INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO
A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES
DIRECCIÓN GENERAL DE ADMINISTRACIÓN
DIRECCIÓN DE RECURSOS MATERIALES Y SERVICIOS GENERALES
SUBDIRECCIÓN DE ADQUISICIONES Y CONTROL PATRIMONIAL

ACTA DE FALLO

Procedimiento de contratación: **Licitación**
Carácter del procedimiento: **Internacional Abierta**
Clave interna: **LPIA-006HHE001-016-17**
Clave electrónica: **LA-006HHE001-E74-2017**

Descripción: **Adquisición de una solución de seguridad de aplicaciones.**

En la Ciudad de México, siendo las **18:00 horas** del día **27 de noviembre de 2017**, en la sala de licitaciones electrónicas ubicada en la planta baja del edificio sede del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (en adelante INAI), sito en Av. Insurgentes Sur No. 3211, Col. Insurgentes Cuicuilco, Delegación Coyoacán, C.P. 04530 (en adelante domicilio de la Convocante), se reunieron los servidores públicos del INAI cuyos nombres, representaciones y firmas se asientan en este documento, con el objeto de llevar a cabo el evento en que tendrá verificativo el Fallo del procedimiento de contratación antes referido.----------
---

1. Se hace constar que la reunión fue debidamente instalada en la fecha antes citada y presidida por el Lic. Ibo Brito Brito, Subdirector de Adquisiciones y Control Patrimonial. Esto, con fundamento en el Capítulo I, numeral *4.2 Responsables de presidir eventos de los procedimientos de contratación*, del documento denominado "Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales" (en adelante las Balines), quien pasó lista de asistencia, encontrándose presentes los servidores públicos siguientes:----------
---
Por la Dirección General de Tecnologías de la Información, Área técnica y requirente.----------
Mtro. Guillermo Preciado López, Director de Soluciones Tecnológicas ----------
Por el Órgano Interno de Control----------
Lic. Marco Antonio Contreras Uribe, Auditor.----------
---

2. El Lic. Ibo Brito Brito, con fundamento en el artículo 36, fracciones II y VI del Reglamento de Adquisiciones, Arrendamientos y Servicios del Instituto Federal de Acceso a la Información y Protección de Datos (en adelante el Reglamento) y del Capítulo I, numeral 4.3 *Responsables de evaluar las proposiciones* de las Balines, informa que una vez realizado el análisis cualitativo por la Convocante de los *"Documentos e información que deberán presentar los licitantes como parte de su proposición"*, citados en el apartado 6 de la Convocatoria de este procedimiento de contratación (en adelante la Convocatoria), da a conocer lo siguiente:

La proposición presentada por el licitante **GRUPO DE TECNOLOGIA CIBERNETICA, S.A. DE C.V.,** cumple con las manifestaciones bajo protesta de decir verdad que se solicitan como requisitos de participación establecidos en el numeral 6.3 de la convocatoria.

Asimismo, por lo que corresponde al análisis jurídico, fue emitido el Dictamen legal por la Dirección General de Asuntos Jurídicos del INAI, mediante oficio INAI/DGAJ/3083/17, de fecha 27 de noviembre de 2017, debidamente firmado por su titular, Mtro. Pablo Francisco Muñoz Díaz, derivado de la revisión a la documentación presentada por el licitante participante para acreditar su personalidad jurídica y en su caso su existencia legal, mediante el cual se determinó lo siguiente:

La proposición presentada por el licitante **GRUPO DE TECNOLOGIA CIBERNETICA, S.A. DE C.V.**: *Presenta Anexo 3, en el cual, se omite requisitar el siguiente apartado del formato establecido en la convocatoria:*

- *Fecha de inscripción en el Registro Público de Comercio de las reformas del acta constitutiva.*

ACTA DE FALLO

Procedimiento de contratación: **Licitación**
Carácter del procedimiento: **Internacional Abierta**
Clave interna: **LPIA-006HHE001-016-17**
Clave electrónica: **LA-006HHE001-E74-2017**

Descripción: **Adquisición de una solución de seguridad de aplicaciones.**

Con relación a lo antes expuesto del licitante **GRUPO DE TECNOLOGIA CIBERNETICA, S.A. DE C.V.**, esta convocante manifiesta que con fundamento en el penúltimo párrafo del artículo 34 del Reglamento, que a la letra se cita: *"Entre los requisitos cuyo incumplimiento no afecte la solvencia de la proposición se considerarán..." "...el no observar requisitos que carezcan de fundamento legal o cualquier otro que no tenga por objeto determinar objetivamente la solvencia de la proposición presentada.",* esta proposición fue considerada solvente en este aspecto y pasó a ser evaluada técnicamente. ----------

3. El Lic. Ibo Brito Brito hace constar que la Dirección General de Tecnologías de la Información es el área requirente, técnica y responsable de la verificación y evaluación cualitativa de las proposiciones técnicas y económicas de este procedimiento de contratación, en términos de lo dispuesto por el artículo 2 fracción III del Reglamento, quedando bajo su estricta responsabilidad la formulación del dictamen técnico-económico que se emite con relación a lo dispuesto en el artículo 34 del Reglamento, así como de acuerdo con el Capítulo I, numeral *4.3 Responsables de evaluar las proposiciones de las Balines* y con fundamento en el apartado *5.1 Criterios de Evaluación* de la Convocatoria, mismo que fue recibido mediante oficio No. INAI/SE/DGTI/891/17, de fecha 24 de noviembre de 2017. El dictamen referido adjunto al oficio fue presentado debidamente firmado por el Ing. José Luis Hernández Santana, Director General de Tecnologías de la Información; Mtro. Guillermo Preciado López, Director de Soluciones Tecnológicas; e Ing. Andrés Franco Bejarano, Subdirector de Operaciones, de acuerdo con lo siguiente ----------

----------DICTAMEN DE PUNTOS Y PORCENTAJES----------

CARACTERÍSTICAS DEL BIEN O BIENES OBJETO DE LA PROPUESTA TÉCNICA. Puntaje máximo 20 puntos

A	Características Técnicas		PUNTOS MÁXIMOS	PUNTOS OTORGADOS
A1	El Licitante deberá cumplir con todas y cada una de las Especificaciones Técnicas de la Solución de Seguridad de Aplicaciones propuesta de acuerdo a lo indicado en el numeral **4. DESCRIPCIÓN DE LOS EQUIPOS Y SERVICIOS REQUERIDOS** del Anexo Técnico.		14	Grupo de tecnología Cibernética, S.A. de C.V.
	Cumple con las Especificaciones Técnicas de la Solución de Seguridad de Aplicaciones ofertada.	14		14

ACTA DE FALLO

Procedimiento de contratación: **Licitación**
Carácter del procedimiento: **Internacional Abierta**
Clave interna: **LPIA-006HHE001-016-17**
Clave electrónica: **LA-006HHE001-E74-2017**

Descripción: **Adquisición de una solución de seguridad de aplicaciones.**

A	Características Técnicas		PUNTOS MÁXIMOS	PUNTOS OTORGADOS
	No cumple con las Especificaciones Técnicas de la Solución de Seguridad de Aplicaciones ofertada.	0		

	Durabilidad o vida útil		PUNTOS MÁXIMOS	PUNTOS OTORGADOS
B1	El Licitante deberá incluir en su propuesta una carta del fabricante donde confirme la disponibilidad de refacciones por al menos los próximos 3 (tres) años para los equipos ofertados.		6	Grupo de tecnología Cibernética, S.A. de C.V.
	Carta del fabricante de los equipos ofertados especificando el tiempo de vida útil de 3 años o más	6		6
	Carta del fabricante de los equipos ofertados especificando que el tiempo de vida útil es de más de 1 año y menos de 3 años	0		

