SFP
SECRETARÍA DE LA FUNCIÓN PÚBLICA

Órgano Interno de Control en el Instituto Mexicano del Petróleo.

Área de Responsabilidades.

Expediente: INC-005/2014

RESOLUCIÓN

En la Ciudad de México, Distrito Federal, a veintidós de enero de dos mil quince.----------

VISTO para resolver los autos del expediente administrativo número INC-005/2014, integrado en esta Área de Responsabilidades del Órgano Interno de Control en el Instituto Mexicano del Petróleo, con motivo del escrito de inconformidad presentado por el [redacted], en su carácter de Apoderado Legal de las empresas Servicios Alestra, S.A. de C.V. y Alestra, S. de R.L. de C.V., así como por el C. [redacted], Apoderado Legal de la empresa SK Holdings, S.A. de C.V., a través del cual interponen inconformidad en contra del fallo de fecha once de julio del dos mil catorce, emitido en la Licitación Pública Electrónica de Carácter Nacional a precio fijo, para la Contratación del Servicio de Seguridad Perimetral para la Red IMP. No. LA-018T0O004-N152-2014. ----------

R E S U L T A N D O

PRIMERO.- Que con fecha cuatro de agosto del dos mil catorce, se recibió en esta Área de Responsabilidades el acuerdo 115.5.2068 de fecha veintiuno de julio del dos mil catorce, emitido dentro del expediente 433/2014 por el Director General de Controversias y Sanciones en Contrataciones Públicas de la Secretaría de la Función Pública, a través del cual ordenó remitir el escrito de inconformidad presentado por el [redacted], en su carácter de Apoderado Legal de las empresas Servicios Alestra, S.A. de C.V., y Alestra, S. de R.L. de C.V., así como por el [redacted], Apoderado Legal de la empresa SK Holdings, S.A. de C.V. a través del cual interponen inconformidad en contra del fallo de fecha once de julio del dos mil catorce, emitido en la Licitación Pública Electrónica de Carácter Nacional a precio fijo, , para la Contratación del Servicio de Seguridad Perimetral para la Red IMP. No. LA-018T0O004-N152-2014.----------

SEGUNDO.- Que mediante acuerdo de fecha cinco de agosto de dos mil catorce, se tuvo por admitida la inconformidad, teniendo por acreditada la personalidad del [redacted], Apoderado Legal de las empresas Servicios Alestra, S.A. de C.V. y Alestra, S. de R.L. de C.V., con la copia certificada de las escrituras públicas [redacted] del veintidós de octubre del dos mil doce y veinticinco de julio del dos mil trece respectivamente, pasada ante la fe del Notario Público No. 115, de San Pedro Garza García Nuevo León, y por lo que hace al [redacted], quedó acreditada su personalidad como Apoderado Legal de la empresa SK Holdings, S.A. de C.V., con la copia certificada de la escritura pública [redacted] del tres de diciembre del dos mil cuatro, pasada ante la fe del Notario Público No. 42 del Distrito Federal.----------

TERCERO.- Que mediante oficio 18/474/JOA-405/2014 de fecha seis de agosto de dos mil catorce, se comunicó al Apoderado Legal de la empresa Servicios Alestra, S.A. de C.V., la admisión de su inconformidad y que se acordó lo correspondiente a las pruebas ofrecidas. ---

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

Además, se le informó que se solicitaría a la convocante el expediente vinculado al proceso de contratación, y una vez recabado se acordaría lo que en derecho procediera. ----------

CUARTO.- Que mediante oficio número 18/474/JOA-404/2014 de fecha seis de agosto de dos mil catorce, se corrió traslado a la Gerenta de Proveeduría y Servicios del Instituto Mexicano del Petróleo de la inconformidad presentada por el [redacted], en su carácter de Apoderado Legal de las empresas Servicios Alestra, S.A. de C.V. y Alestra, S. de R.L. de C.V., así como por el [redacted], Apoderado Legal de la empresa SK Holdings, S.A. de C.V., a efecto de que rindiera informe previo en el que proporcionara los datos generales del procedimiento de contratación y del tercero interesado en el procedimiento de referencia. Además, el monto económico autorizado del procedimiento de contratación y en su caso el monto del contrato, y se pronunciara sobre la suspensión decretada de oficio. ------

Asimismo, se solicitó el informe circunstanciado de cada uno de los puntos manifestados por las inconformes, así como las pruebas correspondientes. Además se le requirió el expediente vinculado al proceso de contratación. ----------

QUINTO.- Que mediante oficio 350209/AA/338/2014 de fecha once de agosto de dos mil catorce, el Encargado del Despacho de la Administración de Recursos en Adquisiciones de Bienes y Servicios de la Gerencia de Proveeduría y Servicios del Instituto Mexicano del Petróleo, informó el estado que guardaba el proceso de la Licitación Pública Electrónica de Carácter Nacional a precio fijo No. LA-018T0O004-N152-2014, para la Contratación del Servicio de Seguridad Perimetral para la Red IMP, señalando que no era posible suspender actos relacionados con el fallo, en razón de que el acto impugnado ya estaba consumado. ----

SEXTO.- Que mediante acuerdo de fecha catorce de agosto de dos mil catorce, se tuvo por recibido el oficio número 350/AA/340/2014 de esa misma fecha, mediante el cual el Encargado del Despacho de la Administración de Recursos en Adquisiciones de Bienes y Servicios de la Gerencia de Proveeduría y Servicios del Instituto Mexicano del Petróleo, rindió el informe circunstanciado relativo a los hechos planteados en la inconformidad presentada por el [redacted], en su carácter de Apoderado Legal de las empresas Servicios Alestra, S.A. de C.V. y Alestra, S. de R.L. de C.V., así como por el [redacted], Apoderado Legal de la empresa SK Holdings, S.A. de C.V. ----------

SÉPTIMO.- Que con fecha once de agosto del dos mil catorce, se emitió el oficio 18/474/JOA-412/2014, mediante el cual se corrió traslado a la empresa Optimiti Network, S.A. de C.V., en su calidad de tercero interesado, la inconformidad presentada por la empresa Servicios Alestra, S.A. de C.V. y otros, con el propósito de que manifestara lo que a su derecho conviniera, el cual le fue notificado el diecinueve del mes y año en cita, recibiéndose en este Órgano Interno de Control con fecha veintiséis de agosto del dos mil catorce, escrito signado por la [redacted], en su calidad de Administrador Único del tercero interesado, en la que manifestó lo que en derecho de su representada convenía. ----------

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

OCTAVO.- Con fecha veinte de agosto del dos mil catorce, se recibió el oficio 18/474/JOB-214/2014, suscrito por el Titular del Área de Auditoría Interna de este Órgano Interno de Control, a través del cual remite el expediente original de la Licitación Pública Electrónica de Carácter Nacional a precio fijo, para la Contratación del Servicio de Seguridad Perimetral para la Red IMP, número LA-018T0O004-N152-2014, el cual le fue proporcionado por el Encargado del Despacho de la Administración de Recursos en Adquisiciones de Bienes y Servicios del Instituto Mexicano del Petróleo. ----------

NOVENO.- Que con oficio 18/474/JOA-430/2014 de fecha veintiuno de agosto de dos mil catorce, esta Autoridad procedió en términos del artículo 71, párrafo sexto de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público; por lo que puso a disposición del Apoderado Legal de la empresa Servicios Alestra, S.A. de C.V., el informe circunstanciado rendido por la Convocante, a efecto de que en el término de tres días hábiles, procediera en su caso, a realizar la ampliación de los motivos de su impugnación. Por lo que con fecha veintiséis de agosto del mismo año, se recibió escrito, signado por el [redacted], representante de las empresas inconformes mediante el cual amplió sus conceptos de inconformidad. ----------

En base a lo anterior, solicitó se tuviera como presentada la presente ampliación a la inconformidad y, en su oportunidad, se dictara la resolución que en derecho correspondiera.--

DÉCIMO.- Que mediante oficio 18/474/JOA-444/2014 del uno de septiembre del dos mil catorce, se corrió traslado al Área Convocante del Instituto Mexicano del Petróleo, del escrito de ampliación de los motivos de inconformidad hechos valer por el [redacted], representante de las inconformes, a efecto de que rindiera el informe circunstanciado correspondiente, dando respuesta a través de su diverso 350209/AA/393/2014 del nueve de septiembre del mismo año. ----------

DÉCIMO PRIMERO.- Que mediante oficio 18/474/JOA-443/2014 del uno de septiembre del dos mil catorce, se corrió traslado a la empresa Optimiti Network, S.A. de C.V., en su calidad de tercero, del escrito de ampliación de los motivos de inconformidad hechos valer por las empresas inconformes, a efecto de que manifestara lo que a su derecho conviniera, recibiéndose en este Órgano Interno de Control con fecha veinticuatro del mismo mes y año, escrito firmado por la [redacted], Administrador Único de Optimiti Network, S.A. de C.V., en la que expresó lo que a su representada convenía. ----------

DÉCIMO SEGUNDO.- Que con fecha doce de septiembre del dos mil catorce, se emitió acuerdo a través del cual se tuvo por admitida la prueba pericial ofrecida por las empresas inconformes, acordándose en el mismo, que se requiriera a la empresa Optimiti Network, S.A. de C.V., nombrara a un perito de su parte, además de que adicionara el cuestionario de preguntas a formularse a los peritos. ----------

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

DÉCIMO TERCERO.- Que con fecha siete de octubre del dos mil catorce, esta Autoridad levantó acta de comparecencia del perito para aceptación y protesta del cargo conferido al [redacted], perito ofrecido por las inconformes, quien con fecha catorce de octubre del mismo año, presentó su dictamen.----------

DÉCIMO CUARTO.- Que con fecha siete de octubre del dos mil catorce, esta Autoridad levantó acta de comparecencia del perito para aceptación y protesta del cargo conferido al [redacted], perito ofrecido por la empresa Optimiti Network, S.A. de C.V., quien con fecha trece de octubre del mismo año, presentó su dictamen.----------

DÉCIMO QUINTO.- Que con fecha diez de octubre del dos mil catorce, se emitió acuerdo en el que se admitieron las pruebas ofrecidas por las empresas inconformes en su escrito de ampliación, indicándose respecto a la prueba marcada con el numeral 3, que se ingresara a las páginas de Internet, a efecto de obtener una impresión de la información contenida en dichas páginas. ----------

DÉCIMO SEXTO.- Que con fecha dieciséis de octubre del dos mil catorce, se emitió acuerdo a través del cual se hizo constar que una vez que se ingresó a las páginas de Internet señaladas por las inconformes en su escrito de ampliación de sus motivos de inconformidad, se les requiriera exhibieran la correspondiente traducción al castellano. ----------

DÉCIMO SÉPTIMO.- Que a través del diverso 18/474/JOA-545/2014 del veinte de octubre del dos mil catorce, se solicitó a la Coordinadora General de Servicios Periciales de la Procuraduría General de la República, su apoyo para la designación de un perito en informática, con el propósito de que emitiera dictamen pericial respecto de los equipos propuestos por las empresas inconformes, por lo que con fecha veinticuatro de octubre del dos mil catorce, se recibió el oficio con número de folio 76311 signado por el Director General de Ingenierías Forenses de la citada Procuraduría, en el que propone como peritos en materia de informática, a los Ingenieros Jorge Alberto Grande Arriola y José Héctor Cortes Becerril, quienes con fecha cuatro de noviembre de dos mil catorce, protestaron ante esta Autoridad el cargo de peritos; presentado el día veinticinco del mes y año en cita, su dictamen pericial. -----

DÉCIMO OCTAVO.- Que a través del escrito de veintidós de octubre del dos mil catorce, el [redacted] en su calidad de Apoderado Legal de Alestra, S. de R.L. de C.V., exhibió la traducción al castellano de los documentos que le fueron requeridos. ----------

DÉCIMO NOVENO.- Que mediante acuerdo de fecha veintisiete de octubre del dos mil catorce, se ordenó dar vista tanto a la convocante como al tercero interesado, de las traducción de los documentos exhibidos por las empresas inconformes para que manifestaran su conformidad con la traducción, o bien, hicieran los señalamientos correspondientes; por lo que mediante oficio 350209/AA/516/2014 del treinta y uno de octubre del dos mil catorce, y escrito del cuatro de noviembre del mismo año respectivamente, el Encargado del Despacho de la Administración de Recursos en Adquisiciones de Bienes y Servicios del Instituto Mexicano del

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

Petróleo, y el Administrador Único de la empresa Optimiti Network, S.A. de C.V., manifestaron su inconformidad respecto de algunos puntos de la traducción exhibida por parte de las inconformes. ----------

VIGÉSIMO.- Que con fecha treinta y uno de octubre del dos mil catorce, se recibió escrito del [redacted] en su calidad de Apoderado Legal de Alestra, S. de R.L. de C.V., el cual acompaña traducción certificada efectuada por un perito traductor autorizado por el H. Tribunal Superior de Justicia del Distrito Federal, la cual se integró al expediente, al no contraponerse a la traducción exhibida el veintidós del mismo mes y año. ----------

VIGÉSIMO PRIMERO.- Que mediante oficio 18/474/JOA-600/2014 del seis de noviembre del dos mil catorce, se solicitó a la Procuraduría General de la República, su colaboración con el propósito de que a través de un perito traductor e interprete, se realizara la traducción al castellano de los puntos que fueron cuestionados por el Área Convocante del Instituto Mexicano del Petróleo y por la empresa Optimiti Network, S.A. de C.V., dictamen que fue emitido por la C. Rosa María Cervantes Negrete, perito traductor adscrita al Departamento de Traducción de la Agencia de Investigación Criminal de la citada Procuraduría, el cual fue remitido a través del oficio con número de folio 81898 de fecha veintiocho de noviembre del mismo año. ----------

VIGÉSIMO SEGUNDO.- Que con fecha diez de diciembre del dos mil catorce, se emitió el oficio 18/474/JOA-638/2014, dirigido al Administrador Único de la empresa Optimiti Network, S.A. de C.V., a efecto de hacerle del conocimiento que se ponía a su disposición las actuaciones del expediente en que se actúa, para que en el plazo de tres días formulara sus alegatos, recibiéndose con fecha dieciséis de diciembre del mismo año, escrito signado por la [redacted] Administrador Único de la citada empresa, quien manifestó lo que a derecho de su representada convenía. ----------

VIGÉSIMO TERCERO.- Que con fecha diez de diciembre del dos mil catorce, se emitió el oficio 18/474/JOA-639/2014, dirigido al Apoderado Legal de la empresa Servicios Alestra, S.A. de C.V., a efecto de hacerle del conocimiento que se ponían a su disposición las actuaciones del expediente en que se actúa, para que en el plazo de tres días formulara sus alegatos, recibiéndose con fecha dieciocho de diciembre del mismo año, escrito signado por el [redacted], Apoderado Legal de la citada empresa, quien manifestó lo que a derecho de las inconformes convenía. ----------

VIGÉSIMO CUARTO.- Que con fecha catorce de enero de dos mil quince, se emitió acuerdo de cierre de instrucción del presente asunto; y ----------

CONSIDERANDO

PRIMERO.- Que el Titular del Área de Responsabilidades del Órgano Interno de Control en el Instituto Mexicano del Petróleo es competente para conocer y resolver la presente

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

inconformidad, con fundamento en lo dispuesto por los artículos 37, fracciones XII, XVI y XXVII de la Ley Orgánica de la Administración Pública Federal en relación con el Segundo y Noveno Transitorios del Decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Ley Orgánica de la Administración Pública Federal publicado en el Diario Oficial de la Federación el dos de enero de dos mil trece; 6, fracciones I y VIII y 25 del Estatuto Orgánico del Instituto Mexicano del Petróleo; 1, fracción IV, 11, 65, fracción III, 66, 69, 71, 72, 73 y 74 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público; 121, 122, 123 y 124 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público; y 1, 3, punto D y 80, fracción I, numeral 4 del Reglamento Interior de la Secretaría de la Función Pública. ----------

SEGUNDO.- Que el expediente en que se actúa ha quedado debidamente integrado en términos de las disposiciones aplicables, tal y como se describió en los Resultandos de la presente Resolución. ----------

TERCERO.- Que esta Área de Responsabilidades procede al análisis de los argumentos que hacen valer los Apoderados Legales de las empresas Servicios Alestra, S.A. de C.V., Alestra S. de R.L. de C.V. y SK Holdings, S.A de C.V., en su calidad de inconformes en contra del fallo de fecha once de julio del dos mil catorce, emitido en el procedimiento de la Licitación Pública Electrónica de Carácter Nacional a precio fijo, para la Contratación del Servicio de Seguridad Perimetral para la Red IMP. No. LA-018T0O004-N152-2014, a las manifestaciones realizadas por el Área Convocante del Instituto Mexicano del Petróleo, por el tercero interesado, en este caso la empresa Optimiti Network, S.A. de C.V. así como a la valoración de las pruebas ofrecidas por los involucrados, con base en las siguientes consideraciones: ----------

Respecto a los puntos señalados como hechos por las inconformes, es de manifestarse que el dieciocho de junio de dos mil catorce, el Instituto Mexicano del Petróleo, publicó la convocatoria correspondiente a la Licitación Pública Electrónica de Carácter Nacional a precio fijo, para la Contratación del Servicio de Seguridad Perimetral para la Red del IMP. No. LA-018T0O004-N152-2014; que el día veinticuatro de junio de dos mil catorce, se llevó a cabo la junta de aclaraciones; que el cuatro de julio del mismo año, se realizó el acto de presentación y apertura de proposiciones, y que el día once de julio de dos mil catorce, se llevó a cabo el acto de fallo correspondiente a la citada licitación. ----------

Las empresas inconformes, hacen valer como argumentos en la primera parte de su primer y único agravio de su escrito del veintiuno de julio del dos mil catorce, lo siguiente: ----------

"...

AGRAVIOS

***PRIMERO**. El fallo impugnado viola en perjuicio mi representada lo dispuesto en el artículo 36, párrafo segundo y 37, fracción I de la LAASSP, ya que la convocante no verificó que la propuesta técnica de mi representada sí cumplían con los requisitos solicitados en la convocatoria de la licitación e indebidamente*

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

desechó la misma, con motivo de un análisis técnico carente de exhaustividad, al considerar que los equipos ofertados, no cumplen con los requisitos previstos en la convocatoria.

A continuación se analizan cada uno de los supuestos incumplimientos.

En primer término la convocante señala que el equipo FortiDDoS no cumple con las características técnicas solicitadas. Conviene acudir al texto mismo de la convocatoria para dilucidar la ilegalidad del fallo.

En la convocatoria foja 44 V) punto 1 se precisó:

> *"V) Sistema de Protección de la Disponibilidad y mitigación de ataques de DDoS*
>
> *1) El sistema deberá de ser un appliance dedicado a proporcionar disponibilidad por lo que no se aceptarán dispositivos que mantengan el estado de la conexión como firewall, sistemas de prevención y detección y las variantes o combinaciones como UTM, NGFW, NGIPS ya que al conservar el estado de la conexión son por sí mismos susceptibles a DDoS ."*

Mi representada cumplió con el requisito anterior.

Sin embargo, a foja 8 del fallo controvertido la convocante señaló que mi representada:

"No cumple técnicamente con lo siguiente:

1. *Descripción del servicio de seguridad perimetral para la red IMP, punto 6.*
   "El sistema deberá ser un appliance dedicado a proporcionar disponibilidad por lo que no se aceptarán dispositivos que mantengan el estado de la conexión como firewall, sistemas de prevención y detección y las variantes o combinaciones como UTM, NGFW, NGIPS ya que al conservar el estado de la conexión con por sí mismos susceptibles a DDoS.
   V) Sistema de Protección de la Disponibilidad y mitigación de ataques de DDoS, punto 1 "El sistema deberá de ser un appliance dedicado a proporcionar disponibilidad por lo que no se aceptaran dispositivos que mantengan el estado de la conexión como firewall, sistemas de prevención y detección y las variantes o combinaciones como UTM, NGFW, NGIPS ya que al conservar el estado de la conexión son por sí mismos susceptibles a DDoS."

El contenido del fallo impugnado revela falta de exhaustividad al hacer el estudio cualitativo del equipo, al no tomar en consideración las convenciones establecidas en el handbook del equipo FortiDDoS 400B.

A continuación se describen las características relevantes del equipo citado en el párrafo anterior traducidas al español, que deben ser confrontadas con el requisito de la convocatoria consistente en que los dispositivos ofertados no deben mantener el estado de la conexión (stayfull).

Dichas características pueden ser consultadas en la siguiente liga:
http://docs-legacy.fortinet.com/fddos/4-1-0/index.html#page/FortiDDoS Handbook/differences and simularities.html

"Diferencias y ventajas entre un equipo FortiDDos y un firewall convencional:

Diferencias y similitudes con los firewalls convencionales
Los firewalls de estado convencionales eliminan paquetes o conexiones con estado, pero no pueden correlacionar los paquetes con una fuente. FortiDDoS tiene una característica única que le permite correlacionar rápidamente ataques y verificar si son iniciadas por un solo host. Si puede hacer eso (en

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.
Tel.: (55) 9175 8084 facosta@imp.mx

caso de que sea un ataque no autentico), bloquea la fuente infractora durante un período de tiempo más largo.
Es importante comprender las diferencias entre un firewall de estado y un sistema de Análisis de Comportamiento de estado de Red (NBA) tal como FortiDDoS. Aquí están las principales diferencias:
Los firewalls convencionales tienen reglas que permiten o niegan paquetes o conexiones individuales en función de sus características individuales. No se acuerdan de los paquetes en forma agregada.
FortiDDoS opera sobre una base agregada. Observa las tasas de paquetes, normalmente dentro de un segundo, durante un período de tiempo. Mide las tasas de paquetes para varios parámetros de capa 3, 4, y 7, y compara frente a umbrales establecidos para ellos.
Si la tasa supera el umbral, las bloquea durante un período configurado.
En un firewall, el administrador puede establecer una regla que permite al puerto de destino UDP 1434, independientemente de la tasa.
En cambio, un administrador de FortiDDoS puede establecer una regla que permita UDP 1434 sólo si la tasa está dentro de 10 paquetes por segundo. Más allá de este caso, los paquetes UDP con destino a ese puerto se descartan.
Hay algunas características en FortiDDoS que son similares a un firewall. Portante, es importante aprender a graduarse a FortiDDoS.
Al igual que un firewall, FortiDDoS le permite configurar condiciones de bloqueo de capa 3, 4 y 7. Para ver una descripción de los parámetros de tráfico que se pueden configurar, consulte "Listas de control de acceso (ACL)".

En cuanto al funcionamiento del equipo en esta liga se puede apreciar la siguiente información traducida al español:

http://docs-legacy.fortinet.com/fddos/4-1-0/index.html#page/FortiDDoS_Handbook/strategies_for_protection.html

Estrategias para la protección:
Las mejores estrategias de seguridad abarcan personas, operaciones y tecnología. Los dos primeros suelen caer dentro de un dominio autónomo, por ejemplo, dentro de una empresa o departamento de TI que pueda hacer cumplir los procedimientos entre los empleados, contratistas o socios. Pero debido a que el Internet es un recurso público, tales políticas no se pueden aplicar a todos los usuarios potenciales de un sitio web público o un servidor de correo electrónico. Afortunadamente, la tecnología ofrece una gama de productos de seguridad para hacer frente a las diversas vulnerabilidades.
Firewalls
Los firewalls pueden hacer mucho para resolver algunos problemas limitando el acceso a los usuarios autorizados y bloqueando protocolos no deseados. Como tales, son una parte valiosa de una estrategia de seguridad. Pero los sitios web públicos y servidores de comercio electrónico no pueden saber de antemano quién va a tener acceso a ellos y no se puede "preseleccionar" a los usuarios a través de una lista de acceso. Algunos protocolos pueden ser bloqueados por los firewalls, pero la mayoría de los ataques de denegación de servicio (DoS) utilizan los puertos autorizados (por ejemplo, el puerto TCP 80 para un servidor web) que no pueden ser bloqueados por un firewall sin bloquear con eficacia todo el tráfico HTTP legítimo al sitio, con lo que completa la tarea del hacker.
Los firewalls ofrecen cierta seguridad contra un ataque de DoS de usuario único denegando el acceso a la conexión de la delincuencia (una vez que se le conoce), pero la mayoría los ataques de DoS actualmente se distribuyen entre cientos o miles de zombies, cada uno de los cuales podría estar enviando paquetes legales que pasarían el escrutinio del firewall. Los firewalls realizan un servicio valioso en una estrategia integrada de seguridad, pero los firewalls por sí solos no son suficientes.

Estrategias para la protección:

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.
Tel.: (55) 9175 8084 facosta@imp.mx

Consultable en:
http://docs-legacy.fortinet.com/fddos/4-1-0/index.html#page/FortiDDoS_Handbook/strategies_for_protection.html

Las mejores estrategias de seguridad abarcan personas, operaciones y tecnología. Los dos primeros suelen caer dentro de un dominio autónomo, por ejemplo, dentro de una empresa o departamento que pueda hacer cumplir los procedimientos entre los empleados, contratistas o socios. Pero desde que el Internet es un recurso público, tales políticas no se pueden aplicar a todos los usuarios potenciales de un sitio web público o un servidor de correo electrónico. Afortunadamente, la tecnología ofrece una gama de productos de seguridad para hacer frente a las diversas vulnerabilidades.

