cargo de la Secretaría de la Función Pública que forma parte de uno de los poderes del Estado.

Adicionalmente, la unidad administrativa manifestó que 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 dar a conocer la información relativa a la descripción de los componentes, mecanismos y el entorno tecnológico mediante los cuales proporcionó el servicio Integral de Seguridad Informática, permitiría el análisis de potenciales vulnerabilidades de la red institucional y potencializa la comisión de conductas que son tipificadas por el Código Penal Federal como delitos.

Abundo, en que las instalaciones de tecnologías de esta dependencia, como son la red institucional, consistente en sistemas de comunicaciones y de seguridad de la información, 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 protegidos por los mecanismos de seguridad de la Secretaría de la Función Pública, por lo que aún y cuando los servicios del contrato DC-027-2014 "SERVICIO INTEGRAL DE SEGURIDAD INFORMÁTICA" concluyeron, es necesario reservar la información relacionada con la arquitectura tecnológica y el entorno de operación de los mecanismos de seguridad mediante los cuales prestó el servicio.

El riesgo real, identificable y demostrable que ocasionaría la difusión de esta información, se traduce en hacer del conocimiento general elementos del entorno tecnológico actual de la Secretaría, que al ser sujetos de un análisis dirigido, se podrían explotar posibles vulnerabilidades sobre la operación de los procesos críticos de las tecnologías de información y comunicaciones de la red, equipos y sistemas institucionales aun 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, impactando en el cumplimiento de las atribuciones de esta Dependencia.

Además, hacer pública la información implicaría la necesidad inmediata de establecer medidas contingentes para prevenir cualquier situación de riesgo, 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. Lo anterior, ya que como ha sido señalado hacer público el conocimiento del entorno tecnológico en donde se prestó el servicio, potencializa la vulnerabilidad a que están expuestas las instalaciones de tecnologías de información de la Secretaría, inclusive, ante la probabilidad de conductas tipificadas por la Legislación Penal Federal como delitos.

Finalmente, el riesgo se materializaría toda vez que la información del entorno tecnológico con el que se presta a la fecha el servicio de seguridad de la información, en estricto sentido, contiene antecedentes que podrían ser vulnerados, como es el caso de perfiles de uso, mecanismos de frontera de red, especificaciones del monitoreo y acciones de reacción, todos destinados a prevenir y disminuir el impacto de eventos adversos que potencialmente pueden afectar el logro de los objetivos institucionales o constituir una amenaza a la seguridad nacional, y que de darse a conocer, podrían configurar inclusive como lo ha expuesto, la comisión de conductas sancionadas por el Código Penal Federal como delitos.

Adicionalmente, la unidad administrativa señaló que las características especiales y específicas del equipo de propiedad de la empresa Mainbit con el que en su momento prestó el servicio integral de seguridad informática, se refiere a información de carácter patrimonial que es necesario que se reserve, ya que dicha empresa no ha otorgado autorización para que la misma se haga pública.

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 clasificación de reserva, comunicada por la Dirección General de Tecnologías de la Información y la Dirección General de Recursos Materiales y Servicios Generales, por el 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.

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 Plataforma Nacional de Transparencia, de conformidad con el artículo 136 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, 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 la unidad administrativa responsable ejerza las facultades que tiene conferidas, la información de mérito obra de forma impresa en su archivo, sin que disponga de una versión electrónica.

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 fotocopiarse 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 138 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 las unidades administrativas responsables de contar con la información, en este caso, la Dirección General de Tecnologías de la Información y la Dirección General de Recursos Materiales y Servicios Generales, las cuales contarán con un plazo de hasta 6 días hábiles contados a partir de la fecha en que se le comunique haberse realizado 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.

En virtud 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 Gubernamental, por lo que no es posible exceptuar el pago de reproducción y envío.

Por lo expuesto y fundado, es de resolver y se

RESUELVE

PRIMERO.- Se confirma la clasificación de los confidenciales y reservados comunicados por la Dirección General de Tecnologías de la Información y la Dirección General de Recursos Materiales y Servicios Generales, por lo que se pone a disposición del peticionario versión pública de la información solicitada, en la forma y términos señalados en el Considerando Segundo de esta determinación.

SEGUNDO.- 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.

TERCERO.- 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: Lío. Ivonne Guerra Basulto

Revisó: Lío. Lilitana Olvera Cruz