CAPACIDAD DEL LICITANTE. Puntaje máximo 13 puntos

A.- CAPACIDAD DE LOS RECURSOS ECONÓMICOS, TÉCNICOS Y DE EQUIPAMIENTO

A	CAPACIDAD DE LOS RECURSOS ECONÓMICOS, TÉCNICOS Y DE EQUIPAMIENTO	PUNTOS MÁXIMOS		PUNTOS OTORGADOS
A1	**El licitante deberá demostrar que cuenta con el personal técnico certificado por parte del Fabricante:** Para la evaluación de este rubro, el LICITANTE deberá demostrar que el equipo de trabajo es personal certificado de acuerdo a lo solicitado en los numerales: **5. SERVICIOS DE INSTALACIÓN Y SOPORTE TÉCNICO, 5.3. ADMINISTRADOR DE PROYECTO PARA LA IMPLEMENTACIÓN DE LA SOLUCIÓN5.4. LÍDER TÉCNICO y 5.2.1. MESA DE AYUDA** en el Anexo Técnico.			Grupo de tecnología Cibernética, S.A. de C.V.
	Administrador de Proyecto con certificación vigente del PMI	1	6	2
	Un Líder técnico que deberá contar con las siguientes certificaciones: Certified Information System Auditor (CISA) del ISACA Certified Information Security Manager (CISM) del ISACA Certified in Ethical Hacking (CEH) del EC-Council Master Seguridad Informática ITIL Foundation v3	3		
	Tres Operadores de la mesa de ayuda, que deberán contar con la certificación ITIL Foundation v3 y por lo menos uno de ellos con la certificación ITIL Operational Support and Analysis (OSA)	2		

ACTA DE FALLO

Procedimiento de contratación: **Licitación**
Carácter del procedimiento: **Internacional Abierta**
Clave interna: **LPIA-006HHE001-016-17**
Clave electrónica: **LA-006HHE001-E74-2017**

Descripción: **Adquisición de una solución de seguridad de aplicaciones.**

	CAPACIDAD DE LOS RECURSOS ECONÓMICOS, TÉCNICOS Y DE EQUIPAMIENTO	PUNTOS	PUNTOS MÁXIMOS	PUNTOS OTORGADOS
	El licitante deberá demostrar que cuenta capacidad técnica.			Grupo de Tecnología Cibernética, S.A. de C.V.
A2	El Licitante deberá presentar en su propuesta técnica, una carta del fabricante que lo acredite como distribuidor autorizado de la marca que oferta. La carta del fabricante deberá estar dirigida a la convocante mencionando la presente convocatoria.	2	3	3
	El Licitante deberá incluir en su propuesta técnica, una carta firmada por su representante legal, en la que se mencione que todo el equipamiento informático para el balanceo de aplicaciones, certificados SSL y Firewall de aplicaciones Web que oferta es nuevo y con soporte dentro de la República Mexicana.	1		
	El Licitante deberá proporcionar el servicio descrito en el numeral **5.2.1. Mesa de Ayuda**, del Anexo Técnico. La Mesa de ayuda para el reporte de fallas de la solución de Seguridad de Aplicaciones ofertada, tendrá como objetivo, dirigir los incidentes y requerimientos relacionados con dicha solución hacia el fabricante y deberá estar alineada a la metodología de Mejores Prácticas de ITIL y contar con una herramienta de gestión avalada ante Pink Elephant. Lo que se deberá demostrar a través de la consulta del portal de Pink Elephant, o mediante carta firma por representante legal de Pink Elephant: http://www.pinkelephant.com/PinkVERIFY/PinkVERIFY_2011_Tool sets.htm	3	3	3

A.3.- PARTICIPACIÓN DE DISCAPACITADOS	PUNTOS MÁXIMOS	PUNTOS OTORGADOS
PERSONAS CON DISCAPACIDAD O SI DENTRO DE LA PLANTILLA LABORAL (PARA PERSONAS MORALES) CUENTA CON PERSONAL DISCAPACITADO.		Grupo de Tecnología Cibernética, S.A. de C.V.
Mínimo 5% del total de la plantilla para personas morales y constancia para personas físicas. El LICITANTE para poder obtener estos puntos deberá presentar el aviso de alta al régimen obligatorio del Instituto Mexicano del Seguro Social, con por lo menos seis meses de antigüedad a la presentación de las propuestas de este proceso de contratación.	0.5	0

ACTA DE FALLO

Procedimiento de contratación: **Licitación**
Carácter del procedimiento: **Internacional Abierta**
Clave interna: **LPIA-006HHE001-016-17**
Clave electrónica: **LA-006HHE001-E74-2017**

Descripción: **Adquisición de una solución de seguridad de aplicaciones.**

A.4.- PARTICIPACIÓN DE MIPYMES	PUNTOS MÁXIMOS	PUNTOS OTORGADOS
SI EL LICITANTE PERTENECE A LAS MIPYMES Y DENTRO DE LOS SERVICIOS QUE OFRECEN PRODUCE BIENES CON INNOVACIÓN TECNOLÓGICA		Grupo de tecnología Cibernética, S.A. de C.V.
Para poder obtener estos puntos, el LICITANTE deberá acreditar mediante constancia emitida por el Instituto Mexicano de la Propiedad Industrial, la cual no podrá tener una vigencia mayor a cinco años.	**0.5**	0

EXPERIENCIA Y ESPECIALIDAD DEL LICITANTE. Puntaje máximo 7 puntos

A.- EXPERIENCIA DEL LICITANTE

A1. EXPERIENCIA DEL LICITANTE EN CONTRATOS SIMILARES AL OBJETO DE ESTE PROCESO DE CONTRATACIÓN	PUNTOS MÁXIMOS	PUNTOS OTORGADOS
El licitante deberá comprobar su experiencia en el suministro de Soluciones de Seguridad de Aplicaciones similares a los solicitados en la presente licitación. Para obtener estos puntos el licitante deberá acreditar mediante la presentación de copia de contratos celebrados debidamente suscritos y/o órdenes de compra donde se describa alguna Solución de Seguridad de Aplicaciones similar a lo solicitado por la convocante. Se tomará como referencia la fecha de firma de cada contrato. Se tomarán en cuenta únicamente contratos que hayan concluido a la fecha de presentación de las propuestas de la presente licitación. Se asignará la mayor puntuación o unidades porcentuales (3.5 puntos) a los LICITANTES que acrediten el mayor número de años de experiencia (seis años), mediante la presentación de contratos. Se evaluará la cantidad de años de experiencia y la cantidad de años máxima a considerar para obtener la máxima puntuación que será de 6 años. Si algún LICITANTE acredita más años de los máximos solicitados, sólo se le asignara la mayor puntuación o unidades porcentuales, 3.5 puntos, que corresponden al límite máximo determinado por esta convocante. A partir del o los LICITANTES que hubieren obtenido la mayor puntuación o unidades porcentuales asignadas (3.5 puntos) en términos de lo dispuesto en el párrafo que antecede, se distribuirá de manera proporcional la puntuación o unidades porcentuales a los demás LICITANTES en razón de los años de experiencia que acrediten, aplicando para ello una regla de tres, con la siguiente formula: Experiencia = (P*a)/M Dónde: "P" es igual a los puntos a otorgar "a" es igual al número de años acreditados por el LICITANTE evaluado y estos sean aceptados. "M" es igual al máximo de años acreditados por un LICITANTE en la licitación, no más de 6 años, y estos sean aceptados. A los LICITANTES que no acrediten el mínimo de experiencia requerida o determinada por la convocante, 1 año, no se les asignara puntuación alguna o unidades porcentuales	3.5	Grupo de tecnología Cibernética, S.A. de C.V. 3.5