Firewalls

Firewalls
Los firewalls pueden hacer mucho para resolver algunos problemas limitando el acceso a los usuarios autorizados y bloqueando protocolos no deseados. Como tales, son una parte valiosa de una estrategia de seguridad. Pero los sitios web públicos y servidores de comercio electrónico no pueden saber de antemano quién va a tener acceso a ellos y no se puede "preseleccionar" a los usuarios a través de una lista de acceso. Algunos protocolos pueden ser bloqueados por los firewalls, pero la mayoría de los ataques de denegación de servicio (DoS) utilizan los puertos autorizados (por ejemplo, el puerto TCP 80 para un servidor web) que no pueden ser bloqueados por un firewall sin bloquear con eficacia todo el tráfico HTTP legítimo al sitio, con lo que completa la tarea del hacker.
Los firewalls ofrecen cierta seguridad contra un ataque de DoS de usuario único denegando el acceso a la conexión de la delincuencia (una vez que se le conoce), pero la mayoría los ataques de DoS actualmente se distribuyen entre cientos o miles de zombies, cada uno de los cuales podría estar enviando paquetes legales que pasarían el escrutinio del firewall. Los firewalls realizan un servicio valioso en una estrategia integrada de seguridad, pero los firewalls por sí solos no son suficientes.

Listas de control de acceso del router
De igual modo, las listas de acceso en el router se pueden utilizar para bloquear ciertas direcciones, si dichas direcciones pueden ser conocidos a priori. Pero las páginas web abiertas al público están, por naturaleza, abiertas a conexiones desde equipos individuales, que son exactamente los agentes que utilizan los hackers para iniciar ataques. En un DoS distribuido (DDoS) se utilizan en paralelo miles de conexiones aparentemente inocentes. Si bien las listas de acceso enrutador pueden ser utilizados para eliminar los paquetes ofensivos una vez que se identifican, los routers carecen de la capacidad de procesamiento y la heurística de perfiles para hacer tales identificaciones por su cuenta. Adicionalmente, las listas de acceso complejas pueden causar cuellos de botella de procesamiento en los routers, cuya función principal es enrutar los paquetes IP. La realización de inspecciones de paquetes en las capas 3, 4 y 7 reduce los recursos del router y puede limitar el rendimiento de la red.

El software antivirus
Los sistemas finales no pueden considerarse seguros sin un software AntiVirus. Este tipo de software explorará todas las entradas al sistema en busca de virus y gusanos conocidos que pueden causar daños en el sistema final y cualesquiera otras que puedan infectar. Incluso después de que un virus se conoce y se caracteriza, aún hay rastros del mismo circulando en Internet, a través de correo electrónico, en discos compactos (CD) y discos flexibles. Una buena suscripción de antivirus que se actualiza con frecuencia para la protección más reciente tiene un valor incalculable para cualquier usuario de computadora de empresa o individual.

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.
Tel.: (55) 9175 8084 facosta@imp.mx

Pero incluso el software antivirus no es suficiente para detener a los ataques que han sido hábilmente disfrazadas. Una vez que el sistema está infectado con una nueva cepa, el daño puede ser hecho antes de que se detecte el virus o gusano, y que se desinfecte el sistema.

Protección de aplicaciones

Estos paquetes incluyen software que vigila las anomalías de correo electrónico, las consultas con acceso de base de datos, u otros comportamientos que pueden explotar la vulnerabilidad en la aplicación. Debido a que debe ser muy específica para la aplicación que está protegiendo (y muy cercana a ella), la protección de aplicaciones se implementa como software en el host. Los servidores dedicados se beneficiarían de un software bien diseñado de seguridad de aplicaciones que mantendrá la integridad del código y detectará comportamientos anómalos que podrían indicar un ataque. Determinado código malicioso puede intentar sobrescribir registros en el sistema final y de ese modo secuestrar el hardware con fines destructivos.

Sistemas de detección de intrusiones

Los Sistemas de Detección de Intrusiones (IDS) están diseñados para "escuchar" el tráfico y el comportamiento y programar una alarma si se cumplen ciertas condiciones. Algunas implementaciones IDS viven en el huésped, mientras que otros están desplegados en la red. El sensor del IDS monitoriza el tráfico en busca de violaciones de protocolo, variaciones del tipo de tráfico o coincidencias con conocidos "firmas" de ataque. Cuando se detecta una amenaza, se envía una alarma para notificar a un administrador de red (humano) que debe intervenir. Todos los IDS utilizan software, pero algunos se ejecutan en computadoras de propósito general, mientras que otros hacen uso de hardware especialmente diseñado.

Sistemas de detección y prevención de intrusiones basados en host

Algunos sistemas de detección de intrusiones están diseñados como software que se ejecuta en plataformas informáticas de propósito general. No debe confundirse con el software de seguridad de aplicaciones (mencionado anteriormente), que se ejecuta en el sistema final y se centra principalmente en la capas 5-7; los sistemas de intrusión de basados en software también deben centrarse en las capas 3 y 4 de la pila de protocolos. Estos paquetes se basan en la potencia del CPU del sistema host para analizar el tráfico conforme entra en el servidor. Las computadoras de propósito general a menudo carecen de las prestaciones requeridas para monitorear el tráfico de red en tiempo real y realizar sus funciones primarias. La creación de un cuello de botella en la red o en el servidor, en realidad, ayuda al hacker a lograr su objetivo mediante la restricción del acceso a recursos valiosos. Los sistemas finales proporcionan el mejor entorno para el reconocimiento de firmas porque los paquetes están completamente rearmados y se ha realizado cualquier descifrado necesario. Sin embargo, la detección de intrusos basada en firmas tiene sus limitaciones, como se describe a continuación.

Sistemas de prevención de intrusiones basados en el contenido

El siguiente paso en la evolución de la seguridad de intrusión da lugar a los Sistemas de Prevención de Intrusiones (IPS). A diferencia de los Sistemas de Detección de Intrusiones, que requieren la intervención manual de un administrador para detener un ataque, un IPS tomará automáticamente medidas para prevenir un ataque una vez que se reconoce. Esto puede reducir el tiempo de respuesta a cerca de cero, que es el objetivo final de la seguridad de intrusión.

La prevención de intrusos debe ser inteligente, no obstante, o el remedio puede realmente alcanzar el objetivo de los hackers de denegar recursos a los usuarios legítimos. Los mecanismos de prevención también pueden ser perjudiciales si la detección está sujeta a falsos positivos o a una incorrecta identificación de la intrusión. Si la acción de prevención es deshabilitar un puerto, protocolo, o dirección, un falso positivo podría resultar en la denegación de servicio a uno o más usuarios legítimos.

Análisis del comportamiento de la red

Una alternativa para el reconocimiento de firmas es el análisis de comportamiento de la red. Los sistemas basados en tasas deben proporcionar análisis y/o controles detallados de flujo de tráfico. Se establece una referencia de los patrones de tráfico, por lo general durante un modo de aprendizaje en el que el dispositivo sólo "escucha" sin actuar conforme a las condiciones de alarma. Un buen sistema tendrá parámetros predeterminados establecidos a niveles razonables, pero se requiere el período de

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

"escucha" para conocer el comportamiento del tráfico en varios sistemas. El periodo de escucha debe ser 'típico', en el sentido de que no debe haber ataques o patrones inusuales de tráfico. Por ejemplo, el sábado y el domingo probablemente no sean buenos días para construir una referencia para un servidor empresarial que es mucho más concurrido entre semana. Los períodos de tráfico inusualmente alto o bajo también representan malos intervalos de escucha, como la semana de vacaciones de Navidad; lo mismo sucede con el tráfico inusualmente alto debido a eventos externos (comunicados de prensa, promociones de ventas, espectáculos de medio tiempo del Super Bowl, y así sucesivamente). Una vez que se establece una referencia, los sistemas basados en tasas observan las desviaciones de los patrones conocidos de tráfico para detectar anomalías. Los buenos sistemas permitirán a un administrador reemplazar los parámetros de referencia si se prevén eventos que provocarán oleadas de tráfico; por ejemplo, una copia de seguridad del servidor programada durante la noche. Mientras que los sistemas basados en firmas son examinados en busca de falsos negativos, o por no identificar un ataque, los sistemas basados en tasas deben ser examinados en busca de falsos positivos, o por no identificar como ataques cambios legítimos en los patrones de tráfico. Ya sea mediante la creación de alarmas o la toma de medidas preventivas, los sistemas basados en tasas deben estar bien diseñados para evitar una sobrecarga innecesaria.

Las herramientas de análisis son igualmente importante para los sistemas basados en tasas. Los administradores deben ser capaces de ver sus patrones de tráfico en varios niveles y utilizar esta información para ajustar sus recursos de red.

Comportamiento de un equipo FortiDDos para el análisis del comportamiento de una red convencional:

Consultable en: http://docs-legacy.fortinet.com/fddos/4-1-0/index.html#page/FortiDDoS_Handbook/comparing_fortiddos_to_conventional nba.html

Comparación de FortiDDoS con el análisis convencional del comportamiento de la red (NBA)

La prevención de ataques de DDoS requiere mantener estadísticas altamente granulares en las Capas 3, 4 y 7. Es esencial rastrear fuentes individuales, destinos, protocolos, conexiones y puertos que se pueden sumar a millones de parámetros. FortiDDoS es una solución de NBA basada en hardware y, a diferencia de las soluciones basadas en software, mantiene los niveles normales de procesamiento y transferencia de datos durante ataques de denegación de servicio.

El diseño de hardware a la medida de FortiDDoS supervisa los umbrales de todo el tráfico en las capas 3, 4 y 7. Mide recuentos de paquetes y bytes, transiciones de estado, fragmentos, checksum, banderas, nuevas conexiones, pares de direcciones, etc. Puede establecer umbrales en cualquiera de estos parámetros de red para limitar la tasa de tráfico para particulares sistemas o aplicaciones. Para reconocer y prevenir ataques, FortiDDoS monitoriza decenas de parámetros para detectar cambios sutiles en el comportamiento del tráfico de red. La siguiente tabla muestra la capacidad mecanismos de medición provistos por FortiDDoS.

Tabla 1: Tabla de Umbral de Tráfico de FortiDDoS

Capa	*Tipo*	*Medidores*
3	*1. Inundación de protocolos*	*256*
	2. Inundación de fragmentos	*1*
	3. Inundación de fuente IP y rastreo de fuentes	*1 millón*
	4. Inundación de destinos IP	*1 millón*
4	*1. Inundación de puerto TCP*	*65535*
	2. Inundación de puerto UDP	*65535*
	3. Inundación de tipo/código ICMP	*65535*

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

	4. Inundación de conexión TCP	*1 millón*
	*5. Tabla de IP legítimos (para inundación de **zombies y SYN**)*	*2 millones*
	6. Inundación de SYN	*1*
	7. Fuente/tasa excesiva de SYN	*1 millón de fuentes*
	8. Fuente/conexiones concurrentes excesivas	*1 millón de fuentes*
	9. Destinos/conexiones concurrentes excesivas	*1*
	10. Destinos/ACK excesivos	*1*
	11. Destinos/RST excesivos	*1*
	12. Destinos/FIN excesivos	*1*
7	*1. Métodos HTTP*	*8*
	2. Inundación de URL	*65536*
	3. Host	*512*
	4. Referente	*1*
	5. Cookie	*1*
	6. Usuario-Agente	*1*
	7. Encabezados HTTP Obligatorios	*1*
	8. Accesos Secuenciales	*1*
	9. URL/fuente	*1 millón de fuentes*
	10. Fuente/solicitudes SIP INVITE excesivas	*1 millón de fuentes*
	11. Fuente/solicitudes SIP INVITE concurrentes excesivas	*1 millón de fuentes*
	12. Fuente/solicitudes SIP REGISTER excesivas	*1 millón de fuentes*

De lo que se advierte que, contrario a lo considerado por la convocante, el equipo FortiDDoS ofertado por mi representada sí cumple con los requisitos previstos en la convocatoria, pues el FortiDDoS es una solución basada en hardware de la NBA y la diferencia de las soluciones basadas en software, mantiene los niveles normales de procesamiento y transferencia de datos durante ataques de denegación de servicio, pero no mantiene el estado de la conexión, de modo que no incumple las condiciones de la convocatoria."

Que el Encargado del Despacho de la Administración de Recursos en Adquisiciones de Bienes y Servicios de la Gerencia de Proveeduría y Servicios del Instituto Mexicano del Petróleo, dio respuesta a los planteamientos de las inconformes, a través de su oficio 350209/AA/340/2014 del catorce de agosto del dos mil catorce, manifestando que como parte del análisis previo a las necesidades para la licitación en cuestión, se identificaron criterios tecnológicos que dieran cumplimiento a este fin, siendo uno de los principales requerimientos que permiten garantizar la disponibilidad de la información de las instituciones públicas, se relaciona con la capacidad de respuesta a ataques de denegación de servicios, conocidos como DDoS.----------

Señala la convocante haber identificado que las soluciones tecnológicas que en sus especificaciones técnicas indican el concepto "stateful" implican un riesgo en la estrategia de

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

disponibilidad de los servicios tecnológicos, razón por lo cual en la convocatoria se precisó que la solicitud ofrecida no debería mantener el estado de la conexión, esto es, no ser "stateful". --

Que de la valoración de la propuesta presentada por las inconformes, se advierte que el equipo ofertado no cumple con la especificación solicitada de la sección "Sistemas de protección de la disponibilidad y mitigación de ataques DDoS". ----------

Por su parte, la empresa Optimiti Network, S.A. de C.V., en su calidad de tercero interesado, señaló en su escrito del veintiséis de agosto del dos mil catorce, con el cual da respuesta a los planteamientos de las empresas inconformes, que respecto al requisito del Instituto Mexicano del Petróleo, de presentar una propuesta técnica que incluya dispositivos que NO mantengan el estado de la conexión (stateless); que es ampliamente conocido en el medio de seguridad informática que cualquier dispositivo (independientemente de la marca) que sí mantenga el estado de la conexión (stateful), rastrea/mantiene todas las conexiones que fluyen a través de él para su inspección y las almacena en una tabla de conexiones. Indica además, que cada paquete se compara contra dicha tabla para verificar-validar que fue transmitida sobre una conexión legítima, señalando que las tablas típicas de conexiones pueden almacenar decenas de miles de conexiones activas, lo cual es suficiente para la actividad normal de una red; sin embargo, refiere el tercero interesado, que un ataque de DDoS puede incluir miles de paquetes por segundo. Dado que los dispositivos "stateful", abrirán una nueva conexión en su tabla de conexiones por cada paquete malicioso, esto resultaría en un rápido agotamiento ("exhaustation attacks") de dicha tabla, por lo que una vez que la tabla alcance su capacidad máxima, no permitirá que conexiones adicionales sean abiertas, impidiendo y bloqueando finalmente a los usuarios legítimos, y que no puedan establecerse conexiones. ----------

Que con fecha veintiséis de agosto del dos mil catorce, se recibió escrito signado por el [redacted] representante de las inconformes mediante el cual amplió sus conceptos de inconformidad, señalando entre otros puntos lo siguiente: ----------

"...

AGRAVIOS

***PRIMERO**. Del informe contenido en el oficio 350209/AA/340/2014, se advirtió como primer argumento de la convocante, el consistente en que ya se firmó el contrato de la licitación impugnada y que la migración comenzó a partir del 14 de julio de 2014, por lo que es un acto consumado.*

Argumento que es infundado ya que el hecho de que ya se haya suscrito el contrato respectivo, no significa que ya haya surtido sus efectos jurídicos y materiales de manera inmodificable a pesar de que ya comenzó la migración. Los efectos del acto impugnado no han cesado, toda vez que las consecuencias de los actos se efectúan de momento a momento durante la vigencia del contrato de 48 meses.

Una interpretación en el sentido que pretende la convocante, es inaceptable, pues como lo propone se estaría convalidando un acto que tiene origen en una actuación ilegal de la Convocante en donde no efectuó el debido análisis de los equipos ofrecidos en la propuesta de mi representada por lo que violó los principios esenciales de las licitaciones.

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

Se considera aplicable al caso concreto por analogía e identidad de razón, las siguientes tesis:

Octava Época
Instancia: Tribunales Colegiados de Circuito
Tesis Aislada
Fuente: Semanario Judicial de la Federación
XIII, Junio de 1994
Materia(s): Administrativa
Tesis:
Página: 676

"SUSPENSIÓN DEFINITIVA. ACTOS CONSUMADOS EN QUE PROCEDE CONTRA LOS EFECTOS DE LOS. *Si existe una resolución favorable a un particular; y con posterioridad la autoridad administrativa la revoca mediante un decreto, debe concederse la suspensión provisional, así como la definitiva, si fueron solicitadas en cuanto a los efectos y consecuencias legales de este acto (que no hayan sido consumados), pues no obstante que reviste la característica de consumado, son los efectos los que deben ser paralizados ya que le pueden causar perjuicio, en tanto se resuelve el fondo del juicio de amparo."*

CUARTO TRIBUNAL COLEGIADO EN MATERIA ADMINISTRATIVA DEL PRIMER CIRCUITO.

Incidente en revisión 544/94. Guillermo Zamudio Villanueva. 13 de abril de 1994. Unanimidad de votos. Ponente: Hilario Bárcenas Chávez. Secretario: Francisco Alonso Fernández Barajas.

Séptima Época
Instancia: Tribunales Colegiados de Circuito
Tesis Aislada
Fuente: Semanario Judicial de la Federación
217-228 Sexta Parte
Materia(s): Administrativa
Tesis:
Página: 627
Genealogía:
Informe 1987, Tercera Parte, Tribunales Colegiados de Circuito, tesis 37, página 144.

"SUSPENSIÓN, ACTOS DE TRACTO SUCESIVO PARA EFECTOS DE LA. *En materia de suspensión cabe distinguir entre actos de tracto sucesivo, es decir, los que se consuman de momento a momento, y aquellos actos que se consuman de una sola vez pero que al hacerlo crean una situación jurídica que se prolonga en el tiempo. En el primer caso (por ejemplo la intervención de una negociación) el acto reclamado se repite una y otra vez en el tiempo, consumándose y perfeccionándose reiteradamente, de manera que la suspensión puede otorgarse, sin que la medida tenga efectos restitutorios pues los actos ya realizados quedan intactos (la intervención se consuma en cada una de las operaciones verificadas por el interventor y la suspensión hace cesar la intervención sin invalidar sus actos anteriores). En el segundo caso (embargo sin intervención o clausura) el acto se consuma una sola vez, no necesita repetirse en el futuro y sus efectos se prolongan en el tiempo creando un estado jurídico determinado respecto del cual es improcedente la suspensión pues equivaldría a privar de eficacia el acto ya realizado (el embargo se traba una sola vez y también una sola ocasión se entregan al depositario los bienes, pero éstos quedan en lo sucesivo sujetos a un estado jurídico; en la clausura, ejecutada la orden y colocados los sellos, se*

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

prolongan en el tiempo sus efectos al impedir el funcionamiento del giro; en ambos casos es improcedente la suspensión porque con ella se dejaría sin efectos los actos de traba del embargo y entrega de bienes al depositario, o la ejecución de la orden de clausura y colocación de sellos, siendo por tanto la medida suspensiva de naturaleza restitutoria)."

TERCER TRIBUNAL COLEGIADO EN MATERIA ADMINISTRATIVA DEL PRIMER CIRCUITO.

Queja 27/87. Delegado del Departamento del Distrito Federal en Cuauhtémoc y otras. 27 de marzo de 1987. Ponente: Genaro David Góngora Pimentel. Secretaria: Adriana Leticia Campuzano Gallegos
Nota: En el Informe de 1987, la tesis aparece bajo el rubro "SUSPENSIÓN. ACTOS DE TRACTO SUCESIVO PARA EFECTOS DE LA SUSPENSIÓN.".

En este sentido, considerando la naturaleza del acto impugnado, contrariamente a lo manifestado por la convocante la licitación pública número ***LA-018T00004-N152-2014,*** *no es un acto consumado de manera irreparable.*

Es importante precisar que el fallo impugnado incumple con el principio de congruencia que debe tener todo acto administrativo, toda vez que la convocante considera que es un acto consumado de modo irreparable, porque consideró que el procedimiento de la licitación ya había concluido al suscribirse el contrato respectivo y encontrarse la licitante adjudicada efectuando la migración licitada, sin embargo, pasa por alto que un acto consumado es aquel cuya realización hace física y legalmente imposible volver las cosas al estado que guardaban antes de la violación.

Sobre todo, si el artículo 54 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, prevé que la dependencia o entidad podrá dar por terminados anticipadamente los contratos cuando se determine la nulidad de los actos que dieron origen al contrato, con motivo de la resolución de una inconformidad o intervención de oficio emitida por la Secretaría de la Función Pública.

Aunado a lo anterior, es importante precisar que la presente licitación pública tiene por objeto el brindar el servicio de seguridad perimetral para la red IMP, del 12 de julio de 2014 al 11 de julio de 2018, lo cual no significa que el hecho de que se haya comenzado con la migración de los bienes objeto del mismo se pueda considerar como un acto consumado, además de que tampoco ha transcurrido el plazo para el cual se previó la licitación pues no se han agotado sus efectos y sus consecuencias, por lo que no se puede considerar que se está en presencia de un acto consumado.

Para conocer si ello ocurrió irreparablemente, debe atenderse a las consecuencias de su ejecución y, en ese sentido, la reparación física y material no es imposible, pues la autoridad administrativa puede implementar los mecanismos necesarios para retrotraer a las cosas al estado en el que se encontraban.

Sirve de apoyo a lo anterior la tesis de jurisprudencia de la Novena Época, Instancia Segundo Tribunal Colegiado en Materia Administrativa y de Trabajo del Séptimo Circuito, Tesis Aislada, Materia (s) Administrativa, Tesis Vil, 2o.A.T.25 A, Página 1072, que a la letra establece:

"ACTO CONSUMADO DE UN MODO IRREPARABLE LA INSTALACIÓN DE SOFTWARE PARA EQUIPO DE CÓMPUTO NO PUEDE ESTIMARSE COMO TAL, PARA EFECTOS DE LA CAUSAL DE IMPROCEDENCIA PREVISTA POR EL ARTÍCULO 51, FRACCIÓN IV, DE LA LEY DE JUSTICIA ADMINISTRATIVA DEL ESTADO DE VERACRUZ. *Si bien el artículo 51, fracción IV, de la referida ley, establece como causal de improcedencia en el juicio de nulidad, que el acto impugnado se haya consumado de un modo irreparable, lo cierto es que si aquél se hizo consistir en la resolución*

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

que aprobó la licitación pública respecto de software para equipo de informática, éste no puede estimarse consumado irreparablemente por el hecho de que se haya instalado dicho equipo por parte de la empresa que resultó ganadora en la citada licitación, pues de conformidad con la doctrina y la jurisprudencia, sólo tienen tal carácter aquellos cuya realización hace que física y legalmente sea imposible volver las cosas al estado que guardaban antes de la violación, lo que no acontece tratándose de la instalación del citado equipo de cómputo, ya que es , evidente que de revocarse la resolución impugnada en el/ juicio de nulidad respectivo, en su caso, podría ser desinstalado, volviendo así las cosas al estado que guardaban antes de las violaciones alegadas en el citado juicio contencioso administrativo.
SEGUNDO TRIBUNAL COLEGIADO EN MATERIAS ADMINISTRATIVA Y DE TRABAJO DEL SÉPTIMO CIRCUITO
Amparo directo 774/2000. Niveles, S.A. de C.V. 31 de enero de 2001. Unanimidad de votos. Ponente: Víctor Hugo Mendoza Sánchez. Secretario: Alejandro Quijano Álvarez."

Así como la tesis de jurisprudencia I.4o.A.794 A de la Novena Época, Cuarto Tribunal Colegiado en Materia Administrativa del Primer Circuito, Tomo XXXIV, Septiembre de 2011, Materia Administrativa, Página 2151, que a la letra establece:

***"JUICIO CONTENCIOSO ADMINISTRATIVO FEDERAL NO QUEDA SIN MATERIA CUANDO SE IMPUGNA UN PROCEDIMIENTO DE LICITACIÓN PÚBLICA EN EL QUE CONCLUYO LA VIGENCIA DEL CONTRATO RELATIVO, AL NO TRATARSE DE UN ACTO CONSUMADO IRREPARABLEMENTE.** El artículo 9o., fracción V, de la Ley Federal de Procedimiento Contencioso Administrativo prevé como causal de sobreseimiento en el juicio contencioso administrativo, que éste quede sin materia, situación que no se actualiza cuando se impugna un procedimiento de licitación pública en el que concluyó la vigencia del contrato relativo, al no tratarse de un acto consumado irreparablemente. Ello es así, pues el hecho de que una licitación pública tenga por objeto otorgar un contrato con vigencia determinada, no significa que concluido el término de éste, por el solo transcurso del tiempo, se agoten sus efectos y consecuencias, pues si bien es cierto que puede considerarse que por ese hecho se está en presencia de actos consumados, entendidos como aquellos que han realizado en forma total todos sus efectos, también lo es que para discernir si ello ocurrió irreparablemente, debe atenderse a las consecuencias de su ejecución y, en ese sentido, la reparación física y material no es imposible, pues la autoridad administrativa puede implementar los mecanismos necesarios para indemnizar al actor por los daños causados, máxime que, de no resolverse el asunto, se convalidarían las ilegalidades eventualmente generadas en su perjuicio; de ahí el interés cualificado de éste para exigir la restauración del orden jurídico transgredido a través de la declaratoria en el juicio contencioso administrativo de la ilicitud del acto impugnado, interés que proviene de la referida afectación, ya sea directa o derivada, de la situación particular del individuo Respecto del orden jurídico, y que será base para obtener la restitución correspondiente.*
CUARTO TRIBUNAL COLEGIADO EN MATERIA ADMINISTRATIVA DEL PRIMER CIRCUITO
Amparo directo 254/2011. Biodist, S.A. de C.V. 14 de julio de 2011. Unanimidad de votos. Ponente: Jesús Antonio Nazar Sevilla. Secretario: Ernesto González."

SEGUNDO.- *A continuación la argumentación técnica que soporta los argumentos de la inconforme:*

a) Del análisis del informe efectuado por la convocante, se advierte que confunde el termino STATEFUL de la convocatoria, sin diferenciar y comprender el significado de cada una de las características donde se apreciaba el término Stateful en las páginas de internet que cita, es claro que omitió analizar exhaustivamente en estas páginas, todas las características del equipo FortiDDoS 400B, ofrecido por mi representada.

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

De acuerdo a las características técnicas del equipo citado en el párrafo anterior, el concepto técnico STATEFUL INSPECTION, que es la característica de funcionalidad que aplica para los equipos FIREWALL, no corresponde al concepto Stateful de la convocatoria, sin embargo, la convocante efectúa una traducción desafortunada de la palabra Stateful, sin tomar en consideración que las palabras que la acompañan en la característica reflejan la funcionalidad de esta y no necesariamente se refiere a que esta mantenga el estado de conexión, como indebidamente lo considera la convocante, de conformidad con lo siguiente:

STATEFUL MONITORING la traducción es MONITOREO DE ESTADO, lo que es un concepto diferente a STATEFUL INSPECTION de la convocatoria.

- STATEFUL PACKET INSPECTION la traducción es INSPECCIÓN DE ESTADO DE PAQUETES, lo que también es un concepto muy diferente a STATEFUL INSPECTION.

Lo planteado por la convocante es inexacto, al no hacer la diferencia de los términos debido a una mala traducción e interpretación de estos. Lo anterior, porque para la convocante el concepto de stateful implica un riesgo en la estrategia de disponibilidad de los servicios tecnológicos, razón por la cual se indicó en las bases de la licitación que la solución ofrecida no debe mantener el estado de conexión, esto es no ser stateful como se conoce en el sector de seguridad de la información.

En el informe de la convocante, se hace referencia a como los dispositivos de segundad, principalmente firewalls, realizan la inspección de estados con el objetivo de bloquear paquetes que se desvían del estado esperado, además de que se describen los lineamientos de los dispositivos de seguridad firewalls y no hace referencia a soluciones para mitigar ataques DDoS. Un Firewall convencional como al que hace referencia la convocante en su informe mantiene el estado de la conexión y cuenta con reglas que permiten o bloquean paquetes o conexiones individuales basadas en sus características individuales, además de que no cuenta con la capacidad de recordar paquetes de una manera agregada.

Sin embargo, el sistema FortiDDoS ofertado opera con base de agregación, en la que se revisan las tasas de paquetes por un periodo de tiempo (típicamente de un segundo) y lleva a cabo la medición de la tasa de paquetes de varias capas 3, 4 y 7 así como parámetros y los compara contra umbrales fijados por cada uno de ellos. Si la tasa excede el umbral, se bloqueará por el periodo configurado o predeterminado. En un firewall, el administrador configura una regla para un puerto: ejemplo UDP puerto destino 1434 sin tomar en cuenta la tasa de paquetes.

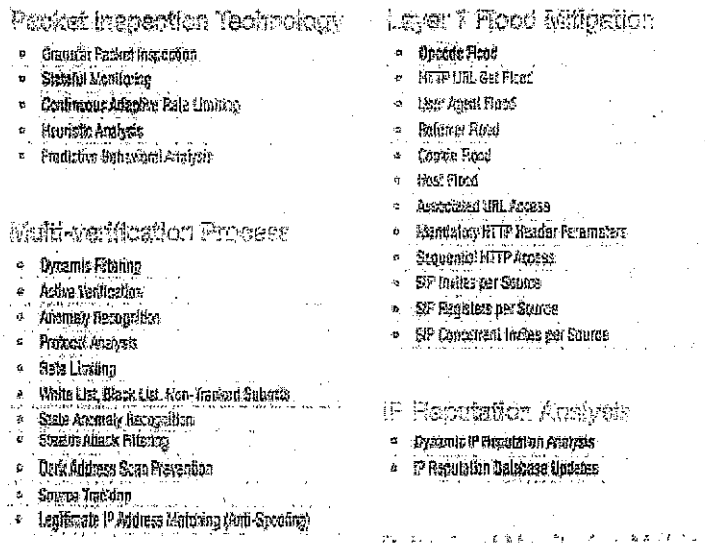
La prevención de ataques DDoS requiere el mantenimiento de estadísticas altamente granulares en las capas 3, 4, y 7 del Modelo OSI por lo que es esencial hacer un seguimiento individual de fuentes, destinos, protocolos, las conexiones y puertos que pueden sumar a millones de parámetros. FortiDDoS es una solución basada en hardware de la NBA y la diferencia de las soluciones basadas en software, mantiene niveles normales de procesamiento y transferencia de datos durante ataques de denegación de servicio.

Sin embargo, la convocante presentó las siguientes referencias de la página del fabricante.

a) De la revisión del documento presentado en sus anexos llamado FortiDDoS 1000B entre sus características describe al dispositivo como "Stateful Monitoring" que su traducción al español significa "Monitoreo de Estado"

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx



Referencia

http://www.fortinet.com/sites/default/files/productdatasheets/FortiDDos-1000B.pdf

Asimismo, del análisis que se efectúa al informe de la convocante se advierte que erróneamente considera un equipo que no es el ofertado por mi representada, porque destaca que el contenido presentado en la matriz de cumplimiento solo hace referencia a la descripción del producto identificado como FortiDDoS 1000B, y no así al ofrecido por mi representada que es el FortiDDoS 400B.

Lo anterior, es porque el sistema llamado FortiDDoS 1000B hace referencia a la familia de dispositivos Fortinet para mitigar y bloquear ataques que se caracterizan por el uso excesivo de red y que son conocidos en el medio de Sistemas de Información como DDoS attacks.

http://www.fortinet.com/sites/default/files/productdatasheets/FortiDDos-1000B.pdf

En la referencia pública presentada por la convocante, se especifica que el FortiDDoS es stateful, basando su criterio en una información en un documento catalogado como "legacy".

http://docs-legacy.fortinet.com/fddos/4-1-07index.html#page/FortiDDoS Handbook/basic topology.html

Esta referencia significa que no es la versión más actual o pertenece a generaciones anteriores del producto, pasando por alto que la solución de FortiDDoS propuesta, no es un dispositivo stateful en términos de la convocatoria, sino que cuenta con la capacidad de brindar protección ante ataques específicos de DDoS.

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

671

Además de que en la referencia pública de un tercero, que no es el fabricante del equipo propuesto, la Convocante se precisa que el equipo FortiDDoS 400B, es un Stateful Packet Inspection o su traducción en español "Inspección de estado de paquetes", lo que suma en contra de su argumentación.

http://www.cnet.com/products/fortinet-fortiddos-400b-securitv-appliance/specs/

Depth	16.3 in
Height	1.8 in
Weight	17.2 lbs
Manufacturer	Fortinet
NETWORKING	
Form Factor	external
Connectivity Technology	wired
Data Link Protocol	Ethernet
Remote Management Protocol	CLI
Features	Stateful Packet Inspection (SPI)
Encryption Algorithm	SSL
Type	security appliance
Data Link Protocol	Ethernet
Features	Stateful Packet Inspection (SPI)

De lo anterior, es evidente que la convocante erróneamente tomó en consideración equipos que no corresponden al ofertado por mi mandante."

El Área Convocante, a través del Encargado del Despacho de la Administración de Recursos en Adquisiciones de Bienes y Servicios de la Gerencia de Proveeduría y Servicios del Instituto Mexicano del Petróleo, por medio de su oficio 350209/AA/393/2014 de nueve de septiembre del dos mil catorce, dio respuesta a los planteamientos hechos por las inconformes, manifestando entre otros puntos que el concepto "stateful" hace referencia a que los dispositivos de red que tienen esta naturaleza, mantiene un registro del estado de la conexión de la red y son capaces de mantener atributos significativos de cada conexión de la memoria. Estos atributos son colectivamente conocidos como el estado de la conexión. ----------

Que en su escrito de fecha diez de septiembre del dos mil catorce, la empresa Optimiti Network, S.A. de C.V., dio respuesta a los conceptos de ampliación hechos valer por la inconforme, reiterando que el equipo ofertado por las inconformes es un "Stateful". ----------

Finalmente, con fecha dieciocho de diciembre del dos mil catorce, se recibió en esta Área de Responsabilidades, escrito signado por el [redacted], en representación de

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.
Tel.: (55) 9175 8084 facosta@imp.mx

las inconformes, a través del cual formula sus alegatos, en el que expresó respecto a este punto lo siguiente: ----------

"...

A L E G A T O S

*1. El día **18 de junio de 2014** se publicó en COMPRANET la convocatoria para la licitación pública nacional mixta de servicios número LA-018T0O004-N152-2014, denominada "Convocatoria a la Licitación Pública, Electrónica, de carácter Nacional, a precio fijo, para la contratación del Servicio de Seguridad Perimetral para la red IMP." Y entre los requisitos se solicitó:*

a) En la convocatoria foja 44 V) punto 1 se precisó:

"V) Sistema de Protección de la Disponibilidad y mitigación de ataques DDoS.
1) El sistema debe ser un appliance dedicado a proporcionar disponibilidad por lo que no se aceptaran dispositivos que mantengan el estado de la conexión como firewall, sistemas de prevención y detección y las variantes o combinaciones como UTM, NGFW NGIPS ya que al conservar el estado de la conexión son por si mismos susceptibles a DDoS."

*Los equipos **FortiDDoS 400B y Fortianalyzer 300E** ofertados por mi representada si cumplen con las características requeridas, lo que se demuestra con las especificaciones técnicas de éstos, en donde se advierte que los éstos si cuentan con las características solicitadas por el área convocante, de conformidad con lo siguiente:*

***El equipo Fortinet FortiDDoS 400B, no mantiene el estado de la conexión tal y como se advierte de la página de internet** http://docs-legacy.fortinet.com/fddos/4-1-0 index.html/#page/fortiDDos_Handbook/differences_and_simularities.html, página en donde se precisan las diferencias entre un firewall de estado y un sistema de Análisis de Comportamiento de estado de Red (NBA) tal como FortiDDoS. Los firewalls convencionales tienen reglas que permiten o niegan paquetes o conexiones individuales en función de sus características individuales. El FortiDDoS opera sobre una base agregada que observa las tasas de paquetes, normalmente dentro de un segundo, durante un periodo de tiempo y mide las tasas de paquetes para varios parámetros de capa y compara frente a umbrales establecidos para ellos, si la tasa supera el umbral, las bloquea durante un periodo configurado.*

El funcionamiento del equipo FortiDDoS se puede consultar en esta liga http://docs-legacy.fortinet.com/fddos/4-1-0-index.html/#page/FortiDDos_handbook/strategies_for_protection.html. en donde se aprecia que las mejores estrategas de seguridad abarcan personas, operaciones y tecnología, toda vez que de conformidad con las probanzas ofrecidas se podrá advertir que el FortiDDoS efectúa un análisis convencional del comportamiento de la red (NBA) al ser una solución basada en hardware y, a diferencia de las soluciones basadas en software, mantienen los niveles normales de procesamiento y transferencia de datos durante ataques de denegación de servicios. El diseño de hardware a la medida de FortiDDoS supervisa umbrales de todo tráfico y mide recuentos de paquetes y bytes, transiciones de estado, fragmentos, checksum, banderas, nuevas conexiones, pares de direcciones, etc., además de que para reconocer y prevenir ataques, FortiDDoS monitoriza decenas de parámetros para detectar cambios sutiles en el comportamiento del tráfico de red.

*En la probanza consistente en la página de internet http://www.cnet.com/products/fortianet-fortiddos-400b-security-applaince/specs/, se precisan las especificaciones técnicas del producto **Fortinet FortiDDoS 400B** en donde se señala que ese equipo NO mantiene el estado de la conexión, por lo que podrá advertir que la convocante no analizo debidamente las características de este equipo.*

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

...

Por lo que es evidente que del análisis que se efectúe de todas las documentales ofrecidas como pruebas por mi representada, así como de la instrumental de actuaciones, se podrá advertir que los equipos ofertados por mi representada sí cumplen con las características requeridas por la convocante, al ser un hecho notorio el que los equipos FortiDDoS 400B y Fortianalyzer 3500E cumplen con todas y cada una de las características solicitadas en la convocatoria, ya que el primero de estos no mantiene el estado de la conexión y el segundo de los referidos sí recibe logs de terceros al menos vía SYSLOG, WMI, ODBC e integración vía parsers personalizados, de lo que es evidente que los equipos ofrecidos por mi representada sí cumplen con las características precisadas en las bases de la licitación.

Ahora bien, por lo que se refiere a la prueba pericial ofrecida por la tercero interesada (Optimity) no acredita fehacientemente que en el peritaje realizado se haya efectuado un debido análisis de todas las características de los equipos ofrecidos por mi representada, ya que de haberlo realizado hubiera advertido que sí cumplen con las características requeridas en la convocatoria.

Aunado a esto, de los peritajes ofrecidos por los peritos terceros de la PGR no se advierte que se hayan analizado debidamente todas las documentales que se encuentran en el expediente al basarse únicamente en las páginas de internet http://www.fortinet.com/sites/default/files/productdatas/sheets/FortiDDos-100B.pdf y http://www.fortinet.com/sites/default/files/productdatas/sheets/FortiDDos-3500E.pdf no efectuando un análisis de todas las documentales de donde se advierten con claridad todas y cada una de las características de los equipos ofertados, por lo que no se puede llegar a una conclusión tajante sin analizar todos los documentos en los que se precisen todas y cada una de las características de los equipos ofertados.

Por último, es importante precisar que el perito que efectúa la traducción de las páginas de internet cae en diversas contradicciones al precisar en el inicio del peritaje que:

> *"Es importante señalar que la perito que emite este dictamen no es experto en terminología de redes y telecomunicaciones, específicamente seguridad de redes, que es al materia sobre la que versa la documentación materia de los cuestionamientos. Además, cabe mencionar que no es materia de la especialidad en traducción emitir una opinión sobre cuestionamientos relacionados con el funcionamiento, características o aplicaciones de un dispositivo de este tipo o con respecto al cumplimiento de las bases de una licitación pública. En todo caso estos cuestionamientos deberán remitirse a un perito o experto en seguridad de redes informáticas.*
>
> *Con las salvedades antes expuestas, la perito que suscribe procedió a realizar una investigación sobre los términos controvertidos tanto en fuentes escritas como en fuentes electrónicas por internet para posteriormente emitir una opinión sobre cada punto."*

Y al finalizar el peritaje precisa:

> *"En conclusión, la inconforme, en el documento en cuestión evita y omite el término "stateful", ya que precisamente este es la palabra clave que define al dispositivo FortiDDoS como stateful y que por consecuencia sabemos que al mantener el estado de la conexión dicha inconforme en su propuesta no cumple con lo solicitado en las bases."*

De lo que se advierte que efectúa una conclusión que no debe ser tomada en consideración ya que a su decir no es experto en seguridad de redes informáticas sino en traducción de documentos e

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

indebidamente concluye que los equipos ofrecidos por mi representada no cumplen con las características de la convocatoria."

Por su parte, la empresa Optimiti Network, S.A. de C.V., mediante su escrito de fecha dieciséis de diciembre del dos mil catorce, formuló sus alegatos, expresando que con base a la documentación presentada por las inconformes, así como lo encontrado públicamente sobre los dispositivos Fortinet, FortiDDoS 400B, éstos son dispositivos que mantienen un estado de cada conexión y son "stateful" y mantiene una conexión similar a un firewall, incumpliendo con lo solicitado en las bases; señala además que las inconformes se condujeron con dolo desde la promoción de la inconformidad, ya que en la traducción de los documentos, se evitó y omitió el término original "stateful", al ser precisamente esta la palabra clave que define al dispositivo FortiDDoS como "stateful" y que por consecuencia al mantener el equipo que ofertaron el estado de la conexión, las inconformes en su propuesta no cumplían con lo solicitado en la convocatoria. ----------

Visto lo anterior, las empresas inconformes Servicios Alestra, S.A. de C.V., Alestra S. de R.L. de C.V., y SK Holdings, S.A. de C.V., esencialmente expresan que la convocante desechó la propuesta que de manera conjunta presentaron, al determinar que su equipo FortiDDoS 400B, no cumple con las características técnicas solicitadas en la convocatoria para la Licitación Pública Electrónica de Carácter Nacional a precio fijo, para la contratación del Servicio de Seguridad Perimetral para la Red IMP, No. LA-018T0O004-N152-2014, por lo que el fallo revela falta de exhaustividad al hacer el estudio cualitativo del equipo, al no tomar en consideración las convenciones establecidas en el handbook del equipo FortiDDoS 400B, además de que el citado equipo es una solución basada en hardware de la NBA y la diferencia de las soluciones basadas en software, mantiene los niveles normales de procesamiento y transferencia de datos durante ataques de denegación de servicio, pero no mantiene el estado de la conexión, de modo que no incumple las condiciones de la convocatoria. ----------

Precisado lo anterior, esta Autoridad considera que resulta pertinente transcribir lo dispuesto por el párrafo tercero del artículo 134 de la Constitución Política de los Estados Unidos Mexicanos, que a la letra dice: ----------

"Artículo 134. ...

...

Las adquisiciones, arrendamientos y enajenaciones de todo tipo de bienes, prestación de servicios de cualquier naturaleza y la contratación de obra que realicen, se adjudicarán o llevarán a cabo a través de licitaciones públicas mediante convocatoria pública para que libremente se presenten proposiciones solventes en sobre cerrado, que será abierto públicamente, a fin de asegurar al Estado las mejores condiciones disponibles en cuanto a precio, calidad, financiamiento, oportunidad y demás circunstancias pertinentes."

De lo anterior, podemos decir que la licitación es el procedimiento a través del cual la Administración Pública elige a la persona física o moral, que le ofrece las condiciones más convenientes en cuanto a precio, calidad, financiamiento, oportunidad, eficiencia, eficacia y

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

honradez, para celebrar un contrato determinado, y para ello hace un llamado a los particulares de manera impersonal para que participen, y en su caso formulen sus ofertas a fin de llevar a cabo la contratación. ----------

Por su parte, el artículo 36 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, establece lo siguiente: ----------

"...

ARTICULO 36. LAS DEPENDENCIAS Y ENTIDADES PARA LA EVALUACION DE LAS PROPOSICIONES DEBERAN UTILIZAR EL CRITERIO INDICADO EN LA CONVOCATORIA A LA LICITACION.
EN TODOS LOS CASOS LAS CONVOCANTES DEBERAN VERIFICAR QUE LAS PROPOSICIONES CUMPLAN CON LOS REQUISITOS SOLICITADOS EN LA CONVOCATORIA *A LA LICITACION; LA UTILIZACION DEL CRITERIO DE EVALUACION BINARIO, MEDIANTE EL CUAL SOLO SE ADJUDICA A QUIEN CUMPLA LOS REQUISITOS ESTABLECIDOS POR LA CONVOCANTE Y OFERTE EL PRECIO MAS BAJO, SERA APLICABLE CUANDO NO SEA POSIBLE UTILIZAR LOS CRITERIOS DE PUNTOS Y PORCENTAJES O DE COSTO BENEFICIO. EN ESTE SUPUESTO, LA CONVOCANTE EVALUARA AL MENOS LAS DOS PROPOSICIONES CUYO PRECIO RESULTE SER MAS BAJO; DE NO RESULTAR ESTAS SOLVENTES, SE EVALUARAN LAS QUE LES SIGAN EN PRECIO.*

..."

De la lectura a dicho precepto legal se establece la obligación por parte de la convocante de verificar que todas las proposiciones presentadas dentro de un proceso licitatorio, cumplan con los requisitos solicitados en la convocatoria. ----------

Ahora bien, con fecha dieciocho de junio de dos mil catorce, fue publicada en el Diario Oficial de la Federación y en el Sistema Electrónico Compranet, la convocatoria a la Licitación Pública Electrónica de Carácter Nacional a precio fijo, para la Contratación del Servicio de Seguridad Perimetral para la Red del IMP, No. LA-018T0O004-N152-2014, que en su Apartado II, Anexo Técnico, numeral 1 "Descripción del Servicios de Seguridad Perimetral", punto 6; indicó lo siguiente: ----------

"...

6. Sistema perimetral de Protección de la Disponibilidad y mitigación de ataques de DDoS que deberá de ser un appliance dedicado por lo que no se aceptaran dispositivos que mantengan el estado de la conexión como firewall, sistemas de prevención y detección de intrusiones y las variantes o combinaciones como UTM, NGFW, NGIPS y deberá ser conectado directamente después del cable que proporciona el ISP, o en defecto, podrá conectarse después del router. La solución propuesta podrá ser de la misma o diferente marca que el sistema de seguridad tipo firewall. En caso de ser marca distinta al sistema de seguridad perimetral, podrá administrase fuera de la solución."

Documental que se valora de conformidad con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción II, 197 y 202 del Código Federal de Procedimientos Civiles, ambas disposiciones de aplicación supletoria

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.
Tel.: (55) 9175 8084 facosta@imp.mx

en materia administrativa, del que se desprende que la convocante señaló que no se aceptarían *"... dispositivos que mantengan el estado de la conexión como firewall, sistemas de prevención y detección de intrusiones y las variantes o combinaciones como UTM, NGDW, NGIPS...."* ----------

Asimismo, en la convocatoria de la licitación pública en comento, en el Apartado II, Anexo Técnico, Apéndice A "Especificaciones Técnicas por tipo firewall de nueva generación", Inciso V) "Sistema de Protección de la Disponibilidad y mitigación de ataques DDoS", en su punto 1, mencionó: ----------

"...

1) El sistema deberá ser un appliance dedicado a proporcionar disponibilidad por lo que no se aceptaran dispositivos que mantengan el estado de la conexión como firewall, sistemas de prevención y detección y las variantes o combinaciones como UTM, NGDW, NGIPS ya que al conservar el estado de la conexión son por sí mismos susceptibles a DDoS."

Documental que se valora de conformidad con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción II, 197 y 202 del Código Federal de Procedimientos Civiles, ambas disposiciones de aplicación supletoria en materia administrativa, del que se desprende que la convocante estableció como requisito que **no se aceptarían "... dispositivos que mantengan el estado de la conexión como firewall, sistemas de prevención y detección y las variantes o combinaciones como UTM, NGDW, NGIPS ya que al conservar el estado de la conexión son por sí mismos susceptibles a DDoS."** ----------

Que en el fallo de fecha once de julio del dos mil catorce, emitido por el Encargado del Despacho de la Administración de Recursos en Adquisiciones de Bienes y Servicios de la Gerencia de Proveeduría y Servicios del Instituto Mexicano del Petróleo, señaló lo siguiente respecto de la propuesta presentada de manera conjunta por las empresas Alestra, S. de R.L. de C.V., SK Holdings, S.A. de C.V., y Servicios Alestra, S.A. de C.V.: ----------

"No cumple técnicamente con lo siguiente:

En las siguientes referencias del anexo técnico de la convocatoria se solicitó:

1. ***Descripción del servicio de seguridad perimetral para la red IMP, punto 6.***
   *"El sistema deberá ser un appliance dedicado a proporcionar disponibilidad por lo que **no se aceptarán dispositivos que mantengan el estado de la conexión** como firewall, sistemas de prevención y detección y las variantes o combinaciones como UTM, NGFW, NGIPS ya que al conservar el estado de la conexión con por sí mismos susceptibles a DDoS.*

V) Sistema de Protección de la Disponibilidad y mitigación de ataques de DDoS, punto 1
*"El sistema deberá de ser un appliance dedicado a proporcionar disponibilidad **por lo que no se aceptarán dispositivos que mantengan el estado de la conexión** como firewall, sistemas de prevención y detección y las variantes o combinaciones como UTM, NGFW, NGIPS ya que al conservar el estado de la conexión son por sí mismos susceptibles a DDoS.*

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.
Tel.: (55) 9175 8084 facosta@imp.mx

En ambas se solicita "que no se aceptaran dispositivos que mantengan el estado de la conexión"

Y el licitante está ofertando dispositivos que mantiene el estado de la conexión *(FortiDDoS 400B) ya que es stateful (mantiene el estado de la conexión) como lo indica en su página FORTINET*

http://docs-legacy.fortinet.com/fddos/4-1-0/index.html#page/FortiDDoS_Handbook/basic_topology.html

..."