ACTA DE FALLO

Procedimiento de contratación: **Licitación**
Carácter del procedimiento: **Internacional Abierta**
Clave interna: **LPIA-006HHE001-016-17**
Clave electrónica: **LA-006HHE001-E74-2017**

Descripción: **Adquisición de una solución de seguridad de aplicaciones.**

B.- ESPECIALIDAD DEL LICITANTE

B1. ESPECIALIDAD DEL LICITANTE	PUNTOS MÁXIMOS	PUNTOS OTORGADOS
El licitante deberá comprobar su especialidad en el suministro de soluciones de Seguridad similares a los solicitados en la presente licitación. Para obtener estos puntos el licitante deberá acreditar mediante la presentación de copia de contratos celebrados debidamente suscritos y/o órdenes de compra donde se describa alguna Solución de Seguridad de Aplicaciones similar a lo solicitado por la convocante. Se tomarán en cuenta únicamente contratos que hayan concluido a la fecha de presentación de las propuestas de la presente licitación. Se asignará la mayor puntuación o unidades porcentuales (3.5 puntos) a los LICITANTES que acrediten el mayor número de contratos (6 contratos), mediante la presentación de contratos y/o órdenes de compra. Se evaluará la cantidad de contratos y la cantidad máxima de contratos a considerar para obtener la máxima puntuación que será de 6 contratos. Si algún LICITANTE acredita más contratos o número de anexos de los máximos solicitados, sólo se le asignara la mayor puntuación o unidades porcentuales, 3.5 puntos, que corresponden al límite máximo determinado por esta convocante que son 6 contratos. A partir del o los LICITANTES que hubieren obtenido la mayor puntuación o unidades porcentuales asignadas (3.5 puntos) en términos de lo dispuesto en el párrafo que antecede, se distribuirá de manera proporcional la puntuación o unidades porcentuales a los demás LICITANTES en razón de los años de experiencia que acrediten, aplicando para ello una regla de tres, con la siguiente formula: *Experiencia = (P*a)/M* Dónde: "*P*" es igual a los puntos a otorgar "*a*" es igual al número de contrataos y/o órdenes de compra acreditados por el LICITANTE evaluado y estos sean aceptados. "*M*" es igual al máximo de contrataos y/o órdenes de compra acreditados por un LICITANTE en la licitación, no más de 6 contratos y/o órdenes de compra, y estos sean aceptados. A los LICITANTES que no acrediten el mínimo de especialidad requerida o determinada por la convocante, 3 contratos, no se les asignara puntuación alguna o unidades porcentuales.	3.5	Grupo de tecnología Cibernética, S.A. de C.V. 3

CUMPLIMIENTO DE CONTRATOS. Puntaje máximo 10 puntos

C1 CUMPLIMIENTO DE CONTRATOS	PUNTOS MÁXIMOS	PUNTOS OTORGADOS
El licitante deberá integrar en su propuesta técnica, copia de los documentos con los que acredite haber dado cumplimiento adecuado y oportuno de contratos y/o órdenes de compra similares a los establecidos en la presente convocatoria, que acrediten el suministro de soluciones de Seguridad de Aplicaciones que son iguales o muy similares a la naturaleza, características, volumen, complejidad, magnitud o condiciones a los que se están solicitando en el Anexo técnico de la presente convocatoria.	10	Grupo de tecnología Cibernética, S.A. de C.V. 10

ACTA DE FALLO

Procedimiento de contratación: **Licitación**
Carácter del procedimiento: **Internacional Abierta**
Clave interna: **LPIA-006HHE001-016-17**
Clave electrónica: **LA-006HHE001-E74-2017**

Descripción: **Adquisición de una solución de seguridad de aplicaciones.**

El LICITANTE para poder obtener estos puntos deberá integrar en su propuesta técnica copia simple de cartas o copias simples de documentos que acrediten la liberación de la garantía de cumplimiento de contratos adecuada y oportunamente (liberación de fianzas) o cartas dirigidas al INAI donde el cliente especifique que los bienes y/o servicios se recibieron en tiempo y forma debiendo señalar número de contrato, fecha y alcance de la contratación. Los documentos o cartas presentadas deberán estar relacionados con los contratos presentados para el rubro de especialidad del LICITANTE. Se tomarán en cuenta únicamente contratos que hayan concluido a la fecha de presentación de las propuestas técnicas y económicas en la mencionada licitación. Se asignará la mayor puntuación o unidades porcentuales (10 puntos) a los LICITANTES que acrediten el mayor número de cartas o documentos (6 contratos) que acrediten la liberación de la garantía de cumplimiento de contratos adecuada y oportunamente (liberación de fianzas) de cumplimiento de los contratos presentados para comprobar la experiencia y/o especialidad. Si algún LICITANTE acredita más cartas o liberación de garantías de las solicitadas (6 cartas), sólo se le asignara la mayor puntuación o unidades porcentuales, 10 puntos, que corresponden al límite máximo determinado por esta convocante. A partir del o los LICITANTES que hubieren obtenido la mayor puntuación o unidades porcentuales asignadas en términos de lo dispuesto en el párrafo que antecede, se distribuirá de manera proporcional la puntuación o unidades porcentuales a los demás LICITANTES en razón de los documentos que acrediten, aplicando para ello una regla de tres, con la siguiente formula: Cumplimiento = (P*B)/M Dónde: "P" es igual a los puntos a otorgar "B es igual al número de cartas o documentos que acrediten la liberación de la garantía de cumplimiento de contratos presentadas por el LICITANTE evaluado y estas sean aceptadas. "M" es igual al máximo de cartas o documentos que acrediten la liberación de la garantía de cumplimiento de contratos presentadas por un LICITANTE en la licitación y estas sean aceptadas. A los LICITANTES que no acrediten el mínimo de cumplimento de contratos requerido o determinado por la convocante, 1 contrato, no se les asignara puntuación alguna o unidades porcentuales.		

Resumen de la ponderación de los criterios de evaluación técnica:

PONDERACIÓN DE LOS CRITERIOS	PUNTOS	Grupo de Tecnología Cibernética, S.A. de C.V.
CARACTERÍSTICAS DEL BIEN O BIENES OBJETO DE LA PROPUESTA TÉCNICA	20	20
CAPACIDAD DEL LICITANTE	13	8
EXPERIENCIA Y ESPECIALIDAD DEL LICITANTE	7	6.5
CUMPLIMIENTO DE CONTRATOS	10	10
Puntaje máximo para cada licitante en la evaluación técnica	**50**	**44.5**

ACTA DE FALLO

Procedimiento de contratación: **Licitación**
Carácter del procedimiento: **Internacional Abierta**
Clave interna: **LPIA-006HHE001-016-17**
Clave electrónica: **LA-006HHE001-E74-2017**

Descripción: **Adquisición de una solución de seguridad de aplicaciones.**

RESULTADOS DE LA EVALUACIÓN TÉCNICA

Especificaciones	Cumplimiento
2. ALCANCE DEL SERVICIO	
El proveedor implementará una solución de balanceo y seguridad de aplicaciones en alta disponibilidad que permita asegurar y mantener la conectividad de los usuarios a las aplicaciones del INAI. Así mismo requiere que se mantenga y mejore el nivel de seguridad, a través del uso de certificados SSL y el uso de políticas a sus aplicaciones web.	Cumple
Deberá considerar lo siguiente:	
La solución integral ofertada deberá cumplir con las especificaciones técnicas establecidas en el presente documento. Las descripciones que se enuncian en este documento, relativas a componentes, especificaciones técnicas y requerimientos específicos de los equipos y servicios son las mínimas requeridas, por lo que los licitantes podrán ofertar equipos con especificaciones iguales o superiores a las solicitadas.	Cumple
Todo el Hardware y el Software deberán ser nuevos y con soporte dentro de la República Mexicana.	Cumple
Toda la información transferida a través del Hardware o contenida en este, será propiedad del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.	Cumple
· El proveedor deberá proporcionar, el hardware, software y servicios profesionales de implementación, soporte y mantenimiento necesarios para asegurar la correcta operación de todos los componentes de la solución. El proveedor debe contar con experiencia probada en:	Cumple
o Implementación de la solución integral de seguridad redes y aplicaciones.	Cumple
o Soporte técnico para atención de incidentes / problemas vía una mesa de servicios con herramientas adecuadas para control y seguimiento de casos con apego a ITILV3 como mínimo.	Cumple
o Cambios de configuraciones, actualizaciones, alta de nuevas funcionalidades.	Cumple
o Conocimientos comprobables sobre las infraestructuras ofertadas y sobre la seguridad a nivel de análisis, control de vulnerabilidades y consultoría de seguridad.	Cumple
· Los equipos serán entregados e instalados en el edificio sede del INAI sita en la ciudad de México, sita en Insurgentes Sur Nº 3211, Col Insurgentes Cuicuilco, Delegación Coyoacán, Ciudad de México C.P. 04530.	Cumple
3. DESCRIPCIÓN DE LOS EQUIPOS Y SERVICIOS REQUERIDOS.	
El licitante deberá ofertar la infraestructura de hardware y software necesaria para brindar el balanceo de aplicaciones, certificados SSL y Firewall de aplicaciones Web del INAI. Por lo que deberá considerar en su propuesta una solución que incluya como mínimo 2 (dos) equipos en Alta Disponibilidad (*High Ability - HA*).	Cumple
Para la presentación de las propuestas técnicas, cada uno de los ítems enumerados en esta sección de **descripción de los equipos y servicios requeridos**, deberán ser documentados punto por punto con referencias generadas por el fabricante, ya sea con documentos adjuntos o URL. Estas referencias deberán contener lo siguiente:	Cumple
· Nombre del documento donde se encuentra la información, página y citar el texto donde se acredite la funcionalidad solicitada.	Cumple
· En el caso de referencias en URL ésta deberá ser pública, en caso de no ser accesible se contará como no cubierto el punto.	Cumple

ACTA DE FALLO

Procedimiento de contratación: **Licitación**
Carácter del procedimiento: **Internacional Abierta**
Clave interna: **LPIA-006HHE001-016-17**
Clave electrónica: **LA-006HHE001-E74-2017**

Descripción: **Adquisición de una solución de seguridad de aplicaciones.**

Especificaciones	Cumplimiento
· Se deberá documentar la liga específica, el párrafo al que se hace referencia y citar el texto que describa la funcionalidad solicitada.	Cumple
· En caso de no presentar la información como se está solicitando se desechará la propuesta técnica.	Cumple
Los equipos y componentes de la solución propuesta deberán cumplir como mínimo con los siguientes requerimientos:	Cumple
· Debe soportar su implementación en modo transparente, actuando como un Bridge L2.	Cumple
· Debe implementar mecanismo de chequeo de "salud" en servicios remotos a través de al menos los siguientes protocolos: ICMP, TCP Echo, TCP, HTTP, HTTPS, DNS, RADIUS, SMTP, POP3, IMAP4, Contabilidad RADIUS, FTP, TCP Half, Open SSL TCP, SNMP, SSH, detección L2, UDP, ARP y NDP (IPv6).	Cumple
· Debe contar con la funcionalidad de Firewall stateful incluyendo IPv4 e IPv6.	Cumple
· Debe habilitar la configuración de directiva de firewall (permitiendo o bloqueando tráfico) basado en interfaces de entrada, interfaces de salida, dirección (o grupo de direcciones) IP de origen y destino y el servicio (o grupo de UDP y servicios TCP).	Cumple
· Debe permitir implementar políticas de firewall (bloquear o permitir nuevas conexiones) con base a los límites de conexión que se generan por dirección (o grupo de direcciones) IP de origen y destino, servicio (o grupo de servicio UDP y TCP).	Cumple
· Debe implementar la funcionalidad de bloqueo del tráfico basado en listas de reputación, las cuales son mantenidas y actualizadas recurrentemente por el fabricante de la solución.	Cumple
· Debe contar con un mecanismo de clasificación de la severidad de las conexiones bloqueados por reputación (Bajo, Medio y Alto), así como el registro de sus logs.	Cumple
· Debe ser capaz de bloquear el tráfico en función del país de origen conexión. La base de datos que asigna la dirección IP al país debe ser mantenido y actualizado periódicamente por el fabricante del equipo.	Cumple
· Debe contar con un mecanismo de clasificación de la severidad de las conexiones bloqueados con base al País (Bajo, Medio y Alto), así como el registro de sus logs.	Cumple
· Debe contar con un firewall de aplicaciones Web (WAF), basado en el análisis de las solicitudes y respuestas HTTP y su posterior mapeo con firmas de ataques, métodos permitidos y filtros usados para clasificar el tráfico.	Cumple
· Las políticas de aplicación web deben tomar la decisión de permitir, bloquear o alerta (a través de logs) de tráfico basado en el análisis de las peticiones HTTP o sus respuestas.	Cumple
· Debe ser posible de aplicar excepciones a la inspección del tráfico, mediante las políticas de firewall de aplicaciones web.	Cumple
· Debe ser posible aplicar políticas basadas en firmas que identifiquen ataques basados en las cabeceras HTTP, HTTP Request Body, y HTTP Response body.	Cumple
· Las firmas deben ser actualizadas por el fabricante de forma automática sin la necesidad de intervención por parte del administrador de la solución.	Cumple
· Las firmas deben tener niveles de severidad basado en Open Web Application Security Project (OWASP) Risk Rating Methodology.	Cumple
· Las firmas deben ser organizadas en categorías y subcategorías.	Cumple
· Debe ser posible implementar políticas de protección URL para permitir la detección de patrones o strings en los URL o extensiones de archivo.	Cumple
· Las políticas de protección URL deben tener acciones para bloquear o alertar (permitir y registrar) y deben permitir la clasificación de su severidad (alta, media y baja).	Cumple

ACTA DE FALLO

Procedimiento de contratación: **Licitación**
Carácter del procedimiento: **Internacional Abierta**
Clave interna: **LPIA-006HHE001-016-17**
Clave electrónica: **LA-006HHE001-E74-2017**