Documental pública que se valora de conformidad con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción II, 197 y 202 del Código Federal de Procedimientos Civiles, ambas disposiciones de aplicación supletoria en materia administrativa, del que se desprende que la convocante señaló que la propuesta presentada por las inconformes, no cumplía con lo solicitado en la convocatoria de la Licitación Pública Electrónica de Carácter Nacional a precio fijo, para la Contratación del Servicio de Seguridad Perimetral para la Red del IMP, No. LA-018T0O004-N152-2014, ya que el equipo FortiDDoS 400B que se ofertó es un dispositivo "Stateful" (que mantiene el estado de la conexión). ----------

Como se indicó en la multicitada convocatoria, no se aceptarían dispositivos que mantuvieran el estado de la conexión, esto es "Stateful", para tal efecto esta Autoridad considera pertinente remitirse a los dictámenes periciales emitidos por el [redacted], perito presentado por la empresa Optimiti Network, S.A. de C.V., quién en su comparecía de aceptación y protesta del cargo ante esta Autoridad, exhibió Cédula Profesional número [redacted] expedida a su favor por la Dirección General de Profesiones de la Secretaría de Educación Pública, que lo acredita como Licenciado en Ingeniería Cibernética y en Sistemas Computacionales; así como por el [redacted], perito presentado por las empresas inconformes, quién en su comparecía de aceptación y protesta del cargo ante esta Autoridad, exhibió Cédula Profesional número [redacted] expedida a su favor por la Dirección General de Profesiones de la Secretaría de Educación Pública, que lo acredita como Licenciado en Ingeniería en Electrónica y Comunicaciones, con lo que acreditaron que ambos cuentan con los conocimientos necesarios para emitir su opinión respecto al punto en controversia, dictámenes en los que señalan lo siguiente: ----------

El [redacted], perito en Materia de Ingeniería Cibernética, Sistemas Computacionales y Seguridad de la Información, nombrado por Optimiti Network, S.A de C.V., manifestó en su dictamen del trece de octubre del dos mil catorce, respecto a este tema lo siguiente: ----------

"...

Respuesta a las preguntas formuladas por el E.D Administración de Recursos en Adquisiciones de Bienes y Servicios de la Gerencia de Proveeduría y Servicios, Dirección de Finanzas y Administración del Instituto Mexicano del Petróleo.

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

1. *Que el perito describa el concepto "stateful" dentro del ámbito de la seguridad de la información.*

Mantener el estado de la conexión o también llamado por su nombre en inglés "stateful" significa que el dispositivo está manteniendo el registro de la conexión de otros dispositivos, ya que sea de forma temporal o en un largo periodo de tiempo.

Una conexión bajo este estado, es cuando cierta información sobre una conexión entre dos sistemas es retenida para un uso futuro. En algunos casos, la conexión se mantiene aun cuando dos sistemas no estén trasmitiendo información."

Dictamen pericial que se valora con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción IV, 197 y 211 del Código Federal de Procedimientos Civiles, ambas disposiciones de aplicación supletoria en materia administrativa, en el que indica que el concepto "stateful" significa que el dispositivo está manteniendo el registro de la conexión de otros dispositivos, ya sea de manera temporal o en un largo periodo de tiempo. ----------

Por su parte, el [redacted], perito en Materia de Telecomunicaciones, nombrado por las empresas inconformes, en su dictamen pericial del catorce de octubre del dos mil catorce, señaló al respecto: ----------

"...

Preguntas efectuadas por el área convocante del Instituto Mexicano del Petróleo a las preguntas de la Prueba Pericial presentada por Alestra S. de R.L. de C.V., al tenor de las cuales el perito rinde su peritaje para el cual fue propuesto:

a. Que describa el concepto de "stateful" dentro del ámbito de seguridad de la información

En materia de tecnologías de la información, se define como Stateful al registro, monitoreo o vigilancia continuo del estado de transmisión y recepción de paquetes de datos con relación a una o más conexiones interesantes (relevantes) para los efectos por los cuales el registro, monitoreo o vigilancia es realizado."

Dictamen pericial que se valora con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción IV, 197 y 211 del Código Federal de Procedimientos Civiles, ambas disposiciones de aplicación supletoria en materia administrativa, en el que indica que el concepto "stateful" en materia de tecnologías de la información, se define como el registro, monitoreo o vigilancia continuo del estado de transmisión y recepción de paquetes de datos con relación a una o más conexiones. ----------

De lo anterior se advierte, que dichos dictámenes coinciden en esencia de que existe transmisión de datos con una o más conexiones, sin embargo, únicamente el dictamen presentado por el perito de Optimiti Network, S.A. de C.V., hace referencia a que el estado de la conexión con otros dispositivos deberá mantenerse. ----------

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

En razón de lo anterior, esta Autoridad realizó las acciones pertinentes para llevar a cabo el desahogo de un peritaje emitido por un tercero, por lo que obra en el expediente el dictamen pericial emitido por los CC. Jorge Alberto Grande Arriola y José Héctor Cortes Becerril, el veinticinco de noviembre del dos mil catorce, peritos oficiales en materia de informática adscritos a la Procuraduría General de la República, quienes durante su comparecía de aceptación y protesta del cargo ante esta Autoridad, exhibieron Cédulas Profesionales con números [redacted] y [redacted] expedidas a su favor por la Dirección General de Profesiones de la Secretaría de Educación Pública, respectivamente, que acredita al primero como Licenciado en Ingeniería en Sistemas Computacionales, y al segundo como Licenciado en Ingeniería en Computación, con lo que se demuestra que ambos cuentan con los conocimientos necesarios para emitir su opinión respecto al punto en controversia y quienes dictaminaron lo siguiente: -

> ***"TERCERA**.- Que el perito describa el concepto de "stateful" dentro del ámbito de la seguridad de la información. **RESPUESTA:** La tecnología de inspección dinámica de paquetes (SPI – Stateful Packet Inspection), es una regla definida para la mayoría de los firewalls que se basa no solamente en las reglas definidas por el usuario (como el filtrado de paquetes), sino también en el contexto establecido por paquetes anteriores que pasaron a través del firewall. Stateful significa, que se guarda el estado de la conexión entre dispositivos en una tabla temporal la cual actualiza dependiendo del análisis que realiza a cada paquete."*

Dictamen pericial que se valora con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción IV, 197 y 211 del Código Federal de Procedimientos Civiles, ambas disposiciones de aplicación supletoria en materia administrativa, en el que se indica que "Stateful" significa que guarda el estado de la conexión entre dispositivos en una tabla temporal la cual actualiza dependiendo del análisis que realice a cada paquete. ----------

De lo anterior, se advierte que el dictamen pericial emitido por los CC. Jorge Alberto Grande Arriola y José Héctor Cortes Becerril, peritos oficiales en materia de informática de la Procuraduría General de la República, coincide con el dictamen pericial del [redacted], perito de la empresa Optimiti Network, S.A. de C.V., respecto a que los dispositivos "Stateful" mantienen el estado de la conexión. ----------

En razón de lo anterior, esta Autoridad puede determinar válidamente que el término "stateful" se refiere a que el dispositivo mantiene el estado de la conexión con otros dispositivos. -------

Ahora bien, de acuerdo a lo señalado por las inconformes, estas propusieron con motivo de su participación dentro de la Licitación Pública Electrónica de Carácter Nacional a precio fijo, para la Contratación del Servicio de Seguridad Perimetral para la Red del IMP, No. LA-018T0O004-N152-2014, el equipo FortiDDoS 400B de la marca Fortinet, el cual, conforme a lo señalado por las inconformes, cumple con las especificaciones solicitadas en la convocatoria, al señalar expresamente a fojas trece y catorce de su escrito de inconformidad que *"... De lo anterior se advierte que, contrario a lo considerado por la convocante, el equipo FortiDDoS ofertado por mi representada sí cumple con los requisitos por la convocatoria, pues el FortiDDoS es una*

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

solución basada en hardware de la NBA y la diferencia de las soluciones basadas en software, mantiene los niveles normales de procesamiento y transferencia de datos durante ataques de denegación de servicio, pero no mantiene el estado de la conexión, de modo que no incumple las condiciones de la convocatoria." ----------

Para tal efecto, la inconforme ofreció como prueba de su parte, la prueba pericial en Materia de Ingeniería en Electrónica y Comunicaciones, a cargo del Ingeniero [redacted] a efecto de que respondiera la siguiente pregunta: "*Cuáles son las funcionalidades del equipo FortiDDoS 400B y señalar si mantiene la conexión como firewall*"; perito que con fecha catorce de octubre del dos mil catorce, rindió su dictamen pericial, en el que señaló lo siguiente:

"1.- Cuáles son las funcionalidades del equipo FortiDDoS 400B y señalar si mantiene la conexión como Firewall?

FortiDDos es un dispositivo de seguridad de propósito específico que actúa como sistemas de prevención de anomalías de compartimiento de la Red o sus siglas en inglés (Network behavior anomaly prevention system) que detecta y bloquea los ataques de red que se caracterizan por el uso excesivo de los recursos de red y que son conocidos como ataque distribuido denegación de servicio (DDoS)

Este equipo y aquellos del fabricante Fortinet utiliza un enfoque 100%ASC personalizado para sus productos DDoS, lo que elimina la sobrecarga y los riesgos asociados con los sistemas híbridos /ASIC CPU o CPU. El sistema FortiDDoS opera con base de agregación, revisando las tasas de paquetes-típicamente de un segundo, por un periodo de tiempo. El procesador de tráfico FortiASIC-TP2 lleva a cabo la medición de la tasa de paquetes de varias capas 3, 4 y 7 así como parámetros y los compara contra umbrales fijados por cada uno de ellos.

Las principales Funcionalidades del FortiDDoS 400B se enumeran a continuación:

- *Detección Avanzada de Amenazas ante ataques conocidos y ataques de día cero ("zero days Attacks")*
- *100% protección ante ataques DDoS basado en Hardware*
- *Capacidad de Autoaprendizaje*
- *Protección Multicapa realizando la inspección y protección de paquetes en las capas 3,4 y 7 del modelo OSI*
- *Protección basada en la reputación de la IP origen*
- *Proceso de verificación Múltiple*
- *Mecanismos de prevención y mitigación de Ataques de inundación de tráfico (Ataques Flood) en las capas 3,4 y 7 del Modelo OSI*
- *Métricas del Monitoreo del Comportamiento*
- *Virtualización, ataques hacia un segmento de red protegido no impacta a otros segmentos de red*
- *Altas tasas de rendimiento de mitigación y detección de amenazas o ataques DDoS*

La siguiente liga sirve de referencia para la para la respuesta a esta pregunta.
http://fortinet.com/sites/default/files/productdatasheets/FortiDDos-1000B.pdf
páginas 2 y 3

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

El equipo FortiDDoS 400B, según su explicación técnica integral, utiliza técnicas de análisis con el fin de proteger los servidores contra ciertos ataques DDoS para los cuales es necesario entender o inspeccionar el estado de la conexión. Este equipo de la familia FortiDDoS, no añade información a la tabla de conexión a menos que sea necesario y tiene diversas características de auto-protección para asegurarse de que la tabla de conexión y otros cuadros no sufran desbordamiento.

Una solución Anti-DDoS sería considerada como incompleta si no cuenta con mecanismos para analizar adecuadamente los estados de conexión y defenderse ante ataques contra las tablas de estado del dispositivo. Al observar las especificaciones técnicas del FortiDDoS 400B se advierten mecanismos que garantizan la seguridad de sus tablas internas por lo cual brinda protección ante ataques de inundación o flood attacks

En opinión nuestra, el análisis de estados se puede habilitar o deshabilitar por configuración en el dispositivo FoortiDDoS y el no tener IP pública hacia internet (debido a que opera en capa 2 del modelo OSI), lo convierte en un dispositivo al que no se le puede atacar directamente

La siguiente liga sirve de referencia para la respuesta a esta pregunta:

http/www.fortinet.com/sites/default/files/whitepapers/DDoS-AttacK-Mitigation-Demystified.pdf."

Dictamen pericial que se valora con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción IV, 197 y 211 del Código Federal de Procedimientos Civiles, ambas disposiciones de aplicación supletoria en materia administrativa, y cuyo dictamen es en el sentido de demostrar que el equipo FortiDDoS 400B, ofrecido por las inconformes dentro del proceso de la Licitación Pública Electrónica de Carácter Nacional a precio fijo No. LA-018T0O004-N152-2014, si cumplía con lo solicitado en la convocatoria, al ser un dispositivo que no mantiene el estado de la conexión. ----------

Como ya se dijo, dentro de la instancia de la inconformidad se dio vista a la empresa Optimiti Network, S.A. de C.V., en su calidad de tercero interesado para que designara a su perito, nombrando para tal efecto al C[redacted]a, quien con fecha trece de octubre del dos mil catorce, presentó su dictamen pericial en los siguientes términos: ----------

"...

Respuesta a las preguntas formuladas por la empresa Servicios Alestra, S.A. de C.V.

1. ¿Cuales son las funcionalidades del equipo FortiDDoS y señalar si mantiene la conexión como firewall?

Mediante una búsqueda en el sitio del fabricante Fortinet, así como búsquedas por el nombre del producto FortiDDoS en el buscador de Internet de Google en fecha ocho de octubre de dos mil catorce, apareciendo varios resultados, adicionalmente conociendo de la existencia de varios modelos de equipos comercializados por el fabricante, se procedió a buscar los documentos técnicos que contiene la información especifica del dispositivo propuesto en el proceso licitatorio que es el FortiDDoS 400B

Se encontró el documento público "FortiDDoS 4.1 Patch 2 Handbook(PDF)" en la siguiente dirección de internet, el cual también fue presentado por la empresa SERVICIOS ALESTRA, S.A. DE C.V. en el proceso licitatorio:

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

http://docs.fortinet.com/uploaded/files/2071/FortiDDoS_4_1_Patch_2_Handbook-Revision1.pdf

En dicho documento, en la página 20, el dispositivo FortiDDoS se define como un dispositivo de análisis de comportamiento de la red (NBA) de tipo "stateful", es decir que maneja el estado de la conexión.

Adicionalmente, se encontró el documento público de donde hace referencia al modelo FortiDDoS 400B en la siguiente dirección de internet, el cual también fue presentado por la empresa SERVICIOS ALESTRA, S.A. DE C.V. en el proceso licitatorio:
http://www.fortinet.com/sites/default/files/productdatasheets/FortiDDos-1000B.pdf

Las funcionalidades técnicas descritas en el documento, se encuentra en la página 3, donde se encuentran:

- *Tecnología de Inspección de Paquetes*
- *Proceso de verificación múltiple*
- *Mecanismos de Prevención de Inundación (de paquetes)*
- *Mitigación de Inundación (de paquetes) Capa 3*
- *Mitigación de Inundación (de paquetes) Capa 4*
- *Mitigación de Inundación (de paquetes) Capa 7*
- *Análisis de Reputación de IP*
- *Métricas de Monitoreo de Comportamiento*
- *Estadísticas de Reporteo*
- *Administración*
- *Reportes de Eventos Centralizados*
- *Trazas de Auditoria y Accesos*

Dentro del documento se puede observar que los dispositivos mencionan el término "stateful monitoring" dentro de la funcionalidad de "Tecnología de Inspección de Paquetes"

Mantener el estado de la conexión o también llamado por su nombre en inglés "stateful" significa que el dispositivo está manteniendo registro de la conexión de otros dispositivos, ya sea de forma temporal o en un largo periodo de tiempo.

Para poder realizar este tipo de monitoreo, es necesario que cierta de la información sobre una conexión entre dos sistemas es retenida para un uso futuro. La conexión se mantiene abierta aun cuando dos sistemas no estén transmitiendo información.

Dentro del documento de inconformidad, la empresa SERVICIOS ALESTRA, S.A. DE C.V., hace referencia en su página 5, que las características del equipo se encuentra en una página web ubicada en: http://docs-legacy.fortinet.com/fddos/4-1-1/index.html#page/FortiDDoS_Handbook/diferences_and_simularities.html .

En dicha página web, precisamente se encuentra que el FortiDDos toma en consideración la cantidad/tasas de paquetes dentro del periodo de tiempo. Lo cual indica claramente que debe de mantener una tabla o algún mecanismo para poder identificarlo.

Dentro del mismo documento, el cual se encuentra traducido por la inconforme en la página 6 de su inconformidad se lee:

"Hay algunas características en FortiDDos que son similares a un firewall"

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

Según la documentación, los equipos FortiDDoS, no solo mantienen un estado de cada conexión, sino que incluso SI mantienen una conexión similar a un firewall, el cual gracias a este registro puede determinar los paquetes que serán permitidos dentro del equipo."

Dictamen pericial que se valora con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción IV, 197 y 211 del Código Federal de Procedimientos Civiles, ambas disposiciones de aplicación supletoria en materia administrativa, y cuyo dictamen es en el sentido de demostrar que el equipo FortiDDoS 400B, ofrecido por las empresas inconformes dentro del proceso de la Licitación Pública Electrónica de Carácter Nacional a precio fijo No. LA-018T0O004-N152-2014, no cumplía con lo solicitado en la convocatoria, al ser un dispositivo que sí mantiene el estado de la conexión.

De lo anterior, se advierte que dichos dictámenes son contradictorios, toda vez que el dictamen del [redacted], perito presentado por las empresas inconformes, es en el sentido de que el equipo FortiDDoS 400B, ofrecido dentro del proceso de la Licitación Pública Electrónica de Carácter Nacional a precio fijo No. LA-018T0O004-N152-2014, sí cumplía con lo solicitado, al ser un dispositivo que no mantiene el estado de la conexión; en tanto qué, el dictamen del [redacted], ofrecido por la empresa Optimiti Network, S.A. de C.V., es en sentido contrario, esto es, que el equipo FortiDDoS 400B, sí mantiene el estado de la conexión, por lo cual no cumple con los requerimientos de la mencionada licitación. ----------

Al existir discordancia entre ambos dictámenes, esta Autoridad, como ya se mencionó, requirió el apoyo a la Procuraduría General de la República, para que a través de un perito tercero, se emitiera un dictamen sobre los hechos controvertidos, que en el caso, obra en el expediente en que se actúa, el dictamen pericial emitido por los CC. Jorge Alberto Grande Arriola y José Héctor Cortes Becerril, el veinticinco de noviembre del dos mil catorce, peritos oficiales en materia de informática adscritos a la Procuraduría General de la República, quienes dictaminaron lo siguiente: ----------

"...

***PRIMERA**.- Cuáles son las funcionalidades del equipo FortiDDoS 400B y señalar si mantiene la conexión como firewall?*

***RESPUESTA**: De manera general en la hoja de datos del fabricante FORTINET, que muestra toda la familia FortiDDoS, la cual se encuentra en la dirección de internet http://www.fortinet.com/sites/default/files/productdatasheets/FortiDDos-1000B.pdf, las funcionalidades de éste dispositivo son:*

- *Detección 100% basada en comportamiento del tráfico de la red.*
- *Protección contra ataques DDoS basada 100% en hardware.*
- *Evaluación continua contra ataques.*
- *Resistente al congestionamiento.*
- *Proceso de aprendizaje automatizado.*
- *Protección contra múltiples ataques.*
- *Capacidad de reporteo comprensivo.*
- *Tecnología de inspección dinámica de paquetes, también conocida como Stateful Monitoring.*

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

La tecnología de inspección dinámica de paquetes (SPI – Stateful Packet Inspection), es una regla definida para la mayoría de los firewalls que se basa no solamente en las reglas definidas por el usuario (como el filtrado de paquetes), sino también en el contexto establecido por paquetes anteriores que pasaron a través del firewall. Stateful significa, que se guarda el estado de la conexión entre dispositivos. El fortiDDoS 400B se comporta como un firewall al tener ésta característica.

...

***QUINTA**.- Que el perito indique si el aplicativo FortiDDoS 400B es "stateful" o no lo es, para cualquier sentido que responda ésta pregunta, deberá justificar los aspectos técnicos que lo llevan a dicha conclusión.*

***RESPUESTA**: De acuerdo a la hoja de datos técnicos del fabricante, claramente se especifica en la parte de Tecnología de Filtrado de Paquetes, que lleva a cabo un monitoreo por inspección dinámica de paquetes o Stateful Monitoring, lo que es el claro indicio de que el dispositivo trabaja bajo esta tecnología."*

Dictamen pericial que se valora con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción IV, 197 y 211 del Código Federal de Procedimientos Civiles, ambas disposiciones de aplicación supletoria en materia administrativa, en el que se indica que el dispositivo FortiDDoS 400B, ofrecido por las empresas inconformes, es un equipo "Stateful", en ese tenor es un dispositivo que mantiene el estado de la conexión, el cual trabaja bajo esa tecnología. ----------

De lo anterior, se advierte que el dictamen pericial emitido por los CC. Jorge Alberto Grande Arriola y José Héctor Cortes Becerril, peritos oficiales en materia de informática de la Procuraduría General de la República, coincide con el dictamen pericial del [redacted], perito presentado por parte de la empresa Optimiti Network, S.A. de C.V., en el sentido de que el dispositivo FortiDDoS 400B, es un equipo "Stateful", siendo un dispositivo que si mantiene el estado de la conexión. ----------

Adicionalmente, las inconformes para demostrar que el dispositivo FortiDDoS 400B, que propusieron dentro de la Licitación Pública Electrónica de Carácter Nacional a precio fijo No. LA-018T0O004-N152-2014, si cumplía con lo solicitado, al ser un dispositivo que no mantiene el estado de la conexión, ofrecieron como pruebas a su favor la traducción del inglés al castellano de las siguientes páginas de Internet. ----------

http://www.cnet.com/products/fortinet-fortidos-400b-security-appliances/specs

Documental privada que se valora con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción III, 197 y 203 del Código Federal de Procedimientos Civiles, traducción con la que las inconformes pretenden acreditar las especificaciones técnicas del producto Fortinet FortiDDoS 400B.----------

http://docs-legacy.fortinet.com/fddos/4-1-0/index.html#page/FortiDDos_Handbook/basic_topology:html

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

Documental privada que se valora con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción III, 197 y 203 del Código Federal de Procedimientos Civiles, traducción que las inconformes refieren que *"en esta página de internet se conecta entre los sistemas protegidos pudiéndose añadir un interruptor derivante para evitar las fallas en la vía de datos protegiendo los servidores"* --------

http://www.fortinet.com/sites/default/files/productdatasheets/FortiDDos-1000B.pdf.

Documental privada que se valora con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción III, 197 y 203 del Código Federal de Procedimientos Civiles, traducción con las que las inconformes pretenden demostrar que este producto es eficaz en la denegación de servicios distribuidos DDoS. -----

Ahora bien, esta Autoridad, dio vista de dichas traducciones tanto al Área Convocante del Instituto Mexicano del Petróleo, como a la empresa Optimiti Network, S.A. de C.V., quienes manifestaron su desacuerdo respecto a la traducción exhibida por las inconformes. ----------

Esto es, a través del oficio 350209/AA/516/ 2014 del treinta y uno de octubre del dos mil catorce, el Encargado del Despacho de la Administración de Recursos en Adquisiciones de Bienes y Servicios, remitió a esta Autoridad la opinión de la Gerencia de Tecnologías de la Información, ambas del Instituto Mexicano del Petróleo, a la traducción de los documentos ofrecidos por las inconformes, en los siguientes términos: ----------

"...

Respecto a la traducción hecha al documento llamado "Topología básica para FortiDDoS" contenido en la página web http://docs-legacy.fortinet.com/fddos/4-1-0/index.html#page/FortiDDos_handbook/basic_topology.html (anexo 3), misma información que fue anexada a su propuesta por el inconforme.

La cual en su página 54 de 290 indica en inglés

> *Because the FortiDDoS appliance is stateful and bidirectional, the date packet traffic is discribed as either incoming (inbound) and outgoing (outbound).*

Lo cual están traduciendo como "Debido a que el aparato FortiDDoS tiene control y es bidireccional....." indicando que stateful se traduce como control, lo cual no es aceptado ya que este término se refiere a mantener el estado, lo cual el mismo inconforme traduce en el documento FortiDDoS TM, dispositivo de mitigación de ataques DDoS en su página web http://www.fortinet.com/sites/default/files/productdatasheets/fortiDDos-1000B.pdf (anexo 4), en su página tercera en el apartado de características "stateful monitoring" como supervisión del estado, así también la traducción del documento "Especificaciones del dispositivo de seguridad Fortinet FortiDDoS 400B contenido en la página web http://www.cnet.com/products/fortinet-Fortidos-400b-security-appliances/specs (Anexo 5) de la página 3 en su inciso 3, de su traducción, llamando características "stateful packet inspectión (SPI)" lo traduce como "inspección del estado completo de paquetes (SPI)", relacionando nuevamente el concepto stateful como mantener el estado y no como lo traduce en la topología como control siendo incongruente en sus conceptos la inconforme."