Descripción: **Adquisición de una solución de seguridad de aplicaciones.**

Especificaciones	Cumplimiento
· Las URLs y extensiones de archivos configuradas para bloquear, deben poder identificarse mediante el uso de expresiones regulares o strings.	Cumple
· Debe permitir, a través de políticas de HTTP, el control de: parámetros y métodos de HTTP request y códigos de respuesta HTTP.	Cumple
· Deben permitir el control del administrador por lo menos los siguientes parámetros HTTP request: longitud máxima de URL, la verificación del nombre de host, comprobación de versión de protocolo HTTP, número máximo de cookies de cabecera HTTP, el número máximo de cabeceras en una petición HTTP, Tamaño maximo cabecera HTTP, el número máximo de caracteres en un parámetro de la URL, tamaño máximo del cuerpo del mensaje HTTP.	Cumple
· Deben poderse configurar por el administrador por lo menos los siguientes parámetros de los métodos HTTP: permitir o bloquear el método HTTP, asignar una severidad (por lo menos tres niveles) para el método bloqueado o permitido. Por lo menos los siguientes métodos deben poderse evaluar: Connect, Delete, GET, HEAD, Options, POST, PUT y Trace.	Cumple
· El administrador debe poder controlar el rango de códigos de respuesta HTTP, ya sea bloqueando o alertando (posibilidad de generar log), así como establecer la severidad en al menos tres niveles para propósitos de registro.	Cumple
· Debe contar con políticas para identificar y bloquear ataques de Cross Site Scripting (XSS) e inyección de SQL.	Cumple
· Debe identificar los ataques Cross Site Scripting a través de análisis del contenido de la URL, el contenido de la cabecera HTTP referes, el contenido de la cabecera HTTP cookie y en el cuerpo de contenido del mensaje de HTTP request.	Cumple
· Debe identificar los ataques de inyeccion SQL a través de análisis del contenido de la URL, el contenido de la cabecera HTTP referes, el contenido de la cabecera HTTP cookie y en el cuerpo de contenido del mensaje de HTTP request.	Cumple
· El equipo debe identificar el tráfico con SQL Injection y XSS y el administrador debe ser capaz de establecer políticas para: bloquear el tráfico o alertarlo y definir el grado de severidad en por lo menos tres niveles para propósitos de registro.	Cumple
· Debería permitir a la configuración de los hosts o patrones de URL que no están sujetos al tratamiento del Firewall de tráfico HTTP. Se debe soportar la definición de los hosts y las URL usando expresiones regulares.	Cumple
· Debe tener mecanismo para prevenir ataques SYN Flood.	Cumple
· Debe permitir el cambiar los puertos HTTP, HTTPS, Telnet y SSH para fines de acceso remoto del equipo por el administrador.	Cumple
· Debe ser compatible con la sincronización de hora a través de NTP.	Cumple
· Debe proporcionar al menos dos tipos de copia de seguridad: Una sencilla que genera la configuración a nivel de línea de comandos y una segunda que complementa la primera con los archivos de configuración del sistema (páginas de error, scripts y archivos de bloque dirección IP asociada con los proveedores).	Cumple
· Debe permitir la actualización a través de la línea de comandos o de la interfaz gráfica.	Cumple
· Debe permitir que el proceso de upgrade en diferentes particiones.	Cumple
· Debe permitir la actualización de la base de datos de firmas de firewall de aplicaciones web, de reputación de direcciones IP y de IP basados en ubicación, todas estas de forma separada y sin necesidad de reiniciar el sistema.	Cumple
· Debe permitir la actualización programada de la base de datos de suscripción, donde se indique los días de la semana y hora del día.	Cumple

ACTA DE FALLO

Procedimiento de contratación: **Licitación**
Carácter del procedimiento: **Internacional Abierta**
Clave interna: **LPIA-006HHE001-016-17**
Clave electrónica: **LA-006HHE001-E74-2017**

Descripción: **Adquisición de una solución de seguridad de aplicaciones.**

Especificaciones	Cumplimiento
· Debe ser compatible con la configuración de un servidor de correo para el envío de alertas por correo electrónico.	Cumple
· Debe contar con servicio de agente SNMP v1, V2c y 3 (RFC 3414).	Cumple
· Debe permitir la configuración de eventos SNMP al menos en lo relacionado con niveles de uso de CPU, memoria y disco.	Cumple
· Debe ser compatible con el uso de certificados para la conexión del cliente incluyendo estos al menos: Extensión TLS Server Name Indicator (SNI), el almacenamiento local de certificados (certificados X.509 v3 claves privadas utilizadas por los servidores), el almacenamiento y el uso de certificados generados a partir de una determinada CA, OCSP (Online Certificate Status Protocol), el CRL (certificate revocation list) y la solicitud de certificado a una entidad emisora a través de SCEP (simple certificate enrollment protocol).	Cumple
· Throughput de al menos 20.0 Gbps	Cumple
· Throughput L7 RPS (Request per second) de al menos 1.5 M	Cumple
· Compresión de al menos 12 Gbps	Cumple
· Debe incluir instancias virtuales	Cumple
· Debe contar con al menos 8 interfaces gigabit ethernet RJ-45	Cumple
· Debe contar con al menos 4 interfaces 10 gigabit ethernet SFP	Cumple
· Las interfaces de red deben soportar el protocolo Ethernet con al menos las siguientes velocidades: 10 Mbps (half y full duplex), 100 Mbps (half y full duplex), 1000 Mbps (half y full duplex) y negociación automática	Cumple
· Debe ser compatible con PPPoE.	Cumple
· Debe ser compatible con CDP (Cisco Discovery Protocol).	Cumple
· Debe soportar el protocolo IEEE 802.3ad para el balanceo de tráfico entre los puertos.	Cumple
· Debe soportar VLAN y ser compatible con el protocolo IEEE 802.1Q.	Cumple
· Debe permitir el enrutamiento entre VLAN diferentes.	Cumple
· Debe soportar la configuración de rutas estáticas incluyendo la distancia administrativa de la misma para decidir el enrutamiento de paquetes.	Cumple
· Debe ser posible configurar políticas de enrutamiento basado en direcciones IP de origen y / o destino.	Cumple
· Debe ser compatible con OSPF v2 - RFC 2328.	Cumple
· Debe poder implementar NAT (Network Address Translation), de los siguientes tipos: Source NAT (cambiar la dirección IP de origen), mapeo 1-1 y traslado de puertos (TCP o UDP).	Cumple
· Debe asignar políticas de ancho de banda, teniendo en cuenta la dirección de origen, destino y el servicio (puertos TCP y UDP).	Cumple
· El equipo ofrecido debe ser capaz de abrir un número limitado de conexiones TCP al servidor real e insertar los paquetes generados por el cliente a estas conexiones, reduciendo la necesidad de establecer conexiones nuevas a los servidores y así aumentar el rendimiento del servicio.	Cumple
· Debe soportar Reverse Path Route caching, para asegurar que la respuesta a un cliente se enrute a través del mismo proveedor utilizado para recibir el mismo paquete.	Cumple
· Debe soportar balanceo de Capa 7 para los siguientes protocolos HTTP, HTTPs, RADIUS, RDP, SIP, TCPs, DNS, SMTP, RTMP, RTSP, MySQL.	Cumple
· Debe balancear el tráfico entre los servidores reales utilizando algoritmos propios y utilizando información de salud de los servidores.	Cumple
· Cuando existe comunicación cifrada, esta debe ser controlada por los protocolos SSL / TLS y la lista protocolos de cifrado.	Cumple

ACTA DE FALLO

Procedimiento de contratación: **Licitación**
Carácter del procedimiento: **Internacional Abierta**
Clave interna: **LPIA-006HHE001-016-17**
Clave electrónica: **LA-006HHE001-E74-2017**