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

Documental pública que se valora con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción II, 197 y 202 del Código Federal de Procedimientos Civiles, con la que el Área Convocante manifiesta su desacuerdo y expresa que existen contradicciones en la traducción del concepto "Stateful", señalando que no es aceptado que "Stateful" sea traducido como control. ----------

Por su parte, la empresa Optimiti Network, S.A de C.V., a través de su Administrador Único, señaló mediante escrito del cuatro de noviembre del dos mil catorce, lo siguiente: ----------

"...

5. Respecto de la traducción del handbook de la solución FortiDDoS que a lo largo del proceso y que bajo la documentación formal siempre fue definida como

a. Because the FortiDDoS appliance is stateful and bidirectional, the date packet traffic is discribed as either incoming (inbound) and outgoing (outbound),

b. Referencia: http://docs-legacy.fortinet.com/fddos/4-1-0/index.html#page/FortiDDos_Handbook/basic_topology.html

Es importante hacer notar que la traducción presentada "no solo omite sino que presenta una traducción errónea para el texto "is stateful", ya que fue definida como:

c. Debido a que el aparato FortiDDoS tiene control y es bidireccional, el tráfico del paquete de datos se describe ya sea como entrante (Inbound) y saliente (outbound)

***En conclusión**, la inconforme en el documento en cuestión evita y omite el término original "stateful", ya que precisamente esta es la palabra clave que define al dispositivo FortiDDoS como "stateful" y que por consecuencia sabemos que al mantener el estado de la conexión, dicha inconforme en su propuesta NO CUMPLE con lo solicitado en bases."*

Documental privada que se valora con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción III, 197 y 203 del Código Federal de Procedimientos Civiles, con la que la empresa Optimiti Network, S.A. de C.V., en su calidad de tercero interesado, manifiesta su desacuerdo respecto a la traducción del concepto "stateful", señalando que la inconforme evita y omite el término original de "stateful", por lo que al mantener el estado de la conexión, no cumple con lo solicitado en la licitación. ----------

En ese tenor, esta Autoridad solicitó el apoyo de la Procuraduría General de la República, requiriéndole realizara la traducción al castellano de los puntos sobre los cuales tanto el Área Convocante del Instituto Mexicano del Petróleo, como la empresa Optimiti Network, S.A. de C.V., manifestaron su desacuerdo respecto a la traducción exhibida por las inconformes. ------

Por lo que con fecha cuatro de diciembre del dos mil catorce, se recibió en esta Área de Responsabilidades el oficio con número de folio 81898 del veintiocho de noviembre del mismo año, suscrito por la C. Rosa María Cervantes Negrete, perito traductor del Departamento de Traducción, Dirección General de Especialidades Periciales Documentales de la Procuraduría

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

General de la República, a través del cual emite el dictamen que le fue solicitado a dicha Procuraduría, y que rindió en los siguientes términos: ----------

"

...

PRIMERA PARTE

A continuación cito en el orden en que aparecen los cuestionamientos por parte del Instituto Mexicano del Petróleo (en lo sucesivo el IMP), incluidos en el manifiesto de fecha 30 de octubre de 2014. El primer cuestionamiento se dividió en dos incisos A) y B) para mayor claridad

...

TERCER CUESTIONAMIENTO

"Respecto a la traducción hecha al documento llamado "Topología básica para FortiDDoS contenido en la página web http://docs-legacy.fortinet.com/fddos/4-1-0-index.html/#page/fortiDDos_handbook/basic_topology.html (anexo 3), misma información que fue anexada a su propuesta por el inconforme como…

La cual en su página 54 de 290 indica en inglés.

> *Because the FortiDDoS appliance is stateful and bidirectional, the date packet traficc is described as either incoming (inbound) and outgoing (outbound)*

*Lo cual están traduciendo como "Debido a que el aparato FortiDDoS tiene control y es bidireccional….." indicando que stateful se traduce como control, lo cual no es aceptado ya que este término se refiere a mantener el estado, lo cual el mismo inconforme traduce en el documento FortiDDoS TM, dispositivos de mitigación de ataque de DDos en su página web http://www.fortinet.com/sites/default/files/productdatasheets/fortiddos-1000.pdf (anexo 4), en su página tercera en el apartado de características "stateful monitoring" como supervisión del estado, así también la traducción del documento "Especificaciones del dispositivo de seguridad Fortinet FortiDDos 400B contenido en la página web http://www.cnet.com/products/fortianet-fortiddos-400b-security-applaince/specs (anexo 5) de la página 3 en su inciso 3, de su traducción, llamado características "stateful packet inspection (SPI)", **lo traduce como "inspección del estado completo de paquetes (SPI)", relacionado nuevamente el concepto stateful con mantener el estado y no como lo traduce en la topología como control siendo incongruente en sus conceptos el inconforme.***

***Análisis del perito.** Según lo señalado en este tercer cuestionamiento, el termino stateful se localiza en la página 11 (que se repite en el anexo 3, página 42), fue traducido como "control" en la página 12; el mismo término se localiza en la página 19 primera columna tercer renglón (que se repite en el anexo 4, página 44) y se tradujo en la página 23 como "estado"; por último se localiza dos veces en la página 3 y es traducido en la página 8 como "estado completo" Se procedió a hacer una búsqueda del término stateful en internet por no haberse localizado en ninguna fuente escrita disponible. Se localizaron las siguientes fuentes: http://oracleapptechnology.blogspot.mx/2007/10/stateful-and-stateless-connections.html, http://www. paysontechnology.com/computer_network_security_glossary2/, estas dos páginas contienen la misma definición para stateful, que a la letra se transcribe:*

"Stateful and stateless are adjectives that describe whether a computer program is design to note and remember one or more preceding events in a given sequence of interactions a with a user, another

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

computer or program, a device, or other outside element. Stateful means the computer or program keeps track of the state of interaction, usally by setting values in a storage field designated for that purpuse"

La siguiente es la traducción de esta definición en español:

Stateful and stateless son adjetivos que describen si una computadora o un programa de computo está diseñado para notar y recordar uno o más eventos anteriores en una secuencia dada de interacciones con un usuario, otra computadora o programa, un dispositivo u otro elemento externo. Stateful significa que la computadora o el programa lleva un registro del estado de la interacción, normalmente fijando valores en un campo de almacenamiento diseñado para dicho fin.

Otra fuente http://sofware.dell.com/products/sonicwall-tz/#features de la marca de productos dell escrita en idioma inglés señala características de dispositivos como sigue:

Firewall Overview	***SonicWALL TZ 215 Series***	***SonicWALL TZ 215 Series***	***SonicWALL TZ 215 Series***
Stateful Packet Inspection Firewall	*S*	*S*	*S*
Deep Packet Inspection Firewall	*O*	*O*	*O*

Y en el sitio http://www.dell.com/mx/empresas/p/sonicwall-tz-series/pd en español aparece el mismo cuadro antes señalado en donde el término Stateful Packet Inspection, ubicado en el segundo renglón de la primera columna, es traducido como inspección de paquetes con estado:

Informacion general del firewall	***Serie TZ 215 de SonicWALL***	***Serie TZ 215 de SonicWALL***	***Serie TZ 215 de SonicWALL***
Firewall de inspección de paquetes con estado	*S*	*S*	*S*
Firewall de inspección profunda de paquetes	*O*	*O*	*O*

Por otra parte, fuentes electrónicas consultadas en español como son www.zonassystem.com/2012/06/tipos-de-firewall-de-red... [Tipos de firewall de red: Stateless, Stateful, SPI, AIC, SPI ...], http://www.cisco.com/c/dam/en/us/td/docs/routers/csbr/rv180w/administration/guide/rv180w_admin_es.pdf y www.computerwoldmexico.mx/Articulos/18629 traducen stateful como "estado" y "de estado".

Opinión del perito. *En la traducción analizada el término staeful fue traducido de tres formas distintas: control, estado y estado completo. Sin embargo, con base en las fuentes consultadas, stateful no debería traducirse como control y, en todo caso podría traducirse como "con estado".*

SEGUNDA PARTE

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

Ahora procedo a emitir mi opinión sobre las observaciones vertidas por el Administrador Único de OPTIMITI NETWORK, S.A. de C.V. en documento sin fecha con sello de recibido en la función pública el 4 de noviembre del presente año.

A continuación cito una por una dichas observaciones para realizar un análisis y emitir una opinión.

...

***5.-** "Respecto a la traducción del handbook de la solución FortiDDos que a lo largo del proceso y que bajo la documentación formal siempre fue definida como:*

a. ***Because the FortiDDoS appliance is stateful and bidirectional, the data packet traffic is described as either incoming (inbound) and outgoing (outbound).***
b. ***Referencia:*** *http://docs-legacy.fortinet.com/fddos/4-1-0-index.html/#page/ FortiDDos Handbook/basic topology.html.*

Es importante hacer notar que la traducción presentada "no solo omite sino que presenta una traducción errónea para el texto "is stateful" ya que fue definida como:

Debido a que el aparato FortiDDos tiene control y es bidireccional, el tráfico del paquete de datos se describe ya sea como entrante (inbound) y saliente (outbound).

***En conclusión,** la inconforme en el documento en cuestión evita y omite el termino original "stateful" ya que precisamente esta es la palabra clave que define al dispositivo FortiDDos como "stateful" y por consecuencia sabemos que al mantener el estado de la conexión, dicha inconforme en su propuesta NO CUMPLE con lo solicitado en las bases."*

***Análisis del perito.** Se realizó el mismo análisis del término "stateful" señalado el tercer cuestionamiento del IMP el cual se da por reproducido a la letra en esta parte. En cuanto a la última parte de la observación 5, arriba transcrita, que la Administradora Única de OPTIMITI NETWORK, S.A. de C.V. hace a manera de conclusión, no puede analizarse puesto que no es materia de la especialidad de traducción.*

***Opinión del perito.** Con base en las fuentes consultadas, stateful no debería traducirse como "control" y, en todo caso, podría traducirse como "con estado". En cuanto a la última parte de la observación que fue vertida a manera de conclusión, no es materia de traducción determinar el cumplimiento o incumplimiento con las bases de licitación en cuestión."*

Documental pública que se valora con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción II, 197 y 202 del Código Federal de Procedimientos Civiles, de la que se advierte que la C. Rosa María Cervantes Negrete, personal de la Procuraduría General de la República, al emitir su dictamen en traducción, refiere que con base a las fuentes consultadas "stateful" no debe traducirse como control y que en todo caso, podría traducirse como "con estado". ----------

En ese tenor, la traducción hecha por la C. Rosa María Cervantes Negrete, perito traductor, es acorde con el dictamen pericial rendido por los CC. José Héctor Cortés Becerril y Jorge Alberto Grande Arriola, peritos oficiales en materia de Informática, todos ellos adscritos a la Procuraduría General de la República, respecto a la traducción que debe dársele al término

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

"stateful" quienes en su dictamen contenido en oficio con número de folio 76311 del veinticinco de noviembre del dos mil catorce, manifiestan lo siguiente: ----------

> ***"TERCERA**.- Que el perito describa el concepto de "stateful" dentro del ámbito de la seguridad de la información. **RESPUESTA:** La tecnología de inspección dinámica de paquetes (SPI – Stateful Packet Inspection), es una regla definida para la mayoría de los firewalls que se basa no solamente en las reglas definidas por el usuario (como el filtrado de paquetes), sino también en el contexto establecido por paquetes anteriores que pasaron a través del firewall. Stateful significa, que se guarda **el estado** de la conexión entre dispositivos en una tabla temporal la cual actualiza dependiendo del análisis que realiza a cada paquete."*

Por lo anterior, de acuerdo a las evidencias probatorias antes señaladas, el término "stateful" está referido a que el equipo guarda el estado de la conexión con otro dispositivo. ----------

Lo anterior se correlaciona con la matriz de cumplimiento presentada por las empresas inconformes como parte de su propuesta técnica con motivo de su participación dentro de la Licitación Pública Electrónica de Carácter Nacional a precio fijo No. LA-018T0O004-N152-2014, en la que respecto al numeral V) Sistema de Protección de Disponibilidad y mitigación de ataques de DDoS, en la que las inconformes en el punto 15, subinciso 3, páginas 21, 23 y 24 señalaron lo siguiente: ----------

"...

Matriz de cumplimiento

		Cumple/No cumple	Documento	Hoja /columna/Reglón	Párrafo	Referencia	Traducción simple al Español
V) Sistema de Protección de la Disponibilidad y mitigación de ataques de DDoS							
...							
15) Realizar la detección y protección de ataques de Red como:							
...							
3 Contratación contra malformación de paquetes		Si	FortiDDoS 1000B	Hoja 3, Renglon 1, Sección Futures	Packet Inspection Technology	Packet Inspection Technology Granular Packet Inspection Stateful Monitoring Continuos Adaptive Rate Limiting Heuristic Analysis Predictive Behavioral Analysis	Packet Inspection Technology Granular Packet Inspection Stateful Monitoring Continuos Adaptive Rate Limiting Heuristic Analysis Predictive Behavioral Analysis

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

Documental privada que se valora con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción III, 197 y 203 del Código Federal de Procedimientos Civiles, de la que se advierte que las inconformes **omitieron realizar la traducción al español de dicho párrafo,** en el que se encontraba el término "Stateful Monitoring", siendo precisamente el término "stateful" el punto en controversia, es decir, si el equipo mantiene el estado de la conexión, y que como quedó señalado en la convocatoria, no se aceptarían equipos que tuvieran esta característica. --------

Es de resaltar por parte de esta Autoridad la conclusión VIGÉSIMAOCTAVA del dictamen en informática rendido por los CC. José Héctor Cortés Becerril y Jorge Alberto Grande Arriola, peritos oficiales en materia de Informática, adscritos a la Procuraduría General de la República, contenido en su oficio con número de folio 76311 del veinticinco de noviembre del dos mil catorce, y recibido en esta Área de Responsabilidades en la misma fecha, en el que concluyen lo siguiente: ----------

*"**CONCLUSIONES***

...

***VIGÉSIMAOCTAVA.-** Determinar si los equipos que fueron ofertados por la inconforme cumplen técnicamente con requerimientos solicitados en Licitación Pública Electrónica de Carácter Nacional a precio fijo NO. LA-018T0O004-N152-2014, convocada por el Instituto Mexicano del Petróleo*

***RESPUESTA:** De acuerdo al punto V) de la convocatoria de la Licitación Pública Electrónica de Carácter Nacional a precio fijo NO. LA-018T0O004-N152-2014, en su página 44, inciso 1), donde a la letra se detalla: "El sistema deberá de ser un appliance dedicado a proporcionar disponibilidad por lo que no se aceptarán dispositivos que mantengan el estado de la conexión como firewall, sistemas de prevención y detección y las variantes o combinaciones como UTM, NGFW, NGIPS ya que al conservar el estado de la conexión son por sí mismos susceptibles a DDoS", derivado de ello y considerando todas las respuestas correspondientes al dispositivo FortiDDoS 400B, éste es un dispositivo stateful, es decir que mantiene el estado de la conexión y se comporta como firewall, tal y como se indica en la hoja de datos proporcionada por el fabricante, por lo que se concluye que éste producto no cumple con las especificaciones técnicas solicitadas."*

Dictamen pericial que se valora con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción IV, 197 y 211 del Código Federal de Procedimientos Civiles, ambas disposiciones de aplicación supletoria en materia administrativa, en el que los CC. José Héctor Cortés Becerril y Jorge Alberto Grande Arriola, peritos oficiales en materia de informática, adscritos a la Procuraduría General de la República, **concluyen que el equipo FortiDDoS 400B ofertado por las inconformes, es un dispositivo "stateful", es decir que mantiene el estado de la conexión y se comporta como firewall, tal y como se indica en la hoja de datos proporcionada por el fabricante, concluyendo que éste producto no cumple con las especificaciones técnicas solicitadas**. ----------

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

Por otra parte, las inconformes plantean en su escrito de alegatos, que su equipo FortiDDoS 400B, no mantiene el estado de la conexión, tal y como se advierte de la páginas de internet que menciona, situación que no fue demostrada como ha quedado precisado en párrafos anteriores. ----------

Agregan las inconformes, que el perito de la empresa Optimiti Network, S.A. de C.V., no realizó un debido análisis de todas características de los equipos ofertados por las inconformes, y que los peritos de la Procuraduría General de la República, no revisaron la totalidad de documentales que se encuentran en el expediente basándose únicamente en dos páginas de Internet; al respecto, como se indicó en párrafos anteriores, los peritos de la empresa Optimiti Network, S.A. de C.V., así como de la Procuraduría General de la República, acreditaron ante esta Autoridad, a través de las cédulas profesionales que les expidió la Dirección General de Profesiones, que cuentan con los conocimientos necesarios para emitir sus dictámenes. ------

Aunado a lo anterior, con fecha cuatro de noviembre del dos mil catorce, comparecieron ante esta Autoridad los CC. José Héctor Cortés Becerril y Jorge Alberto Grande Arriola, peritos oficiales en materia de Informática, adscritos a la Procuraduría General de la República, diligencia en la que éstos aceptaron y protestaron el cargo como peritos, en la que se hizo constar que se ponía a su disposición el expediente INC-005/2014, para que estuvieran en posibilidad de emitir su dictamen, acta en la que se asentó: ----------

"...

Que esta Autoridad Acuerda, que procede a poner a disposición de los CC. Jorge Alberto Grande Arriola y José Héctor Cortes Becerril, en las instalaciones de este Órgano Interno de Control el expediente INC. 005/2014, para que se imponga de los autos que lo integran y estén en posibilidad de emitir su dictamen pericial.

..."

En relación a lo anterior, los CC. José Héctor Cortés Becerril y Jorge Alberto Grande Arriola, peritos oficiales en materia de Informática, adscritos a la Procuraduría General de la República, en su dictamen contenido en su oficio con número de folio 76311 del veinticinco de noviembre del dos mil catorce, indicaron que para emitir su dictamen revisaron las constancias que integran el expediente de inconformidad en que se actúa, señalando: ----------

"

ANTECEDENTES Y ANÁLISIS DE LOS MISMOS

Se tuvo acceso irrestricto al total del expediente que integra la presente investigación, consistente en 3 tomos principales y 2 carpetas con anexos técnicos."

Finalmente, las inconformes refieren que debe desestimarse el dictamen del perito traductor de la Procuraduría General de la República, pues indica en uno de sus párrafos que no es experto en terminología de redes y telecomunicaciones, argumento que resulta improcedente,

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

pues en el mismo dictamen, el perito traductor señala que procedió a realizar una investigación sobre los términos controvertidos, tanto en fuentes escritas como fuentes electrónicas por internet para posteriormente emitir una opinión sobre cada punto, indicando al respecto: -------

"METODO

1.- Análisis de las traducciones de términos cuestionadas por la autoridad solicitante.

2.- Investigación de los significados y traducciones de dichos términos.

3.- Opinión sobre la traducción de los términos cuestionados.

DICTAMEN

Es importante señalar que la perito que emite este dictamen no es experto en terminología de redes y telecomunicaciones, específicamente seguridad de redes, que es la materia sobre la que versa la documentación materia de los cuestionamientos. Además, cabe mencionar que no es materia de la especialidad en traducción emitir una opinión sobre cuestionamientos relacionados con el funcionamiento, características o aplicaciones de un dispositivo de este tipo con respecto al cumplimiento de las bases de una Licitación Pública. En todo caso, estos cuestionamientos deberían remitirse a un perito o experto en seguridad de redes informáticas.

*Con las salvedades antes expuestas, **la perito que suscribe procedió a realizar una investigación sobre los términos controvertidos tanto en fuentes escritas como fuentes electrónicas por Internet para posteriormente emitir una opinión sobre cada punto.**"*

Por todo lo antes expuesto, se advierte por parte de esta Autoridad que el equipo FortiDDoS 400B, ofertado por las inconformes con el que pretendieron cumplir con los requerimientos de la Convocatoria a la Licitación Pública Electrónica de Carácter Nacional a precio fijo, para la Contratación del Servicio de Seguridad Perimetral para la Red del IMP, No. LA-018T0O004-N152-2014, en el que se solicitó que "... *El sistema deberá ser un appliance dedicado a proporcionar disponibilidad **por lo que no se aceptaran dispositivos que mantengan el estado de la conexión como firewall,** sistemas de prevención y detección y las variantes o combinaciones como UTM, NGDW, NGIPS ya que al conservar el estado de la conexión, son por sí mismos susceptibles a DDoS...*" el mismo no cumplía con tal requerimiento, pues como se ha demostrado, el equipo FortiDDoS 400B, es un dispositivo que mantiene el estado de la conexión; en consecuencia, no es procedente el motivo de inconformidad hecho valer por las inconformes respecto de este punto. ----------

Las empresas inconformes, hacen valer como argumentos en la segunda parte de su primer y único agravio de su escrito del veintiuno de julio del dos mil catorce, lo siguiente: ----------

"...

Por otra parte, el fallo impugnado es ilegal, porque desechó la propuesta de la inconforme sin realizar un estudio exhaustivo de las características técnicas del equipo Fortianalizer ofertado.

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

En primer término la convocante señala que el equipo Fortianalizer no cumple con las características técnicas solicitadas. Conviene acudir al texto mismo de la convocatoria para dilucidar la ilegalidad del fallo.

En la convocatoria se precisó, página 42 punto 20:

"Características Generales Mínimas.

El sistema de análisis y reporteo para el sistema de seguridad, deberá permitir el almacenamiento de estadísticas de los dispositivos de seguridad administrados por el sistema de gestión centralizado. Este sistema deberá de ser instalado en las instalaciones del Instituto, y deberá de soportar únicamente la operación del mismo. A continuación se enlistan las características mínimas de la solución requerida.

,,,

20. Posibilidad de recibir logs de terceros al menos vía SYSLOG, WMI, ODBC e integración vía parsers personalizados (customizado)."

Mi representada cumplió con el requisito anterior.

Sin embargo, en el fallo se precisó:

"20) Posibilidad de recibir logs de terceros al menos vía SYSLOG, WMI, ODBC e integración vía parsers personalizados (customizado)

El licitante oferta el FORTIANALYZER 3000E, Fortinet, describe en su página:

http:/www.fortinet.com/sites/default/files/productsdatasheets/FortiAnalyzer-3000E.pdf

Como indica en su página FORTINERT acepta solo syslog o de dispositivos compatibles con SYSLOG y se está pidiendo que maneje SYSLOG, WMI, ODBC e integración vía parsers personalizados (customizado)."

Apreciación de la convocante que resulta incorrecta en virtud de que pasa por alto que los equipos Fortianalyzer ofrecidos por mi representada, sí cumplen con las características requeridas en la convocatoria, esto es, si tienen la posibilidad de recibir logs de terceros al menos vía SYSLOG, WMI, ODBC e integración vía parsers personalizados, tal y como se demostrará a continuación:

SYSLog

Consultable en: http://docs-legacy.fortinet.com/fa/inside-fortianalyzer-50.pdf

Los formatos de registro de proveedores externos están en constante evolución. Normalmente se requieren varios conectores para las soluciones de otros proveedores. FortiAnalyzer fue construido desde cero para ser altamente interoperable con otros productos de Fortinet (como FortiMail y FortiWeb). También puede actuar como un agregador y generar informes de los dispositivos compatibles con SYSLOG. Este diseño aerodinámico asegura que los administradores de TI puedan dedicar más tiempo a la creación de informes y menos tiempo al mantenimiento.

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

WMI:

Consultable en: http://blog.fortinet.com/Hyper-V--Is-Microsoft—s-Free-VM- Readv-for- Primetime-

Instrumentación de Administración de Windows PowerShell / Windows (WMI) - Proporciona cmdlets de Windows PowerShell para el Interruptor Extensible Hyper-V que permite a los clientes y socios construir herramientas de línea de comandos o scripts automatizados para la instalación, configuración, monitoreo y solución de problemas.

ODBC:

Algunos clientes pueden requerir la capacidad de conectar sus dispositivos FortiAnalyzer a una fuente de base de datos externa para diversos fines, tales como la importación de datos de registro adicionales. FortiAnalyzer soporta conexiones a orígenes de ODBC externas, y se puede permitir que esas conexiones siguiendo las instrucciones de abajo.

Al escribir estas líneas, esta característica se admite en la versión 5.0.6 FortiAnalyzerOS y posteriores. Las versiones anteriores no se ponen a prueba para que sea compatible con esta característica.