Descripción: **Adquisición de una solución de seguridad de aplicaciones.**

Especificaciones	Cumplimiento
· Debe ser compatible con el protocolo SSL (v2 y v3) y TLS (v1.0, v1.1, v1.2).	Cumple
· Debe soportar por lo menos las siguientes suites de cifrado: ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES256-SHA384, AES256-GCM-SHA384, AES256-SHA, ECDHE-RSA-AES128-GCM-SHA256, AES128-SHA, RC4- SHA.	Cumple
· Debe ser capaz de reutilizar las sesiones SSL	Cumple
· Para cada uno de los servidores que participan en el algoritmo de balanceo, debería ser posible configurar: peso (de preferencia para fines de control de envío de tráfico), el número máximo de conexiones soportadas por ese servidor, el número máximo de conexiones nuevas por segundo que este servidor soporta, diferentes métodos de control de salud (Health Check), el perfil de cifrado entre el sistema y el servidor (SSL / TLS y cifrado) y el establecimiento para el retraso de envío de las conexiones a este servidor en caso que este se haya reiniciado, el porcentaje máximo de nuevas conexiones durante el intervalo siguiente a que este se reinicie, la cookie de servidor (para fines de identificación de conexiones) y poder indicar si este servidor es un backup de otro (s).	Cumple
· El equipo proporcionado debe ser capaz de balancear las nuevas sesiones, pero preservando las sesiones existentes en el mismo servidor, usando persistencia de sesión de los siguientes tipos: dirección de origen, de hash, hash basado en dirección y el puerto TCP / UDP, hash basado en la cookie proporcionada por el servidor real, ID de sesión SSL, el hash de una palabra específica encontrado en el encabezado HTTP de la solicitud del cliente, hash del parámetro de URL que se encuentra en la solicitud HTTP que viene del cliente, atributo RADIUS.	Cumple
· Debe ser compatible con, al menos, las siguientes reglas de persistencia basado en: dirección de origen, de hash, hash basado en dirección y el puerto TCP / UDP, hash basado en la cookie proporcionada por el servidor real, ID de sesión SSL, el hash de una palabra específica encontrado en el encabezado HTTP de la solicitud del cliente, hash del parámetro de URL que se encuentra en la solicitud HTTP que viene del cliente, atributo RADIUS.	Cumple
· Debe ser capaz de re escribir la cookie desde el servidor real para su utilización en las reglas de persistencia.	Cumple
· Debe poder configurar timeouts de conexión sobre las persistencias	Cumple
· El sistema debe permitir la selección del servidor real basado en la información de cabecera de paquetes TCP / IP y HTTP.	Cumple
· Debe permitir la selección del servidor real basado en el valor del campo de encabezado HTTP que incluye al menos el contenido de host HTTP, HTTP referer, URL HTTP Request y SNI (Server Name Indicator);	Cumple
· La selección de los campos de cabecera HTTP para fines de enrutamiento debe hacerse a través expresiones regulares o match completo.	Cumple
· El sistema debe permitir la reescritura de mensajes de HTTP request, HTTP repsonse y cabecera HTTP.	Cumple
· El sistema debe permitir reescribir el parámetro Location de la respuesta HTTP condicionado al uso de strings o expresiones regulares para identificar patrones en los campos: HTTP host, HTTP location, HTTP referer, HTTP request URL y dirección IP origen.	Cumple
· El sistema debe permitir la reescritura, redireccion, o prohibicion de las peticiones HTTP. Debe permitir la reescritura de los parámetros de host, dirección URL y Referer de la cabecera HTTP. Estas operaciones se acondicionan a utilizar strings o expresiones regulares para identificar patrones en los campos: HTTP host, HTTP location, HTTP referer, HTTP request URL y dirección IP origen.	Cumple
· El sistema debe permitir la compresión de datos incluyendo: aplicaciones (Java Script, XML, SOAP, X-Javascript, XML) y texto (CSS, HTML, JavaScript, Plano, XML).	Cumple

ACTA DE FALLO

Procedimiento de contratación: **Licitación**
Carácter del procedimiento: **Internacional Abierta**
Clave interna: **LPIA-006HHE001-016-17**
Clave electrónica: **LA-006HHE001-E74-2017**

Descripción: **Adquisición de una solución de seguridad de aplicaciones.**

Especificaciones	Cumplimiento
· Soportar almacenamiento en caché del contenido HTTP, permitiendo que los objetos que se almacenan en la memoria y las peticiones HTTP sean contestadas directamente por la solución y que este caché con el fin de controlar recursos debe ser posible controlar: tamaño máximo de objetos, el tamaño máximo de caché del sistema, el número máximo de entradas de caché, el tiempo máximo de caché, las reglas de excepción.	Cumple
· El sistema debe tener perfiles de tráfico pre configurados para su uso en un grupo de servidores reales. Por lo menos los siguientes perfiles de servicios / servidores deben estar pre configurado: FTP, TCP, UDP, HTTP/s (con TLS / SSL offload), RADIUS, TCP seguro (con TLS / SSL offload).	Cumple
· Además de los perfiles preconfigurados, El sistema debe permitir la personalización de perfiles basándose en el bloqueo o permiso de la dirección IP origen, permisos basado en la ubicación por países (TCP, UDP, HTTP, FTP, HTTP), reputación de la dirección origen (TCP, UDP, HTTP, FTP, HTTP) mantenido por el fabricante de la solución, compresión de datos (HTTP), caché de datos (HTTP).	Cumple
· El sistema debe permitir la personalización de las páginas de error enviadas a los clientes en caso de fallo en los servidores vía HTML.	Cumple
· Debe poderse implementar NAT, NAT64 y NAT46 (los dos últimos para permitir NAT en IPv4 e IPv6 entre clientes y servidores).	Cumple
· Ha de implementar el esquema de autenticación Basic (RFC 2617).	Cumple
· Debe tener preconfigurado algoritmos de balanceo de carga incluyendo al menos: Round Robin (selecciona el próximo de una serie de servidores preconfigurados), la selección del servidor con el menor número de conexiones, servidor con mejor "salud", basado en el hash del URI (cabecera HTTP), basado en el hostname (HTTP request), selección basada en el hash de la dirección IP de destino.	Cumple
· Debe contar con funciones de redundancia y alta disponibilidad en cluster del mismo modelo en modo activo-pasivo y activo-activo.	Cumple
· La formación del clúster debe permitir la sincronización de la versión del SO y de la configuración entre los participantes.	Cumple
· Debe contar con mecanismos de monitoreo del estado de interfaz para permitir el cambio de estado del miembro del clúster de activa a pasiva, en caso de fallo.	Cumple
· Los participantes en el clúster deben ser del mismo modelo y tener la misma versión del sistema operativo.	Cumple
· Por lo menos la siguiente información debe ser sincronizada entre los miembros del clúster: Configuración principal (línea de comandos), certificados X.509, archivos de solicitud de firma de certificado (certificate signing request files (CSR)), claves privadas, archivos relacionados a mensajes de error, indica el nivel de conexiones L4, de persistencia L4 y el L7.	Cumple
· En el clúster activo-pasivo solo uno de los miembros enviará el tráfico, el pasivo solo enviará el tráfico en caso de falla del activo.	Cumple
· En el clúster activo-pasivo se debe mantener la sincronización del sistema operativo y la configuración, y así minimizar el impacto en caso de fallo del activo. En este caso la transición debe ser automática, sin intervención externa al clúster.	Cumple
· En la configuración activo-activo todos los miembros del clúster deben reenviar el tráfico.	Cumple
· En la configuración activo-activo, el clúster debe poder contener dos o más miembros de la misma familia. Permitiendo hasta 8 dispositivos.	Cumple
· Debe permitir la configuración de parámetros que permitan la elección del sistema primario en el clúster (el sistema primario, es aquel donde las configuraciones son hechas y enviadas a los otros miembros) dentro del mismo grupo.	Cumple

ACTA DE FALLO

Procedimiento de contratación: **Licitación**
Carácter del procedimiento: **Internacional Abierta**
Clave interna: **LPIA-006HHE001-016-17**
Clave electrónica: **LA-006HHE001-E74-2017**