Para permitir que el FortiAnalyzer para aceptar conexiones de una fuente externa DB:

1. Con el fin de permitir que el FortiAnalyzer SQL DB se conecte con una conexión a SQL externa, debe modificar el archivo de configuración de SQL del FortiAnalyzer a través de la CLI (Command Line Interface).
2. Editar el archivo pg_hba.conf localizado en /var/private/localdb/postgres/pg_hba.conf:

Usted tendrá que hacer el siguiente cambio destacado en el archivo pg_hba.conf:

```
# TYPE DATABASE USER ADDRESS METHOD
# "local" is for Unix domain socket connections only
local all all trust
IPv4 local connections:
host all all 0.0.0.0/0 trust
IPv6 local connections:
host all all :: 1/128 trust
Allow replication connections from localhost, by a user with the
replication privilege.
local replication postgres trust
host replication postgres 127.0.0.1/32 trust
host replication postgres ::1/128 trust
```

En el cambio realizado anteriormente, usted debe reemplazar el 0.0.0.0 / 0 con la dirección IP de la base de datos de envío de registros a k FortiAnalyzer. Si lo deja como 0.0.0.0 / 0, lo que permitirá el libre acceso a cualquier host que desea conectarse a través de ODBC a la FortiAnalyzer

3 Edite el archivo postgressql.conf ubicado en / var / private / localdb / postgres / postgressql.conf:

Usted tendrá que hacer el siguiente cambio destacado en el archivo de postgressql.conf:

```
# (change requires restart)
# Note: Increasing max_connections costs -400 bytes of shared memory per

#       connection slot, plus lock space (see max_locks_per_transaction).
```


Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

superuser_reserved_connections = 3 # (change requires restart) # unix_socket_directory = '' # (change requires restart)
unix_socket_permissions = 0777 # begin with O to use octal notation

(change requires restart)
bonjour = off # advertise server via Bonjour
(change requires restart)
bonjour_name = '' # defaults to the computer name
(change requires restart)

En el cambio realizado anteriormente, usted debe reemplazar el 0.0.0.0 con la dirección IP de la base de datos de envío de registros a la FortiAnalyzer. Si lo deja como 0.0.0.0, lo que permitirá el libre acceso a cualquier host que desea conectarse a través de ODBC a la FortiAnalyzer

El FortiAnalyzer ya está listo para recibir conexiones y los registros de la fuente externa especificada.

Integración con terceros.

Consultable en:
http://www.fortinet.com/sites/default/files/productdatasheets/FortiAnalyzer-3000E.pdf

Resumen gráfico de Informes --- Proporciona informes de toda la red de eventos, actividades y tendencias que se producen en FortiGate® y dispositivos de terceros.

De lo que se advierte que, contrario a lo precisado por la convocante en el fallo impugnado, el equipo Fortianalyzer 3000E, ofertado por mi representada sí cumple con las características requeridas en la convocatoria, aunado a que dentro de la propuesta señalada sí se cumplía con los requisitos ofrecidos por esta, lo cual es un hecho notorio que hubiera advertido la convocante de haber efectuado un debido análisis la propuesta de mi representada.

Para robustecer lo anterior, es conveniente acudir a los principios del hecho notorio. A fin de puntualizar lo que constituye un hecho notorio, partimos de la consideración que nuestro Máximo Tribunal, ha formulado al respecto, en la siguiente tesis de jurisprudencia:

"Época: Novena Época
Registro: 174899
Instancia: Pleno
Tipo de Tesis: Jurisprudencia
Fuente: Semanario Judicial de la Federación y su Gaceta
Localización: Tomo XXIII, Junio de 2006
Materia(s): (Común)
Tesis: P./J. 74/2006

HECHOS NOTORIOS. CONCEPTOS GENERAL Y JURÍDICO. Conforme al artículo 88 del Código Federal de Procedimientos Civiles los tribunales pueden invocar hechos notorios aunque no hayan sido alegados ni probados por las partes. Por hechos notorios deben entenderse, en general, aquellos que por el conocimiento humano se consideran ciertos e indiscutibles, ya sea que pertenezcan a la historia, a la ciencia, a la naturaleza, a las vicisitudes de la vida pública actual o a circunstancias comúnmente

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

conocidas en un determinado lugar, de modo que toda persona de ese medio esté en condiciones de saberlo; y desde el punto de vista jurídico, hecho notorio es cualquier acontecimiento de dominio público conocido por todos o casi todos los miembros de un círculo social en el momento en que va a pronunciarse la decisión judicial, respecto del cual no hay duda ni discusión; de manera que al ser notorio la ley exime de su prueba, por ser del conocimiento público en el medio social donde ocurrió o donde se tramita el procedimiento.

Controversia constitucional 24/2005. Cámara de Diputados del Congreso de la Unión. 9 de marzo de 2006. Once votos. Ponente: José Ramón Cossío Díaz. Secretarios: Raúl Manuel Mejía Garza y Laura Patricia Rojas Zamudio.

El Tribunal Pleno, el dieciséis de mayo en curso, aprobó, con el número 74/2006, la tesis jurisprudencial que antecede. México, Distrito Federal, a dieciséis de mayo de dos mil seis."

La información contenida en internet, es un hecho notorio de conformidad con lo dispuesto por el artículo 88 del Código Federal de Procedimientos Civiles, que en su parte conducente dispone:

"ARTICULO 88.- Los hechos notorios pueden ser invocados por el tribunal, aunque no hayan sido alegados ni probados por las partes."

Al respecto, sirve de apoyo la tesis que a continuación se transcribe:

"Época: Décima Época
Registro: 2004949
Instancia: Tribunales Colegiados de Circuito
Tipo de Tesis: Aislada
Fuente: Semanario Judicial de la Federación y su Gaceta
Localización: Libro XXVI, Noviembre 2013 Tomo 2
Materia(s): (Civil)
Tesis: I.3o.C.35 K (10a.)
Pag: 1373

PÁGINAS WEB O ELECTRÓNICAS. SU CONTENIDO ES UN HECHO NOTORIO Y SUSCEPTIBLE DE SER VALORADO EN UNA DECISIÓN JUDICIAL. Los datos publicados en documentos o páginas situados en redes informáticas constituyen un hecho notorio por formar parte del conocimiento público a través de tales medios al momento en que se dicta una resolución judicial, de conformidad con el artículo 88 del Código Federal de Procedimientos Civiles. El acceso al uso de Internet para buscar información sobre la existencia de personas morales, establecimientos mercantiles, domicilios y en general cualquier dato publicado en redes informáticas, forma parte de la cultura normal de sectores específicos de la sociedad dependiendo del tipo de información de que se trate. De ahí que, si bien no es posible afirmar que esa información se encuentra al alcance de todos los sectores de la sociedad, lo cierto es que sí es posible determinar si por el tipo de datos un hecho forma parte de la cultura normal de un sector de la sociedad y pueda ser considerado como notorio por el juzgador y, consecuentemente, valorado en una decisión judicial, por tratarse de un dato u opinión común indiscutible, no por el número de personas que conocen ese hecho, sino por la notoriedad, accesibilidad, aceptación e imparcialidad de este conocimiento. Por tanto, el contenido de una página de Internet que refleja hechos propios de una de las partes en cualquier juicio, puede ser tomado como prueba plena, a menos que haya una en contrario que no fue creada por orden del interesado, ya que se le reputará autor y podrá perjudicarle lo que ofrezca en sus términos.

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

TERCER TRIBUNAL COLEGIADO EN MATERIA CIVIL DEL PRIMER CIRCUITO.

Amparo en revisión 365/2012. Mardygras, S.A. de C.V. 7 de diciembre de 2012. Unanimidad de votos. Ponente: Neófito López Ramos. Secretaria: Ana Lilia Osorno Arroyo."

En consecuencia, el acto de fallo transgrede en perjuicio del Estado, lo dispuesto en los artículos 36, primer y segundo párrafos, y 36 Bis, fracción I de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, pues la convocante evaluó indebidamente la propuesta técnica en comento, por lo que calificó ilegalmente la propuesta de mi representada y decidió no otorgar el puntaje respectivo."

Al respecto, el Área Convocante a través del Encargado del Despacho de la Administración de Recursos en Adquisiciones de Bienes y Servicios de la Gerencia de Proveeduría y Servicios del Instituto Mexicano del Petróleo, señaló por medio de su oficio 350209/AA/340/2014 del catorce de agosto del dos mil catorce, que como parte de las necesidades para la licitación en cuestión, se determinó que una de las especificaciones técnicas más importante para la correlación de eventos, requiere de una herramienta que permita importar el tipo de bitácoras que actualmente se administra, es por ello que el requerimiento de la convocatoria, es especifico con respecto a que debe recibir logs de terceros al menos vía SYSLOG, WMI, ODBC e integración vía parsers personalizados; señalando que una vez que se realizó la valoración de las propuestas presentadas de manera conjunta por las empresas inconformes, el equipo FortiAnalyzer que propusieron no cumplió con la especificación solicitada en la licitación. ------

Por su parte, la empresa Optimiti Network, S.A. de C.V. en su calidad de tercero, en su escrito del veintiséis de agosto del dos mil catorce, señala que cuando en el mercado de seguridad, se habla del término "correlación" se sobreentiende que técnicamente se solicita una solución SIEM, la cual tiene como característica fundamental que para que se detone una alerta especifica en esta plataforma, la información debe de ser colectada a través de un "archivo de registro/log" de un determinado dispositivo (fuente de datos/datasource) de determinado fabricante de seguridad o de sistemas. ----------

Que las empresas inconformes, mediante escrito de veintiséis de agosto del dos mil catorce, ampliaron sus motivos de inconformidad, señalando respecto a este punto lo siguiente: -------

"...

Ahora bien, por lo que se refiere al Fortianalyzer 3000E, propuesto por mi representada si cumple con las características requeridas:

- El sentido de emplear ODBC como método de integración nativa es porque es una manera común de los SIEM, correlaciones comerciales para recibir información de migradores de base de datos directamente o de soluciones de seguridad que usa base de datos como backends.

La convocante en su anexo técnico de requerimientos para la solución "Sistema de Almacenamiento, Reporteo, Análisis y correlación de Eventos de segundad", no solicitó una solución SIEM o "Security information and event management" (Información de Seguridad y Gestión de Eventos), por lo que la solución Propuesta de Fortianalyzer 3000E cumple con la características de correlación de eventos

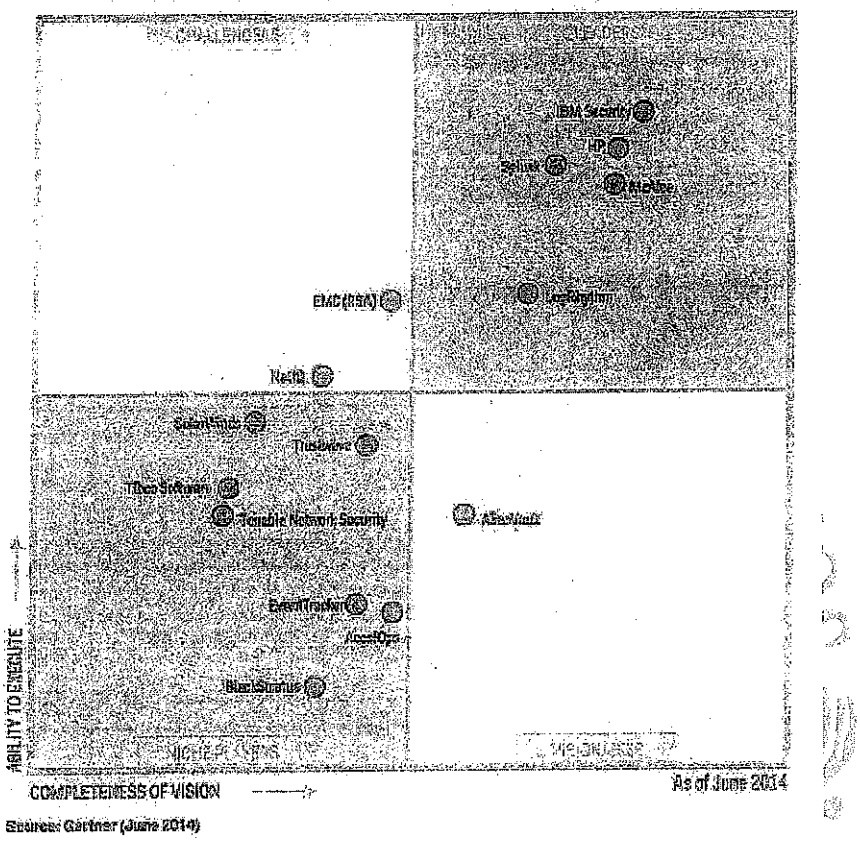
Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

relacionados con un usuario, una IP o un servicio en un periodo de tiempo especificado y como lo solicita la convocante. Cabe mencionar que este no fue un argumento citado en el fallo.

Precisa la convocante en su informe que el producto ofrecido no permitirá correlacionar ni detectar eventos de WMI, ni ODBC, dentro del producto convirtiendo así en información ociosa a toda aquella información que venga con este tipo de vector, por lo que se interpreta como un "no cumple", precisión que es errónea porque la solución Propuesta de Fortianalyzer 3500E, cumple con la características de correlación de eventos relacionados con un usuario, una IP o un servicio en un periodo de tiempo especificado tal cual lo solicita la convocante, tal y como se demuestra a continuación.

Figure 1. Magic Quadrant for Security Information and Event Management



Reference: http://securityintelligence.com/gartner-2014-magic-quadrant-siem-securitv/#.U ZH3l6VsZh.

Cabe señalar que en el anexo técnico de la convocatoria no se solicita como documentación de respaldo, que el equipo Fortianalyzer 3500 E, se encuentre ubicado en el cuadrante de la casa consultora Gartner correspondiente a Security Information and Event Management, hecho que con fundamento en el artículo 123 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público constituye un hecho novedoso no solo para la instancia que se promueve, sino respecto a las condiciones de la convocatoria.

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

La convocante en su informe precisa que el FortiAnalyzer solo está acotado a integrar plataformas propias del portafolio de Fortinet y de dispositivos compatibles a syslog.

http://www.fortinet.com/sites/default/files/productdatasheets/FortiAnalyzer-3500E.pdf

En el documento técnico de la tecnología propuesta llamado Fortianalyzer 3500E menciona que el Fortianalyzer agrega información de logs de dispositivos fortinet third-party device o dispositivos terceros, sin embargo, de las observaciones realizadas por la licitante hace referencia a un documento catalogado como "legacy", el cual significa que no es la versión más actual o que pertenece a generaciones anteriores del producto, por lo que desafortunadamente al tener como referencia equipo de una generación anterior la convocante consideró que el equipo ofrecido no cumplía con lo requerido en la licitación."

Que el Área Convocante, dio respuesta a los motivos de ampliación de la inconformidad hecha valer por las empresas inconformes sobre este punto, a través del oficio 35209/AA/393/2014 del nueve de septiembre del dos mil catorce, suscrito por el Encargado del Despacho de la Administración de Recursos en Adquisiciones de Bienes y Servicios de la Gerencia de Proveeduría y Servicios del Instituto Mexicano del Petróleo, señalando que las inconformes hacen alusión y sustenta parte de su ampliación a su inconformidad a un modelo FortiAnalyzer 3500E, el cual no fue mencionado, ni en el fallo, ni en su oficio de respuesta de la inconformidad. ----------

Señala además la Convocante, que las inconformes que en su matriz de cumplimiento exhibida dentro de su propuesta técnica, no indica que su equipo ofertado pueda recibir logs de terceros al menos vía SYSLOGS, WMI, OBDC e integración vía parsers personalizados: ----------

La empresa Optimiti Network, S.A. de C.V., en su calidad de tercero interesado, mediante escrito de fecha diez de septiembre del dos mil catorce, expresó respecto a los motivos de ampliación de inconformidad, que el equipo FortiAnalyzer 3000E ofertado por las inconformes, no cumple con los requerimientos de recibir logs de terceros al menos vía SYSLOG, WMI, ODBC e integración vía parsers personalizados. ----------

Que las empresas inconformes formularon sus alegatos mediante escrito de fecha dieciocho de diciembre del dos mil catorce, manifestando lo siguiente: ----------

"...

ALEGATOS

*1. El día **18 de junio de 2014** se publicó en COMPRANET la convocatoria para la licitación pública nacional mixta de servicios número LA-018T0O004-N152-2014, denominada "Convocatoria a la Licitación Pública, Electrónica, de carácter Nacional, a precio fijo, para la contratación del Servicio de Seguridad Perimetral para la red IMP." Y entre los requisitos se solicitó:*

...

b) En la convocatoria se precisó, pagina 42 punto 20:

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

"Características Generales Mínimas.
El sistema de análisis y reporteo para el sistema de seguridad, deberá permitir el almacenamiento de estadísticas de los dispositivos de seguridad administrados por el sistemas de gestión centralizado. Este sistema deberá de ser instalado en las instalaciones del Instituto, y deberá de soportar únicamente la operación del mismo. A continuación se enlistan las características mínimas de la solución requerida,

...

20. Posibilidad de recibir logs de terceros al menos vía SYSLOG, WMI, ODBC e integración vía parsers personalizados (customizado)."

*Los equipos **FortiDDoS 400B y Fortianalyzer 300E** ofertados por mi representada si cumplen con las características requeridas, lo que se demuestra con las especificaciones técnicas de éstos, en donde se advierte que los éstos si cuentan con las características solicitadas por el área convocante, de conformidad con lo siguiente:*

...

***Por lo que se refiere al inciso b) mencionado al inicio de este escrito, es conveniente mencionar que el equipo Fortianalyzer 300E, recibe logs de terceros al menos vía SYSLOG, WMI, ODBC e integración vía parsers personalizados,** de acuerdo a los siguientes documentos, ya que recibe logs WMI requeridos, lo cual se precisa en la página http://blog.fortinet.com/post/hyper-v-microsoft-s-free-vm-ready-for-primetime, al señalarse en la página de internet que " El tráfico múltiple de VLAN ahora puede dirigirse a un solo adaptador de red en una máquina virtual - **Monitoreo y amp; Duplicación de Puerto** - Monitorear el tráfico de puertos específicos que fluyen a través de máquinas virtuales específicas en el interruptor y tráfico duplicado que entonces puede entregarse a otro puerto virtual para su procesamiento posterior - **Windows PowerShell/Instrumental de Administración de Windows (WMI, por sus siglas en inglés)** - Proporciona a los cmdlets de Windows PowerShell para el Interruptor Extensible de Hyper-V que permite a los clientes y socios construir herramientas de línea de comando o scripts para configuración, ajuste, monitoreo y solución de problemas."*

Ahora bien, por lo que se refiere al cumplimiento del OBDC en la página de internet http://partners.fortinet.com./FortiPartnerPortal/CMS/Download.do?oid=935 5, se precisa que el equipo fortianalyzer soporta conexiones a fuentes OBDC externas, las cuales se habilitan el seguir una serie de instrucciones al precisarse que ". En el cambio realizado arriba, debe sustituir 0.0.0.0 con la dirección IP de la base de datos que envía los registros al FortiAnalyzer. Si la deja como 0.0.0.0, esto permitirá el acceso abierto a cualquier host que desee conectarse a través de ODBC al FortiAnalyzer", por lo que estará listo para recibir conexiones y registros de la fuente externa especializada, cumpliendo con los requisitos precisados en la convocatoria.

Asimismo, en la página de internet http://www.fortinet.com/sites/default/files/productdatasheets/FortiAnalyzer-3500E.pdf ofrecida como prueba se precisa que los dispositivos Fortianalyzer integran registro, análisis e informes de su red en un solo sistema los cuales recolectan, correlacionan, analizan geográficamente y cronológicamente diversos datos de seguridad. Además de que en la página de internet http://docs-legacy.fortinet.com/fa/inside-fortianalyzer-50.pdf, se advierten las ventajas que tiene dicho dispositivo toda vez que proporciona un informe de eventos de toda la red, que permite identificar las amenazas de seguridad a través de su red, incluye la actividad de tráfico, eventos del sistema, virus, ataques, filtrados web, al generar informes a partir de dispositivos compatibles con Syslog.

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

Por lo que es evidente que del análisis que se efectúe de todas las documentales ofrecidas como pruebas por mi representada, así como de la instrumental de actuaciones, se podrá advertir que los equipos ofertados por mi representada sí cumplen con las características requeridas por la convocante, al ser un hecho notorio el que los equipos FortiDDoS 400B y Fortianalyzer 3500E cumplen con todas y cada una de las características solicitadas en la convocatoria, ya que el primero de estos no mantiene el estado de la conexión y el segundo de los referidos sí recibe logs de terceros al menos vía SYSLOG, WMI, ODBC e integración vía parsers personalizados, de lo que es evidente que los equipos ofrecidos por mi representada sí cumplen con las características precisadas en las bases de la licitación.

Ahora bien, por lo que se refiere a la prueba pericial ofrecida por la tercero interesada (Optimity) no acredita fehacientemente que en el peritaje realizado se haya efectuado un debido análisis de todas las características de los equipos ofrecidos por mi representada, ya que de haberlo realizado hubiera advertido que sí cumplen con las características requeridas en la convocatoria.

Aunado a esto, de los peritajes ofrecidos por los peritos terceros de la PGR no se advierte que se hayan analizado debidamente todas las documentales que se encuentran en el expediente al basarse únicamente en las páginas de internet http://www.fortinet.com/sites/default/files/productdatas/sheets/FortiDDos-100B.pdf y http://www.fortinet.com/sites/default/files/productdatas/sheets/FortiDDos-3500E.pdf no efectuando un análisis de todas las documentales de donde se advierten con claridad todas y cada una de las características de los equipos ofertados, por lo que no se puede llegar a una conclusión tajante sin analizar todos los documentos en los que se precisen todas y cada una de las características de los equipos ofertados.

Por último, es importante precisar que el perito que efectúa la traducción de las páginas de internet cae en diversas contradicciones al precisar en el inicio del peritaje que:

> *"Es importante señalar que la perito que emite este dictamen no es experto en terminología de redes y telecomunicaciones, específicamente seguridad de redes, que es al materia sobre la que versa la documentación materia de los cuestionamientos. Además, cabe mencionar que no es materia de la especialidad en traducción emitir una opinión sobre cuestionamientos relacionados con el funcionamiento, características o aplicaciones de un dispositivo de este tipo o con respecto al cumplimiento de las bases de una licitación pública. En todo caso estos cuestionamientos deberán remitirse a un perito o experto en seguridad de redes informáticas.*
>
> *Con las salvedades antes expuestas, la perito que suscribe procedió a realizar una investigación sobre los términos controvertidos tanto en fuentes escritas como en fuentes electrónicas por internet para posteriormente emitir una opinión sobre cada punto."*

...

De lo que se advierte que efectúa una conclusión que no debe ser tomada en consideración ya que a su decir no es experto en seguridad de redes informáticas sino en traducción de documentos e indebidamente concluye que los equipos ofrecidos por mi representada no cumplen con las características de la convocatoria."

Que la empresa Optimiti Network, S.A. de C.V., en su escrito del dieciséis de diciembre del dos mil catorce, señala entre otros aspectos como alegatos, que de acuerdo a los resultados emitidos con motivo de los peritajes que rindieron, tanto el perito que ésta presentó, así como el de los peritos de la Procuraduría General de la República, el dispositivo FortiAnalyzer 3000E,

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

no soporta los métodos WMI, ODBC ni la integración vía parsers personalizados, soportando únicamente el método Syslog; por lo que no cumple con lo solicitado en la convocatoria. ------

Visto lo anterior, las empresa inconformes Servicios Alestra, S.A. de C.V., Alestra, S. de R.L. de C.V. y SK Holdings, S.A. de C.V., esencialmente expresan que la Convocante desechó la propuesta que de manera conjunta presentaron con motivo de su participación en la Licitación Pública Electrónica de Carácter Nacional a precio fijo, para la Contratación del Servicio de Seguridad Perimetral para la Red IMP, No. LA-018T0O004-N152-2014, al determinar que su equipo FortiAnalyzer 3000E, no cumple con las características técnicas solicitadas en la convocatoria, por lo que el fallo revela falta de exhaustividad de las características técnicas del equipo FortiAnalyzer 3000E que fue propuesto, aduciendo las inconformes que su equipo sí cumple con las características requeridas en la convocatoria, esto es, si tienen la posibilidad de recibir logs de terceros al menos vía SYSLOG, WMI, ODBC e integración vía parsers personalizados. ----------

Al respecto, es de señalar que con fecha dieciocho de junio de dos mil catorce, fue publicada en el Diario Oficial de la Federación y en el Sistema Electrónico Compranet la Convocatoria a la Licitación Pública Electrónica de Carácter Nacional a precio fijo, para la Contratación del Servicio de Seguridad Perimetral para la Red del IMP, No. LA-018T0O004-N152-2014. --------

Ahora bien, la convocatoria en comento, en su Apartado II, OBJETO Y ALCANCE DE LA CONVOCATORIA A LA LICITACIÓN PÚBLICA, Anexo Técnico, Apéndice A "Especificaciones Técnicas por tipo firewall de nueva generación", Inciso III) Sistema Almacenamiento, Reporteo, Análisis y Correlación de Eventos de Seguridad, Características Generales Mínimas, punto 20, solicitó: ----------

"...

El sistema de análisis y reporteo para el sistema de seguridad, deberá permitir el almacenamiento de estadísticas de los dispositivos de seguridad administrados por el sistema de gestión centralizado. Este sistema deberá de ser instalado en las instalaciones del Instituto, y deberá de soportar únicamente la operación del mismo. A continuación se enlistan las características mínimas de la solución requerida.

...

20. Posibilidad de recibir logs de terceros al menos vía SYSLOG, WMI, ODCB e integración de vía parsers personalizados (customizado)"

Documental que se valora de conformidad con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción II, 197 y 202 del Código Federal de Procedimientos Civiles, ambas disposiciones de aplicación supletoria en materia administrativa, del que se desprende que la convocante señaló que el equipo ofertado para dar cumplimiento a este punto, deberá recibir logs de terceros al menos vía SYSLOG, WMI, ODCB e integración de vía parsers personalizados (customizado). ----------

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

Ahora bien, en el fallo de fecha once de julio del dos mil catorce, emitido por el Encargado del Despacho de la Administración de Recursos en Adquisiciones de Bienes y Servicios de la Gerencia de Proveeduría y Servicios del Instituto Mexicano del Petróleo, señaló respecto de la propuesta presentada de manera conjunta por las empresas Alestra, S. de R.L. de C.V., SK Holdings, S.A. de C.V. y Servicios Alestra, S.A. de C.V. lo siguiente: ----------

"No cumple técnicamente con lo siguiente:

...

Respecto al inciso III) Sistema Almacenamiento, Reporteo, Análisis y Correlación de Eventos de Seguridad, características Generales Mínimas, punto 20.

Dice:

20) Posibilidad de recibir logs de terceros al menos vía SYSLOG, WMI, ODBC e integración via parsers personalizados (customizado)

El licitante oferta FOTIANALYZER 3000E, Fortinet, describe en su página http://www.fortinet.com/sites/defaul/files/productdatashetets/FotiAnalyzer-3000E.pdf

- *Fortianalyzer; only ingest logs from other Fortinet appliances and syslog compatible devices (Source Attached: FortiAnalyzer-VM.pdf)*

Como lo indica en su página FORTINET acepta solo syslog o de dispositivos compatibles con SYSLOG y se está pidiendo que maneje SYSLOG, WMI, ODBC e integración de vía parsers personalizados (customizado).

..."

Documental que se valora de conformidad con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción II, 197 y 202 del Código Federal de Procedimientos Civiles, ambas disposiciones de aplicación supletoria en materia administrativa, del que se desprende que la Convocante señaló que la propuesta presentada por las inconformes, no cumplía con lo solicitado en la convocatoria de la Licitación Pública Electrónica de Carácter Nacional a precio fijo, para la Contratación del Servicio de Seguridad Perimetral para la Red del IMP, No. LA-018T0O004-N152-2014, ya que el dispositivo FortiAnalyzer 3000E que ofertaron, únicamente es compatible con Syslog. ----------

Ahora bien, de acuerdo a lo señalado por las inconformes, estas propusieron con motivo de su participación dentro de la Licitación Pública Electrónica de Carácter Nacional a precio fijo, para la Contratación del Servicio de Seguridad Perimetral para la Red del IMP, No. LA-018T0O004-N152-2014, para este punto el equipo FortiAnalyzer 3000E de la marca Fortinet, el cual, conforme a lo expresado por las inconformes, cumple con las especificaciones solicitadas en la convocatoria, al señalar expresamente a fojas quince de su escrito de inconformidad que *"... Apreciación de la convocante que resulta incorrecta en virtud de que pasa por alto que los*

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.
Tel.: (55) 9175 8084 facosta@imp.mx

equipos Fortianalyzer ofrecidas por mi representada, si cumplen con las características requeridas en la convocatoria, este es, si tiene la posibilidad de recibir logs de terceros al menos Vía SYSLOG, WMI, ODBC e integración vía parsers personalizados tal y como se demostrara a continuación." ----------

Para tal efecto, la inconforme ofreció como prueba de su parte, la prueba pericial en materia de ingeniería en electrónica y comunicaciones, a cargo del Ingeniero [redacted], a efecto de que respondiera la siguiente pregunta: "*Cuáles son los lenguajes, log y funcionalidades que puede leer y recibir el equipo fotianalyzer?*"; rindiendo con fecha catorce de octubre del dos mil catorce, su dictamen pericial en el que señaló lo siguiente: ----------

"2.- Cuáles son los lenguajes, logs y funcionalidades que puede leer y recibir el equipo fortianalyzer?

En opinión de este experto, el Fortianalyzer es una plataforma que integra el registro de red, análisis y presentación de informes en un solo sistema, la entrega de un mayor conocimiento de los eventos de seguridad en toda su red. La familia FortiAnalyzer minimiza el esfuerzo necesario para controlar y mantener las políticas de uso aceptable, así como identificar los patrones de ataque para ayudarle a afinar sus políticas.

La plataforma de FortiAnalyzer, puede ser implementada en dispositivos de propósito específico o sobre una plataforma virtual ofreciendo la captura de datos detallada con fines forenses para cumplir con las políticas en material de privacidad y revelación de las violaciones de seguridad de la información.

El equipo Fortianalyzer 3000E es un dispositivo que puede conectarse a base de datos externas para varios propósitos relacionados con el registro y almacenamiento de logs (registros) al igual que soportar conexiones externas a través de ODBC.

Los formatos de Logs de los proveedores externos están en constante evolución y es por esto que Fortianalyzer fue construido desde el principio para ser altamente interoperable. Además, puede actuar como un agregador y generar informes desde dispositivos compatibles con syslog. Este diseño aerodinámico asegura que los administradores de TI pueden centrase más tiempo en elaboración de informes y menos tiempo en mantenimiento.

Las Funcionalidades advertidas por este experto respecto del equipo Fortianalyzer

- *Resumen Gráfico del tráfico de red: Proporciona informes de toda la red de eventos, actividades y tendencias que ocurren en FotiGate y dispositivos de terceros.*
- *Correlación de Eventos de Red: Permite a los administradores de TI identificar y reaccionar ante las amenazas de seguridad de la red de forma rápida.*
- *Rendimiento escalable y Capacidad*
- *Registro Centralizado de múltiples tipos de registros: Incluye la actividad de tráfico, los eventos del sistema, virus, ataques, eventos de filtrado de Web y filtrado de correo electrónico.*
- *Visualización de tráfico de red en tiempo real y opciones de reporteo Avanzado*
- *Fortianalyzer soporta exportar o importar plantillas de reportes*

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

En la junta de aclaraciones en la pregunta 20. Página 52. Realizada por Teléfonos de México, donde la convocante especifica el alcance de la solución de correlación y especifica que deberá de correlacionar todos los dispositivos miembros de la solución de seguridad ofertada por ende con el fortianalyzer se da cumplimiento al requerimiento de la convocante al correlacionar los logs de los dispositivos de seguridad propuestos en la licitación.

20	*43*	*Posibilidad de recibir logs de terceros al menos vía SYSLOG, WMI, ODBC e integración de vía parsers personalizados (customizado)*	*Se pide amablemente a la convocante nos enliste la totalidad de los equipos que serán agregados a la solución de correlación, así como su ubicación física de cada uno de ellos?*
RESPUESTA: Se deberán correlacionar todos los dispositivos miembros de la solución de seguridad ofertada y su ubicación física está indicada en el apéndice B "localidades remotas"			

Las siguientes ligas sirven de referencia para la respuesta a esta pregunta:

- ***Referencias:***

http://www.fortinet.com.sites/default/files/productdatassheets/FortiAnalyzer-3500E.pdf

http://blog.fortinet.com/post/hyper-v-is-microsoft-s-free-vm-ready-for-primetime

- ***Portal de Socios***

https://partners.fortinet.com/FortiPartnerPortal/CMS/Download.do?oid=9355"

Dictamen pericial que se valora con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción IV, 197 y 211 del Código Federal de Procedimientos Civiles, ambas disposiciones de aplicación supletoria en materia administrativa, y cuyo dictamen es en el sentido de demostrar que el equipo FortiAnalyzer 3000E, ofrecido por las inconformes dentro del proceso de la Licitación Pública Electrónica de Carácter Nacional a precio fijo No. LA-018T00004-N152-2014, sí cumplía con lo solicitado, al tener la posibilidad de recibir logs de terceros al menos vía SYSLOG, WMI, ODBC e integración vía parsers personalizados. ----------

Así mismo, como ya se dijo, dentro de la instancia de la inconformidad se dio vista a la empresa Optimiti Network, S.A. de C.V., en su calidad de tercero interesado para que designara a su perito, nombrando para tal efecto al [redacted], quien con fecha trece de octubre del dos mil catorce, presentó su dictamen pericial en los siguientes términos: -------

"...

Respuesta a las preguntas formuladas por la empresa SERVICIOS ALESTRA, S.A. DE C.V.

...

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

2. ***¿Cuáles son los lenguajes, log y funcionalidades que puede leer y escribir el equipo Fortianalyzer?***

El término lenguaje en materia de informática y sistemas es un lenguaje formal diseñado para expresar procesos que pueden ser llevados a cabo por computadoras.

Un log es el término en inglés para un archivo computacional que sirve como bitácora. Este archivo contiene los registros de los eventos que suceden en un sistema operativo o un software. Existe un protocolo estándar de bitácoras computacionales (Syslog) que se encuentra descrito en el RFC 5424 que describe la arquitectura en cómo se envían los mensajes para poder filtrar y almacenar las bitácoras de un sistema en otro sistema independiente.

Mediante una búsqueda en el sitio del fabricante Fortinet, así como búsquedas por el nombre del producto FortiAnalyzer en el buscador de Internet de Google en fecha ocho de octubre del dos mil catorce, apareciendo varios resultados, adicionalmente conociendo de la existencia de varios modelos de equipos comercializados por el fabricante, se procedió a buscar los documentos técnicos que contiene la información específica del dispositivo propuesto en el proceso licitatorio que es el FortiAnalyzer 3000E.

Se encontró el documento público de dicho modelo en la siguiente dirección de internet: http://www.fortinet.com/sites/default/files/productdatasheets/FortiAnalyzer-3000E.pdf

Las funcionalidades técnicas descritas en el documento, se encuentran en la página 3, donde se encuentran:

- *Herramientas de Reporteo y Visualización*
- *API´s JSON y XML (Servicios Web)*
- *Visor de Bitácoras*
- *Respaldo DLP*
- *Alertas*
- *Mejor con FortiManager*
- *Dispositivos Soportados por FortiAnalyzer*

En estos documentos, claramente se puede identificar que las bitácoras soportadas son estrictamente los generados por los dispositivos de la marca Fortinet como: "FortiGate Multi-Threat Security Systems", "FortiMail Messaging Security Systems", "FortiClient EndPoint Security Suite", "FortiWeb Web Application Security" y "FortiManger Centralized Managemet".

El único formato de bitácora soportado según el mismo documento y fuera de los dispositivos mencionados anteriormente es el de dispositivos que sean compatibles con Syslog.

La impresión del documento público RFC 5424 donde se detalla el protocolo Syslog se encuentra adjunto al presente dictamen como ***ANEXO 1.***

En el documento presentado por la inconforme indica que si es posible incorporar otros métodos en la página de internet que se encuentra en la página número 16 de la inconformidad, la cual no existe:

...

Se procedió a buscar información similar y se encontró una página con el mismo título, el cual habla sobre virtualización y no sobre información de bitácoras o métodos como WMI, ODBC o parsers customizados.

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

Según la documentación del dispositivo FortiAnalyzer 3000E NO soporta los métodos WMI, ODBC ni la integración vía parsers personalizados, tan es así que dentro de la misma página de internet del fabricante Fortinet, se encuentra que el fabricante tiene alianzas estratégicas para poder realizar las funciones de SIEM por medio de terceros, ya que el dispositivo por sí mismo no lo hace.

Dicha información se encuentra en las siguientes páginas de internet:

http://www.fortinet.com/press_releases/2014/fortinet-extends-siem-ecosystem.html

http://www.fortinet.com/partners/alliances/SIEM-partners.html

Dictamen pericial que se valora con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción IV, 197 y 211 del Código Federal de Procedimientos Civiles, ambas disposiciones de aplicación supletoria en materia administrativa, y cuyo dictamen fue en el sentido de demostrar que el equipo FortiAnalyzer 3000E, ofrecido por las empresas inconformes dentro del proceso de la Licitación Pública Electrónica de Carácter Nacional a precio fijo No. LA-018T0O004-N152-2014, no cumplía con lo solicitado, ya que no soporta los métodos WMI, ODBC ni la integración vía parsers personalizados, siendo compatible únicamente con SYSLOG. ----------

De lo anterior se advierte, que dichos dictámenes son contradictorios, toda vez que el dictamen del [redacted], perito presentado por las inconformes, es en el sentido de que el equipo FortiAnalyzer 3000E, ofrecido dentro del proceso de la Licitación Pública Electrónica de Carácter Nacional No. LA-018T0O004-N152-2014, sí cumplía con lo solicitado, al tener la posibilidad de recibir logs de terceros al menos vía SYSLOG, WMI, ODBC e integración vía parsers personalizados, en tanto que, el dictamen del [redacted], perito ofrecido por la empresa Optimiti Network, S.A. de C.V., es en sentido contrario, esto es, que el equipo FortiAnalyzer 3000E, no soporta los métodos WMI, ODBC ni la integración vía parsers personalizados, siendo compatible únicamente con SYSLOG. -------

Al existir discordancia entre ambos dictámenes, esta Autoridad como ya se mencionó requirió el apoyo a la Procuraduría General de la República, para que a través de un perito tercero, se emitieran un dictamen sobre los hechos controvertidos, que en el caso, obra en el expediente el dictamen pericial emitido por los CC. Jorge Alberto Grande Arriola y José Héctor Cortes Becerril, el veinticinco de noviembre del dos mil catorce, peritos oficiales en materia de informática adscritos a la Procuraduría General de la República, quienes dictaminaron lo siguiente: ----------

"..

SEGUNDA.- *Cuáles son los lenguajes, log y funcionalidades que puede leer y recibir el equipo Fortianalyzer?*
RESPUESTA: *De acuerdo a la hoja de datos del fabricante Fortianalyzer, que se localiza en la dirección de internet http://www.fortinet.com/sites/default/files/productdatasheets/FortiAnalyzer-3500E.pdf, la*

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

*plataforma de reporteo Fortianalyzer, es capaz de aceptar desarrollos de aplicaciones en los lenguajes JSON (**J**ava **S**cript **O**bject**N**otation) y en XML (E**X**tensible**M**arkup**L**anguage). En lo que se refiere a los log viewer (visualizador de bitácoras) que es capaz de generar, se citan en la misma hoja de datos, los siguientes:*

- Visualizador de logs en tiempo real e históricos.
- Selección de tráfico, eventos y bitácoras UTM (Unified Threat Management – Administración Uniforme de Amenazas).
- Navegación por dispositivo
- Filtrado por bitácora y capacidades de búsqueda
- Inspección granular con detalles de la bitácora en pantalla
- Íconos intuitivos para países, aplicaciones, y más

En la última parte de la pregunta, que se encuentra mal redactada o al menos no es clara, los que suscriben entienden que derivado de los hechos que se investigan, ésta última parte se refiere a los tipos de archivos que puede importar y exportar la plataforma Fortianalyzer, ya que las funcionalidades no se importan ni se exportan, puesto que son inherentes al funcionamiento del dispositivo. En éste orden de ideas, la plataforma Fortianalyzer, utiliza la técnica DLP o Data Loss Prevention (Prevención de pérdida de datos), la cual es capaz de manejar los formatos de archivos:

- *Formato de correo electrónico: protocolos IMAP, POP3 y SMTP.*
- *Formato HTTP: protocolo de transferencia de hipertextos.*
- *Formato FTP: protocolo de transferencia de archivos.*
- *Formato IM (mensajería instantánea): que incluye sesiones de protocolo ICQ, MSN y Yahoo.*

...

***VIGÉSIMAPRIMERA**.- Que diga el perito, en base al documento público que se encuentra en la página del fabricante de la tecnología Fortinet sobre el producto "FortiAnalyzer 3000-E" ¿Cuáles son los dispositivos y métodos soportados nativamente?*
***RESPUESTA:** Los lenguajes que la plataforma Fortianalyzer soporte son solamente JSON y XML, en cuanto a visor de logs utiliza el estándar DLP (Data Loss Prevention), que soporta protocolos HTTP, FTP, IM, SMTP, IMAP y POP3.*

Por otra parte, se indica que los dispositivos soportados por el Fortianalyzer son los siguientes:

- *Sistemas de seguridad de múltiples amenazas FotiGate.*
- *Sistemas de seguridad de mensajería FortiMail.*
- *Suite de seguridad de punto final FortiClient.*
- *Aplicación web de seguridad FortiWeb.*
- *Administrador centralizado FortiManager.*
- *Cualquier dispositivo compatible con Syslog.*

***VIGÉSIMASEGUNDA**.- Que diga el perito, a qué se refiere dispositivos compatibles con syslog.*
***RESPUESTA:** Que debe de tener compatibilidad para el envío y recepción de registros usando el protocolo syslog.*

***VIGÉSIMATERCERA**.- Que diga el perito, si en la lista que aparece en base al documento público que se encuentra en la página del fabricante de la tecnología Fortinet sobre el producto "FortiAnalyzer 3000-E" se encuentran listados los métodos WMI, ODBC e integración vía parsers personalizados.*
***RESPUESTA:** No, tal y como ya se indicó, la hoja de datos técnicos del fabricante, especifica que el Fortianalyzer 3000-E, es compatible con dispositivos de su propia manufactura (plataforma Forti) y con todos aquellos que manejen el protocolo Syslog, no mostrando ningún otro protocolo.*

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

***VIGÉSIMACUARTA**.-Que diga el perito, en base a las respuestas anteriores y documentación existente si el producto FortiAnalyzer-3000E soporta los métodos WMI, ODBC e integración vía parsers personalizados como fueron solicitados en las bases.*
***RESPUESTA:** No se especifican tales protocolos en las hojas de datos técnicos del fabricante."*

Dictamen pericial que se valora con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción IV, 197 y 211 del Código Federal de Procedimientos Civiles, ambas disposiciones de aplicación supletoria en materia administrativa, en el que se indica que el dispositivo FortiAnalyzer 3000E, ofrecido por las inconformes, no soporta los métodos WMI, ODBC e integración vía parsers personalizados como fue solicitado en la convocatoria. ----------

De lo anterior, se advierte que el dictamen pericial emitido por los CC. Jorge Alberto Grande Arriola y José Héctor Cortes Becerril peritos oficiales en materia de informática de la Procuraduría General de la República, coincide con el dictamen pericial del [redacted], perito de la empresa Optimiti Network, S.A. de C.V., en el sentido de que el equipo FortiAnalyzer 3000E, es compatible únicamente con Syslog, y que no soporta los métodos WMI, ODBC e integración vía parsers personalizados como fue requerido en la multicitada convocatoria. ----------

Adicionalmente, las inconformes para demostrar que el dispositivo FortiAnalyzer 3000E, que propusieron dentro de la Licitación Pública Electrónica de Carácter Nacional a precio fijo No. LA-018T0O004-N152-2014, si cumplía con lo solicitado, al ser un dispositivo que soporta los métodos WMI, ODBC e integración vía parsers personalizados como fueron solicitados en la convocatoria, ofreció como pruebas a su favor la traducción del inglés al castellano de las siguientes páginas de Internet: ----------

http://www.fortinet.com/sites/default/files/producdatasheets/FortiAnalyzaer-3500E.pdf

Documental privada que se valora con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción III, 197 y 203 del Código Federal de Procedimientos Civiles, traducción con la que las inconformes pretenden acreditar que los dispositivos FortiAnalyzer integran registros, realizan análisis e informes de su red en un sólo sistema, los cuales recolectan, correlacionan, analizan geográficamente y cronológicamente diversos datos de seguridad. ----------

http://docs-legacy.fortinet.com/fa/inside-fortianalyzer-50.pdf

Documental privada que se valora con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción III, 197 y 203 del Código Federal de Procedimientos Civiles, traducción con la que las inconformes pretenden acreditar las ventajas que tiene dicho dispositivo FortiAnalyzer, toda vez que proporciona

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.
Tel.: (55) 9175 8084 facosta@imp.mx

informes de eventos de toda la red, permite verificar las amenazas de seguridad a través de su red, incluye la actividad de tráfico, de eventos del sistema, virus ataques, filtrados web. ----

Con motivo de lo anterior, esta Autoridad dio vista de dichas traducciones tanto al Área Convocante del Instituto Mexicano del Petróleo, como a la empresa Optimiti Network, S.A. de C.V., quienes manifestaron su desacuerdo respecto a la traducción exhibida por las inconformes, en relación a la información contenida en dichas páginas de la internet. ----------

Esto es, a través del oficio 350209/AA/516/ 2014 del treinta y uno de octubre del dos mil catorce, el Encargado del Despacho de la Administración de Recursos en Adquisiciones de Bienes y Servicios del Instituto Mexicano del Petróleo, remitió a esta Autoridad la opinión de la Gerencia de Tecnologías de la Información ambas del Instituto Mexicano del Petróleo, relativa a la traducción de los documentos ofrecidos por las inconformes, en los siguientes términos: -

"...

*Respecto a la traducción que realiza de la página 2 último inciso de los dispositivos soportados por fotianalyzer con dirección web http://www.fortinet.com/sites/default/files/productdatasheets/fotianalyzer-3500E.pdf (anexo 1), en dicho documento se encuentran en inglés la siguiente frase "any syslog-compatible device", lo cual lo traducen como "cualquier dispositivo compatible con el registro del sistema", **siendo que syslog es un estándar para el envió de registros, siendo una palabra técnica que no tiene la connotación que se le quiere dar en dicha traducción**, el mismo inconforme lo confirma en otro de sus documentos que traduce, el llamado "Inside Fortianalyzer" de la página web http://docs-legacy.fortinet.com/fa/inside-fortianalyzer-50.pdf (anexo 2), el cual en su página 1 inciso interoperability, contiene la palabra syslog y no la traduce al español."*

Documental pública que se valora con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción II, 197 y 202 del Código Federal de Procedimientos Civiles, con la que el Área Convocante del Instituto Mexicano del Petróleo, manifiesta su desacuerdo y expresa que existen contradicciones en la traducción del concepto "Syslog", indicando que es un estándar para el envió de registros, y que no tiene la connotación que se le pretende dar en la traducción ofrecida por las inconformes. ----------

Por su parte, la empresa Optimiti Network, S.A. de C.V., a través de su Administrador Único, señaló mediante su escrito del cuatro de noviembre del dos mil catorce, lo siguiente: ----------

"...

2. De la "hoja de datos" de la solución FortiAnalyzer del rubro "Any Syslog-Compatible Device" (bajo la sección "FortiAnalyzer Supported Devices" en inglés) fue traducido como "Cualquier dispositivo compatible con el registro del sistema. Aquí se continúa reflejando la limitante de colección de eventos desde diferentes tipos de fuentes por la solución ofertada, ya que "syslog" aunque es un estándar de facto para el envío de mensajes de registro a nivel aplicativo como protocolario típicamente a través de UDP por puerto 514 no es soportado por todos los dispositivos de seguridad y por eso se buscan mecanismos de

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

integración adicionales como WMI, ODBC y desarrollo de parsers customizados para soportar dispositivos multimarca.

Al respecto, se destaca como observación que hay tecnicismos en inglés que en ocasiones no siempre es recomendables traducirlos y "syslog", al ser un estándar en la industria de redes, telecomunicaciones y seguridad no es "reconocido" con la traducción "registro del sistema" y en todo caso esto está más reconocido al término "log".

Documental privada que se valora con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción III, 197 y 203 del Código Federal de Procedimientos Civiles, con la que la empresa Optimiti Network, S.A. de C.V., en su calidad de tercero interesado manifiesta su desacuerdo respecto a la traducción del concepto "Syslog", señalado que dicho tecnicismo en inglés no es reconocido con la traducción de "registro del sistema". ----------

En ese tenor, esta Autoridad solicitó el apoyo de la Procuraduría General de la República, requiriéndole realizara la traducción al castellano de los puntos sobre los cuales tanto el Área Convocante del Instituto Mexicano del Petróleo, como la empresa Optimiti Network, S.A. de C.V., manifestaron su desacuerdo respecto a la traducción exhibida por las inconformes. -----

Que con fecha cuatro de diciembre del dos mil catorce, se recibió en esta Área de Responsabilidades, el oficio con número de folio 81898 del veintiocho de noviembre del mismo año, suscrito por la C. Rosa María Cervantes Negrete, perito traductor del Departamento de Traducción, Dirección General de Especialidades Periciales Documentales de la Procuraduría General de la República, a través del cual emite el dictamen que le fue solicitado a dicha Procuraduría, y que rindió en los siguientes términos: ----------

"...

PRIMERA PARTE

A continuación cito en el orden en que aparecen los cuestionamientos por parte del Instituto Mexicano del Petróleo (en lo sucesivo el IMP), incluidos en el manifiesto de fecha 30 de octubre de 2014. El primer cuestionamiento se dividió en dos incisos A) y B) para mayor claridad

PRIMER CUESTIONAMIENTO

A) Respecto a la traducción que realiza de la página 2 último inciso de los dispositivos soportados por fortianalyzer con dirección http://www.fortinet.com/sites/default/files/productdatasheets/fortianalyzer-3500E.pdf (anexo 1), en dicho documento se encuentra en inglés (sic) la siguiente frase "any syslog-compatible device" lo cual lo traducen como "cualquier dispositivo compatible con el registro del sistema" ***siendo que syslog es un estándar para él (sic) envío de registro, siendo una palabra técnica que no tiene la connotación que se le quiere dar en dicha traducción..."***

***Análisis del perito**: Con respecto a la frase referida por el IMP: any syslog-compatible device; dicha frase se localizó en el legajo remitido por la autoridad, al anverso de la página 13 parte inferior izquierda (la cual se repite como Anexo 1, página 38 de dicho legajo) y la traducción de la misma se localiza al final de la*

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

página 16 en donde aparece: Cualquier Dispositivo Compatible con el Registro del Sistema. En esta traducción la palabra syslog se tradujo como "registro del sistema".