Descripción: **Adquisición de una solución de seguridad de aplicaciones.**

Especificaciones	Cumplimiento
· De ser necesario, se pueden aplicar configuraciones en cualquier miembro del clúster, sin importar si este es primario o secundario.	Cumple
· La sincronización de la configuración del clúster, puede ser realizada a través de puertos agregados.	Cumple
· El sistema debe permitir el uso de scripts en lenguaje LUA para manejar las peticiones y respuestas HTTP y seleccionar la ruta basado en el contenido de la información de la cabecera HTTP.	Cumple
· En el caso de appliances, debe soportar la configuración de varias instancias del sistema.	Cumple
· Debe permitir el aprovisionamiento de diferentes administradores para cada uno instancias del sistema.	Cumple
· La solución debe permitir el cifrado / descifrado de sesiones SSL en lugar de dejar esta función a los servidores reales (un proceso conocido como SSL Offload).	Cumple
· Al realizar SSL Offload, la solución debe actuar como servidor proxy para fines de procesamiento SSL, usando certificados y claves de los servidores para: autenticar por si mismo los servidores a clientes, descifrar los request y cifrar las respuestas a los clientes.	Cumple
· Debe ser posible implementar la solución como un proxy SSL, en este caso desempeña el papel de proxy en ambos lados de la conexión (cliente y servidor);	Cumple
· Deben soportar al menos cifrados: RSA, PFS, ECDHE y eNull para SSL Offload.	Cumple
· Debe permitir la configuración del cifrado para SSL Offload.	Cumple
· Debe soportar la creación de cuentas de administrador con diferentes perfiles y derechos de acceso basado en roles (RBAC).	Cumple
· El perfil de los administradores debe definirse sobre la base de los derechos a las diferentes funcionalidades del sistema.	Cumple
· Los derechos de acceso deben ser: Lectura, Escritura (y Lectura) y Sin acceso.	Cumple
· El sistema debe tener al menos las siguientes unidades funcionales para fines del acceso del administrador: Sistema (configuración general del equipo), Routing, Firewall, balanceo de carga de servidores, Seguridad (Web Application Firewall), informes y logs.	Cumple
· El sistema debe tener un panel, a través de la interfaz gráfica que permite al administrador ver la información sobre el sistema, incluyendo al menos: el estado del sistema (versión de firmware, el uso de CPU, uso de memoria, uso de disco, el número de conexiones actuales, el número de Promedio de conexión, de entrada y salida de ancho de banda utilizado, los últimos registros), balanceo de carga.	Cumple
· Debe tener, a través de panel de interfaz gráfica de usuario que muestra los registros de eventos, la seguridad y el tráfico de datos, incluidas las actividades de los administradores y del sistema.	Cumple
· Debe contar con filtros que permiten la visualización de eventos de configuración: indican cambios en la configuración del sistema, el usuario que hizo el cambio, la acción (edición, adición o supresión), configuración que haya sido cambiada.	Cumple
· Debe contar con filtros que permitan la visualización de eventos de administración: las acciones realizadas por los administradores.	Cumple
· Debe contar con filtros que permitan la visualización de eventos del sistema: indicar la información pertinente a la operación, alertas y errores generados por el sistema.	Cumple
· Debe contar con filtros que permitan la visualización de eventos de usuario: indica las actividades de autenticación de usuario, incluyendo información como el nombre de usuario, grupo y la política de autenticación utilizada.	Cumple
· Debe contar con filtros que permitan la visualización de estado de salud del sistema: indicar resultados de la comprobación de salud, estado de certificados, el nombre o identificador del servidor real, comprobar el estado: el satisfactorio o fallido.	Cumple

ACTA DE FALLO

Procedimiento de contratación: **Licitación**
Carácter del procedimiento: **Internacional Abierta**
Clave interna: **LPIA-006HHE001-016-17**
Clave electrónica: **LA-006HHE001-E74-2017**

Descripción: **Adquisición de una solución de seguridad de aplicaciones.**

Especificaciones	Cumplimiento
· Debe contar con filtros que permitan la visualización de los eventos de balanceo de servidores: indicando que se ha alcanzado el número máximo de conexiones; identificador del servidor real, la política relacionada con el evento.	Cumple
· Debe contar con filtros que permitan la visualización de eventos del Firewalls: la política relacionada con el evento.	Cumple
· Debe contar con filtros que permitan la visualización de eventos de seguridad - IP Reputación: indicando el protocolo utilizado, las direcciones IP y los puertos de origen y destino, los países de origen y de destino del tráfico, el nombre de la política y la acción tomada por la política de seguridad.	Cumple
· Debe contar con filtros que permitan la visualización de eventos de seguridad - firewall de aplicaciones Web: indicando el protocolo utilizado, direcciones IP y puertos de origen y destino, los países de origen y de destino del tráfico, el nombre de la regla y la acción tomada por esta y el módulo de firewall de seguridad para aplicaciones web relacionado (suscripción, acceso a la URL no permitida, cross site scripting / SQL Injection), la URL y el contenido de la cabecera del mensaje HTTP.	Cumple
· Debe contar con filtros que permitan la visualización de eventos de seguridad - Geo: muestra el protocolo utilizado, las direcciones IP y los puertos de origen y destino, los países de origen y de destino del tráfico, el nombre de la regla y la acción adoptada por la política de seguridad.	Cumple
· Debe contar con filtros que permitan la visualización de eventos de tráfico de balanceo de carga de capa 4: Protocolo, bytes entrada, bytes salida, las direcciones IP y los puertos de origen y de destino, los países de origen y de destino del tráfico.	Cumple
· Debe contar con filtros que permitan la visualización de eventos de tráfico de balanceo de carga de capa 7: Protocolo, Bytes de entrada, bytes de salida, las direcciones IP y los puertos de origen y de destino, los países de origen y de destino del tráfico, el método HTTP, código de retorno HTTP, URL base, nombre de la cookie, nombre de usuario, nombre del grupo y estado de autenticación (si aplica).	Cumple
· Para cada uno de los eventos (registros de eventos, seguridad y tráfico) debe haber registro mandatorio de: fecha, hora, nivel de registro, id del mensaje.	Cumple
· Debe ser posible almacenar los registros en el propio sistema.	Cumple
· Debe permitir la selección del nivel de log que se guardará localmente (Emergencia, Alerta, crítico, error, advertencia, notificación, información y Debug).	Cumple
· Debe permitir seleccionar el tipo de log a ser almacenados localmente (Eventos, Seguridad y Tráfico) para evitar el uso excesivo de disco.	Cumple
· Debe ser posible enviar notificaciones y logs a un servidor syslog	Cumple
· Debe permitir seleccionar el nivel más bajo de log que se enviará al servidor syslog (Emergencia, Alerta, crítico, error, advertencia, notificación, información y Debug).	Cumple
· Debe permitir el envío de registros al servidor syslog en formato CSV.	Cumple
· Debe permitir seleccionar el tipo de registro para ser enviados al servidor syslog.	Cumple
· La solución debe ser compatible con el envío de alertas a través de mensajes de correo electrónico, estas alertas se pueden configurar de acuerdo con el tipo de evento o niveles de severidad.	Cumple
· Debe ser compatible con el envío de alertas a través de mensajes de correo electrónico relacionados con al menos eventos: alta disponibilidad, administración, configuración, control de salud, el disco de caducidad del certificado.	Cumple
· Debe permitir y generar informes por demanda o programados.	Cumple
· Debe permitir el envío por correo electrónico de los informes programados en formato PDF.	Cumple
3.1. GARANTÍAS	