Al no encontrar la definición del término syslog en las fuentes escritas disponibles en el Departamento de Traducción, se consultó en Internet la página www.networkmagnagementsoftware.com/what-is-syslog, en donde syslog se define en inglés como:

> *"Syslog is a way for network devices to send event messages to a logging server – usually know as a Syslog server".*

A continuación me permito traducir esta definición:

> *Syslog es la forma en que los dispositivos de red envían mensajes de evento a un servidor de registro normalmente conocido como servidor Syslog.*

Y en la página http://hptechnologyconsultant.blogspot.mx/ se localizó la siguiente definición en español.

*"**SYSLOG**: es un estándar de facto para el envío de mensajes de registro en una red informática IP. Por syslog se conoce tanto al protocolo de red como a la aplicación o biblioteca que envía los mensajes de registro".*

*Por otra parte, en las siguientes dos páginas. Como configurar Kiwi Syslog server | eHow en español www.ehowenespanol.com/configurar-kiwi-**syslog**-server-como_151613/ y Recepción Syslog TCP/UDP – ERMEZ Hard& Soft - www.ermez.com/.../Recepcion_**Syslog**_TCP_UDP.htm. En cache, el termino syslog se deja en inglés.*

Finalmente se consultó el termino Registro del sistema en el Diccionario de Informática e Internet Microsoft® en donde aparece traducido al inglés como System Registry.

***Opinión del perito**: Con base en las fuentes consultadas, sería un error traducir el termino syslog como registro del sistema en este contexto y, en todo caso, debería conservarse en inglés cuando el texto va dirigido a un público especializado o bien explicarlo cuando el público receptor no sea especializado.*

***B)** La segunda parte del primer cuestionamiento señala "el mismo inconforme en otro de sus documentos que traduce, el llamado "inside Fortianalyzer" de la página web http://docs-legacy.fortinet.com/fa/inside-fortianalyzer-50.pdf (anexo 2), el cual en su página 1 inciso interoperability, contiene la palabra syslog y no la traduce en español.*

***Análisis del perito**: En la página 27 del legajo remitido por la autoridad, en el penúltimo renglón aparece el termino SYSLOG (que se repite en el Anexo 2 página 40 del legajo) y en la página 29 en la traducción en español se conservó en inglés.*

***Opinión del perito**: La traducción en estudio no fue homologada en cuanto al término syslog ya que en una parte del documento dicho término se tradujo erróneamente como "registro del sistema" y en otra parte se conservó en idioma inglés SYSLOG.*

...

SEGUNDA PARTE

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

Ahora procedo a emitir mi opinión sobre las observaciones vertidas por el Administrador Único de OPTIMITI NETWORK, S.A. de C.V. en documento sin fecha con sello de recibido en la función pública el 4 de noviembre del presente año.

A continuación cito una por una dichas observaciones para realizar un análisis y emitir una opinión.

...

2.- De la "hoja de datos" de la solución FortiAnalizer del rubro "Any Syslog-Compatible Device" (bajo la sección "FortiAnalyzer Supported Devices" en inglés) fue traducido como "Cualquier dispositivo compatible con el registro del sistema". Aquí se continua reflejando la limitante de colección de eventos desde diferentes tipos de fuentes por la solución ofertada, ya que "syslog" aunque es un estándar de facto para el envío de mensajes de registro a nivel aplicativo como protocolario típicamente a través de UDP por el puerto 514 no es soportado por todos los dispositivos de seguridad y por eso se buscan mecanismos de integración adicionales como WMI, ODBC y de desarrollo de parsers customizados para soportar dispositivos multimarca.

Al respecto, se destaca como observación que hay tecnicismos en inglés que en ocasiones no siempre es recomendable traducirlos y "syslog", al ser un estándar en la industria de redes, telecomunicaciones y seguridad no es "reconocido" con la traducción "registro de sistema" y que en todo caso está más referenciado al término "log".

***Análisis del perito**. Con respecto a la frase aludida en el presente 2: Any syslog-compatible device; dicha frase se localizó en el documento remitido por la autoridad al anverso de la página 13 parte inferior izquierda (que se repite en el Anexo 1, página 38) y la traducción de la misma se localiza al final de la página 16 en donde aparece: Cualquier Dispositivo Compatible con el Registro del Sistema. En esta traducción la palabra syslog se tradujo como "registro del sistema".*

Al no encontrar la definición del término syslog en las fuentes escritas disponibles en el Departamento de Traducción, se consultó en Internet la página www.networkmagnagementsoftware.com/what-is-syslogen donde syslog se define en inglés como:

"Syslog is a way for network devices to send event messages to a logging server – usually as a Syslog Server."

A continuación me permito traducir esta definición.

Syslog es la forma en que los dispositivos de red envían mensajes de evento a un servidor de registro normalmente conocido como servidor Syslog.

De igual forma en la página http://hptechnologyconsultant.blogspot.mx/ se encuentra la siguiente definición en español.

*"**SYSLOG**: es un estándar de facto para el envío de mensajes de registro en una red informática IP. Por syslog se conoce tanto al protocolo de red como a la aplicación o biblioteca que envía los mensajes de registro".*

*Por otra parte, en las siguientes dos páginas: Como configurar Kiwi Syslog Server |eHow en Español. www.ehowenespanol.com/configurar-kiwi-**syslog**-server-como_151613/ y Recepción Syslog TCP/UDP - ERMEZ Hard& Soft - www.ermez.com/.../Recepcion_**Syslog**_TCP_UDP.htm En cache, el termino syslog se deja en inglés.*

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

Finalmente se consultó el termino Registro del sistema en el Diccionario de Informática e Internet Microsoft® en donde aparece traducido al inglés como System registry.

***Opinión del perito**. Con base en las fuentes consultadas sería un error traducir el termino syslog como registro del sistema en este contexto y, en todo caso, debería conservarse en inglés cuando el texto va dirigido a un público especializado o bien explicarlo cuando el público receptor no sea especializado. Es importante señalar que una gran parte de la observación en el punto dos citado arriba se relaciona con cuestiones del cumplimiento con los requisitos, dichas cuestiones no son materia de la especialidad de traducción."*

Documental pública que se valora con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción II, 197 y 202 del Código Federal de Procedimientos Civiles, de la que se advierte que la C. Rosa María Cervantes Negrete, personal de la Procuraduría General de la República, al emitir su dictamen en traducción, refiere que con base a las fuentes consultadas, sería un error traducir el término "syslog" como registro del sistema, y que en ese contexto, debería conservarse en inglés el término "syslog", cuando el texto va dirigido a un público especializado; además de que la traducción presentada por las inconformes no fue homogénea, pues como ya se dijo en unas partes Syslog fue traducido erróneamente como "registro del sistema" y en otras se conservó dicho término en inglés.----------

Refiere la perito, que se consultó el término "Registro del Sistema", que es como se tradujo el concepto "Syslog" por parte de las inconformes, consulta que realizó en el Diccionario de Informática e Internet Microsoft, en donde aparece traducido al inglés como "System Registre", por lo que quedó asentado por parte de la perito, que en su opinión, el término Syslog "... ***se tradujo erróneamente*** *como "registro del sistema."* ----------

En razón de lo anterior, la traducción de la hoja de datos de la solución FortiAnalyzer del rubro "any syslog-compatible device" debe entenderse como "Cualquier dispositivo compatible con Syslog". ----------

Lo anterior se correlaciona con la matriz de cumplimiento presentada por las inconformes como parte de su propuesta con motivo de su participación dentro de la Licitación Pública Electrónica de Carácter Nacional a precio fijo No. LA-018T0O004-N152-2014, en la que respecto al numeral 20 del Inciso "III) Sistema de almacenamiento, reporteo, análisis y correlación de eventos de seguridad" que en sus página 15 y 18 de la citada matriz, se señaló lo siguiente: -

"...

Matriz de cumplimiento

		Cumple/No cumple	Documento	Hoja /columna/Reglón	Párrafo	referencia	Traducción simple al español
III) Sistema almacenamiento, reporteo, análisis							

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

y correlación de eventos de seguridad							
...							
20. Posibilidad de recibir logs de terceros al menos vía SYSLOG, WMI, ODBC e integración vía parsers personalizados (customizado)		SYSLOG	FortiAnalyzer 1000D	Hoja 2/Columna 2/Renglón 40	FortiAnalyzer Suported Devices	Any Syslog-Compatible Device	Cualquier Dispositivo Syslog-Compatible
		WMI					
			FortiAnalyzer-1000D	Hoja 2/Región17	JSON and XML (WEB Services)	APIs are available on all FortiAnalyzer hardware models and virtual machines. JASON API-Allows MSSPs/large enterprises to manipulate Fotianalyzer reports, charts/datasets and objects	APIs están disponibles en todos los modelos de hardware FortiAnalyzer y máquinas virtuales. API de JSON-Permite MSSP/grandes empresas para manipular informes FortiAnalyzer gráficos/conjuntos de datos y objetos
		ODBC					

Documental privada que se valora con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción III, 197 y 203 del Código Federal de Procedimientos Civiles, de la que se advierte que las propias empresas inconformes señalan en su propuesta que su equipo FortiAnalyzer es compatible con cualquier dispositivo Syslog, sin hacer ninguna alusión a los protocolos WMI, OBDC y vía parsers personalizados.----------

Esto es, del análisis a dicha matriz de cumplimiento, se advierte que las inconformes únicamente refieren que el equipo FortiAnalyzer que ofrecen, es compatible con SYSLOG, ya que respecto a los protocolos WMI y OBDC, en dicha matriz únicamente los menciona en la columna cumple/no cumple, pero no hacen ninguna otra indicación o señalamiento de ellos en alguna otra de las columnas, careciéndose de cualquier otro tipo de información sobre éstos protocolos; y respecto al protocolo vía parsers personalizados, las inconformes son completamente omisas en su matriz de cumplimiento.----------

Finalmente, es de resaltar por parte de esta Autoridad la conclusión VIGÉSIMAOCTAVA del dictamen en informática rendido por los CC. José Héctor Cortés Becerril y Jorge Alberto Grande Arriola, peritos oficiales en materia de Informática, adscritos a la Procuraduría General de la República, contenido en su oficio con número de folio 76311 del veinticinco de noviembre del dos mil catorce, y recibido en esta Área de Responsabilidades en la misma fecha, en el que concluyen lo siguiente: ----------

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

"CONCLUSIONES

...

***VIGÉSIMAOCTAVA**.- Determinar si los equipos que fueron ofertados por la inconforme cumplen técnicamente con requerimientos solicitados en Licitación Pública Electrónica de Carácter Nacional a precio fijo NO. LA-018T0O004-N152-2014, convocada por el Instituto Mexicano del Petróleo*
***RESPUESTA:** ...*

*En lo que respecta al dispositivo Fortianalyzer, en la convocatoria de la Licitación Pública Electrónica de Carácter Nacional a precio fijo NO. LA-018T0O004-N152-2014, en su página 43, inciso **20)**, claramente se indica: "Posibilidad de recibir logs de terceros al menos vía SYSLOG, WMI, ODBC e integración vía parsers personalizados (customizado).", por lo que de acuerdo a la hoja de datos del fabricante, en ninguna parte se especifica que cuente el dispositivos con manejo de los protocolos WMI y ODBC, o de programación de parsers personalizados, es decir protocolos adaptados a la necesidad de manejo de información en la red, y solamente se tiene el manejo del protocolo Syslog, por lo que se considera que no cumple con las especificaciones técnicas requeridas."*

Dictamen pericial que se valora con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción IV, 197 y 211 del Código Federal de Procedimientos Civiles, ambas disposiciones de aplicación supletoria en materia administrativa, en el que los CC. José Héctor Cortés Becerril y Jorge Alberto Grande Arriola, peritos oficiales en materia de Informática, adscritos a la Procuraduría General de la República, **concluyen que el equipo FortiAnalyzer ofertado por las inconformes de acuerdo a la hoja de datos del fabricante, en ninguna parte se especifica que el dispositivo cuente con manejo de los protocolos WMI y ODBC, o de programación de parsers personalizados, es decir protocolos adaptados a la necesidad de manejo de información en la red, y solamente se tiene el manejo del protocolo Syslog, por lo que se considera que no cumple con las especificaciones técnicas requeridas.** ----------

Que las inconformes reiteran en su escrito de alegatos que su equipo FortiAnalyzer 3000E, recibe logs de terceros al menos vía SYSLOG, WMI, ODBC e integración vía parses personalizados, de acuerdo a la páginas de internet que describe, situación que no fue demostrado como se ha precisado en párrafos anteriores. ----------

Por lo antes expuesto, se advierte por parte de esta Autoridad que el equipo FortiAnalyzer 3000E, propuesto por las empresas inconformes con el que pretendieron cumplir con los requerimientos de la Convocatoria a la Licitación Pública Electrónica de Carácter Nacional a precio fijo, para la Contratación del Servicio de Seguridad Perimetral para la Red del IMP, No. LA-018T0O004-N152-2014, en el que se solicitó que *"...20) Posibilidad de recibir logs de terceros al menos vía SYSLOG, WMI, OBDEC e integración vía parsers personalizados..."* el mismo no cumplía con tal requerimiento, pues como se ha demostrado, el equipo FortiAnalyzer 3000E, únicamente maneja el protocolo SYSLOG, careciendo de los métodos de WMI, ODBC e integración vía parsers personalizados, en consecuencia, no es procedente el motivo de inconformidad hecho valer por las empresas inconformes respecto de este punto. ----------

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

CUARTO.- A continuación, con fundamento en lo establecido por la fracción IV artículo 73 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, se procede a la valoración de los medios de prueba ofrecidos por las inconformes, mediante sus escritos del veintiuno de julio y veintiséis de agosto de dos mil catorce, en términos del artículo 197 del Código Federal de Procedimientos Civiles, de aplicación supletoria en materia administrativa, las cuales se hacen consistir en: ----------

1.- LA DOCUMENTAL PÚBLICA, consistente en las copias certificadas de los poderes notariales con los que se acredita la personalidad de los promoventes y copia simple de las mismas para su cotejo.

2.- LAS DOCUMENTALES PÚBLICAS, consistente en las constancias originales del expediente abierto con motivo de la contratación número LA-018T0O004-N152-2014. Documentos que se ofrecen pero no se exhiben por estar en poder de la convocante, por lo que con fundamento en el artículo 66, fracción IV de la LASSP se solicita su remisión.

3.- LA PERICIAL en materia de ingeniería en electrónica y comunicaciones a cargo del Ingeniero Héctor Daniel Santillanes Chapa, en la que se efectuaran las siguientes preguntas:

¿Cuáles son las funcionalidades del equipo fortiDDoS 400B y señalar si mantienes la conexión como firewall?

¿Cuáles son los lenguajes, log y funcionalidades que puede leer y recibir el equipo fotianalyzer?

4.- LA DOCUMENTAL PRIVADA, consistentes en la traducción al español de las características técnicas de los equipos ofertados por mi representada, que están publicadas en los sitios de internet del fabricante y que son parte de la fe de hechos que se adjunta como prueba a esta inconformidad.

5. LA PRESUNCIONAL LEGAL Y HUMANA, en todo lo que favorezca a mi mandante.

6. LA INSTRUMENTAL DE ACTUACIONES, en todo lo que favorezca a los intereses de mi representada.

7.- LA DOCUMENTAL PÚBLICA, consistente en el oficio 350/AA/340/2014, mediante el cual rindió el informe en la inconformidad

8.-LA CONFESIÓN EXPRESA, consistente en las manifestaciones realizadas por la convocante al rendir su informe

9.- Las documentales privadas consistentes en la información técnica contenidas en las páginas de internet que se señalan a continuación:

http://www.cnte.com/products/fortinet-fortiddos-400b-security-appliance/specs/

http://securitiintelligence.com/gartner-2014-magic-quadrant-siem-security#.U_ZH3I6VsZH

http://www.fortinet.com/sites/default/files/productdatasheets/FortiAnalyzer-3500E.pdf

http://docs-legacy.fortinet.com/fa/inside-fotianalyzer-50.pdf

http://blog.fortinet.com/post/hyper-v-microsoft-sfree-vm-ready-for-primetime

https://partners.fortinet.com/FortiPartnerPortal/CMS/7Download.do?oid=9533

http://www.fortinet.com/sites/default/files/producdatasheets/FortiDDos-1000B.pdf

http://docs-legacy.fortinet.com/fddos/4-1-0/index.html#page/FortiDDos_handbook/basic_topology.html

Por lo que hace a la prueba marcada con el numeral 1, estas se valoran de conformidad con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción II, 197 y 202 del Código Federal de Procedimientos Civiles,

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

ambas disposiciones de aplicación supletoria en materia administrativa, misma que es insuficiente para las pretensiones del oferente, pues con dichos poderes únicamente se acredita la personalidad del [redacted] como Apoderado Legal de las empresas Servicios Alestra, S.A. de C.V. y Alestra, S. de R.L. de C.V., y del [redacted] como Apoderado Legal de la empresa SK Holdings, S.A. de C.V. ----------

Por lo que hace a las probanzas marcadas con los numerales 2, 3 7 y 8, ya fueron materia de análisis en el considerando que antecede, mismas que en obvio de repeticiones innecesarias, deberá estarse a lo expresado al respecto. ----------

Por lo que hace a la prueba marcada con el numeral 4, las inconformes ofrecen la traducción al español de las siguientes páginas de Internet: ----------

http://docs-legacy.fortinet.com/fddos/4-1-0/index.html#page/FortiDDoS_Handbook/differences_and_simularities.html

http://docs-legacy.fortinet.com/fddos/4-1-0/index.html#page/FortiDDoS_handbook/strategies_for_protection.html

http://docs-legacy.fortinet.com/fddos/4-1-0/index.html#page/FortiDDoS_Handbook/comparing_fortiddos_to_conventional_nba.html

Documental privada que se valora de conformidad con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción III, 197 y 203 del Código Federal de Procedimientos Civiles, ambas disposiciones de aplicación supletoria en materia administrativa, mismas que resultan insuficientes, ya que no acredita los extremos que pretende hacer valer con su ofrecimiento, pues de su contenido se advierte que se mencionan aspectos tales como diferencias y similitudes con los firewalls convencionales, estrategias para la protección, comportamiento del FortiDDoS con el análisis convencional del comportamiento de la red (NBA), sin que en ninguno de ellos se refiera a que el equipo FortiDDoS 400B, no mantenga el estado de la conexión, y por el contario hacen mención que hay algunas características de FortiDDoS que son similares a un firewall.----------

Respecto a las pruebas ofrecidas en los numeral 5 y 6, consistente en la instrumental de actuaciones y la presuncional legal y humana, las mismas no tienen vida propia, ya que derivan de todas y cada una de las constancias del expediente administrativo en que se actúa, misma que la legislación federal ha dejado su valoración al prudente arbitrio de la autoridad resolutora, en tal virtud se considera, en atención a las reglas del Código Federal de Procedimientos Civiles, y a los principios procesales de la lógica, que las presentes pruebas derivan de las propias constancias que integran el expediente administrativo y que en el caso que nos ocupa se colige que su alcance jurídico se encuentra sujeto al valor otorgado a las mismas que han sido analizadas y valoradas en los párrafos que anteceden concluyéndose en base a los razonamientos lógico-jurídicos expuestos, que las mismas no favorecen a las inconformes. ---

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

Con el objeto de robustecer lo anterior, esta Autoridad se sustenta en la tesis jurisprudencia emitida por los Tribunales Colegiados de Circuito y publicada en el Semanario Judicial de la Federación del mes de mayo de 1997, página 65, tomo V, Novena Época, Tesis 11, misma que indica: ----------

> ***"PRUEBA INSTRUMENTAL DE ACTUACIONES Y PRESUNCIONAL LEGAL Y HUMANA, NO TIENEN VIDA PROPIA.***- *Las pruebas instrumental de actuaciones y presuncional legal y humana, prácticamente no tiene desahogo, es decir, que no tiene vida propia, pues no es más que el nombre que en la práctica se ha dado a la totalidad de las pruebas recabas en juicio, por lo que respecta a la primera, y por lo que respecta a la segunda, esta deriva de las mismas pruebas que existen en las constancias de autos"*

Finalmente, por lo que hace a la prueba marcada con el numeral 9, consistentes en la documental consistente en la traducción al español de la información técnica contenidas en páginas de internet, es de señalar que las siguientes páginas ya fueron analizas, por lo que obvio de repeticiones innecesarias deberá estarse a lo ya expresado al respecto: ----------

http://www.fortinet.com/sites/default/files/productdatasheets/FortiAnalyzer-3500E.pdf

http://docs-legacy.fortinet.com/fa/inside-fortianalyzer-50.pdf

http://www.fortinet.com/sites/default/files/productdatasheets/FortiDDos-1000B.pdf

http://docs-legacy.fortinet.com/fddos/4-1-0/index.html#page/FortiDDos_Handbook/basic_topology.html

http://www.cnte.com/products/fortinet-fortiddos-400b-security-appliance/specs/

Ahora bien, esta Autoridad procede a valorar la traducción al español de la información técnica contenidas en las páginas de internet: ----------

http://securityintelligence.com/gartner-2014-magic-quadrant-siem-security/#._ZH321VsZh

http://blog.fortinet.com/post/hyper-v-microsoft-Sfree-vm-ready-for-primetime

Documentales privadas que se valoran de conformidad con lo señalado en el artículo 50 de la Ley Federal de Procedimiento Administrativo, en relación con los numerales 79, 93, fracción III, 197 y 203 del Código Federal de Procedimientos Civiles, ambas disposiciones de aplicación supletoria en materia administrativa, mismas que resultan insuficientes, ya que no acreditan los extremos que pretende hacer valer con su ofrecimiento, pues si bien su contenido hace referencia a sistemas de seguridad, también lo es, que en ningún momento aluden o mencionan a los equipos de la marca Fortinet que fueron propuestos por las inconformes, y que cumplen con los requerimientos de la multicitada convocatoria ----------

Finalmente, como ha quedó demostrado en el considerando tercero, se desahogó la prueba pericial ofrecida por la empresa Optimiti Network, S.A. de C.V., en su calidad de tercero, y que en obvio de repeticiones innecesarias, deberá estarse a lo ya expresado al respecto. Así también, respecto al Área Convocante, fueron formulados a los peritos presentados por las

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084 facosta@imp.mx

empresas inconformes, por el tercero interesado, así como de la Procuraduría General de la República, los cuestionamientos planteados en su informe. ----------

QUINTO.- Por todo lo anteriormente expuesto, esta Área de Responsabilidades determina que los agravios que hicieron valer las empresas Servicios Alestra, S.A. de C.V., Alestra, S. de R.L. de C.V., y SK Holdings, S.A. de C.V., son infundados, por lo que de conformidad con lo dispuesto en el artículo 74, fracción II de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, se declara infundada la inconformidad promovida en contra del fallo de fecha once de julio del dos mil catorce, correspondiente a la Licitación Pública Electrónica, de Carácter Nacional a precio fijo, para la Contratación del Servicio de Seguridad Perimetral para la Red IMP, No. LA-018T0O004-N152-2014. ----------

Por lo anteriormente expuesto y fundado, es de resolverse y al efecto se: ----------

R E S U E L V E

PRIMERO.- Resultan infundados los agravios que hicieron valer las empresas Servicios Alestra, S.A. de C.V., Alestra S. de R.L. de C.V., y SK Holdings, S.A. de C.V., por lo que de conformidad con lo dispuesto en el artículo 74, fracción II de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, se determina declarar infundada la inconformidad promovida en contra del fallo de fecha once de julio del dos mil catorce, correspondiente a la Licitación Pública Electrónica, de Carácter Nacional a precio fijo, para la Contratación del Servicio de Seguridad Perimetral para la Red IMP, No. LA-018T0O004-N152-2014. ----------

SEGUNDO.- La presente resolución es recurrible de conformidad con lo establecido en el artículo 83 de la Ley Federal de Procedimiento Administrativo.----------

TERCERO.- Notifíquese a las partes y en su oportunidad archívese el presente expediente. -

ASÍ LO RESOLVIÓ Y FIRMA EL TITULAR DEL ÁREA DE RESPONSABILIDADES DEL ÓRGANO INTERNO DE CONTROL EN EL INSTITUTO MEXICANO DEL PETRÓLEO. -----

LIC. FRANCISCO JAVIER ACOSTA MOLINA

Elaboró: Adalberto Rodríguez Alcántara

"En términos de lo dispuesto en los artículos 13, 14 y 18 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, en esta versión pública se suprimió información clasificada como reservada o confidencial".

Eje Central Lázaro Cárdenas Norte No. 152, Col San Bartolo Atepehuacan, C.P. 07730, Delegación Gustavo A. Madero, México, D.F.

Tel.: (55) 9175 8084.facosta@imp.mx