ACTA DE FALLO

Procedimiento de contratación: **Licitación**
Carácter del procedimiento: **Internacional Abierta**
Clave interna: **LPIA-006HHE001-016-17**
Clave electrónica: **LA-006HHE001-E74-2017**

Descripción: **Adquisición de una solución de seguridad de aplicaciones.**

Especificaciones	Cumplimiento
· Todo el equipo que forme parte de la solución de seguridad de aplicaciones, deberá de tener garantía por un periodo de tres años en todos sus componentes físicos y de software.	Cumple
· El período de garantía iniciará partir de la fecha de firma del contrato. Durante el periodo de garantía deberán proveerse actualizaciones de software y acceso a suscripciones en caso de ser necesario.	
· La garantía deberá ser en sitio sin costo adicional en todas las partes de hardware contra defectos de fabricación, mal funcionamiento y fallas por el periodo de vigencia antes mencionado.	
3.2. TRANSFERENCIA DE CONOCIMIENTOS.	
Deberán proporcionarse al menos tres sesiones de transferencia de conocimiento formales, al finalizar la entrega e instalación para que tres personas, designadas por la DGTI, dominen la configuración, operación, administración y manejo de incidentes de la solución de seguridad de aplicaciones.	Cumple
4. SERVICIOS DE INSTALACIÓN Y SOPORTE TÉCNICO.	
El licitante como parte de su propuesta técnica deberá considerar servicios profesionales para la implementación de todos los componentes de la infraestructura (hardware y software) propuestos desde su configuración, pasando por la puesta a punto y puesta en producción, y para la migración de servicios que se tienen en otro equipo y que tienen las siguientes funciones:	Cumple
· Esquema de balanceo de la aplicación de carga entre 4 (cuatro) servidores productivos.	
· SSL de la Plataforma Nacional de Transparencia del instituto.	
· Balanceo de la aplicación de consultas entre 3 (tres) servidores productivos.	
Posteriormente durante el implementación el proveedor ira depurando las políticas, así como los filtros y firmas con base en un plan de trabajo pactado de común acuerdo con el administrador del contrato y con ventanas de autorización bajo un estricto control de cambios con apego total a las prácticas establecidas en el MAAGTIC-SI, lo cual deberá estar controlado por un PM certificado por el PMI por parte del licitante y el cual deberá firmar todas las minutas de control de cambios durante el contrato.	
4.1. PLAN DE TRABAJO	
El licitante como parte de su propuesta técnica deberá presentar un esbozo del Plan de trabajo, donde especifique como mínimo las actividades y tiempos necesarios para la entrega de los equipos, instalación, configuración, puesta a punto, trasferencia de conocimiento, garantía y soporte. Cada una de estas actividades deberá estar programada de forma independiente.	Cumple
4.2. SOPORTE TÉCNICO	
El licitante como parte de su propuesta técnica deberá considerar cubrir con soporte técnico de especialistas con experiencia en las plataformas a implementar con por lo menos tres recursos certificados en la plataforma solicitada, comprobable mediante certificados. Debe especificar por escrito el procedimiento para la atención a incidentes, la matriz de escalamiento mediante una mesa de ayuda y los siguientes tiempos de respuesta:	Cumple
· Niveles de servicio 7 X 24 (soporte telefónico).	Cumple
· Horario para solicitar servicios (7x24): 24 horas al día, siete días a la semana.	Cumple
· Teléfono de soporte técnico 7X24: El soporte técnico del teléfono será ilimitado a los incidentes de hardware o el equipo de su propuesta, 24 horas al día, 7 días a la semana, todo el año.	Cumple
· El tiempo máximo de atención al reporte y generar el ticket; 15 minutos.	Cumple
4.2.1. MESA DE AYUDA	
El licitante en su propuesta técnica deberá incluir los servicios de una mesa de ayuda, para reporte y canalización de Incidencias por parte del personal autorizado de la DGTI. Siendo alcance del proveedor la atención, seguimiento y remediación de incidentes de falla asociados a los bienes y servicios solicitados en el presente Anexo Técnico.	Cumple

ACTA DE FALLO

Procedimiento de contratación: **Licitación**
Carácter del procedimiento: **Internacional Abierta**
Clave interna: **LPIA-006HHE001-016-17**
Clave electrónica: **LA-006HHE001-E74-2017**

Descripción: **Adquisición de una solución de seguridad de aplicaciones.**

Especificaciones	Cumplimiento
El proveedor deberá contar con alguna herramienta para la gestión de la mesa de ayuda, misma que deberá ofrecer servicio a la DGTI a más tardar diez días naturales después de la entrega e instalación de los equipos, con las siguientes características:	Cumple
A. La herramienta deberá estar certificada por el programa Pink Verify de Pink Elephant en 11 procesos ITIL:	Cumple
1. Gestión de Cambios (CHG)	
2. Gestión de Eventos (EV)	
3. Gestión de Incidentes (IM)	
4. Gestión del Conocimiento (KM)	
5. Gestión de Problemas (PM)	
6. Gestión de la Entrega y Despliegue (REL)	
7. Gestión de Solicitudes (RF)	
8. Gestión de Activos de Servicio y de la Configuración (SACM)	
9. Gestión del Catálogo de Servicios (SCM)	
10. Gestión de Niveles de Servicio (SLM).	
11. Gestión del Portafolio de Servicios (SPM)	
Lo que se deberá demostrar a través de la consulta del portal de Pink Elephant, o mediante carta firma por representante legal de Pink Elephant:	
http://www.pinkelephant.com/PinkVERIFY/PinkVERIFY_2011_Toolsets.htm	
B. La herramienta que el Proveedor utilice para la gestión de incidentes deberá aparecer en el cuadrante de Líderes (Leaders) ó Retadores (Challengers) de Gartner de acuerdo con el: *Gartner MQ for ITSM Tools 2017*	Cumple
C. Para la gestión de incidentes y solicitudes, la herramienta deberá permitir:	Cumple
1. Gestionar el ciclo de vida de todo incidente o solicitud reportada	
2. Asignar un número de caso a las solicitudes o incidentes reportados para su identificación y seguimiento	
3. Administrar el estado de las solicitudes o incidentes durante su ciclo de vida. Por lo que debe contemplar por lo menos los estados: Abierto, Asignado, En espera y Cerrado, dichos estados son enunciativos más no limitativos, por lo que la **DGTI** podrá solicitar durante la vida del contrato añadir más estados, sin que esto requiera el uso de código o programación	
4. Clasificar los incidentes y solicitudes en categorías y subcategorías	
5. Configurar los servicios, categorías y subcategorías en que se clasificarán los incidentes y solicitudes, así como las prioridades y SLA's sin el uso de lenguaje de programación	
6. Generar reportes y estadísticas personalizados desde el portal web	
7. Deberá contar también con tableros de control y estadísticas que permitan identificar el estado en que se encuentren las solicitudes de servicio, El cual puede ser consultado por la **DGTI** a través de un portal web, sin que esto genere el uso de licenciamiento de la herramienta	
D. Podrá generar flujos de trabajo o tareas automatizadas a través de una interfaz gráfica, sin necesidad del uso de lenguaje de programación.	Cumple
E. La herramienta de mesa de ayuda deberá contar con un módulo de seguimiento o gestión de proyectos, donde se registran las actividades correspondientes a la implementación y desarrollo del servicio.	Cumple
F. Permitirá también la administración de los Items de configuración (CI's) mediante una CMDB la cual es parte del sistema. Los CI's que sean reportados con falla a la mesa de ayuda, pueden asociarse al o los tickets que sean generados, con el fin de identificar tendencias o elaborar estadísticas de falla.	Cumple

ACTA DE FALLO

Procedimiento de contratación: **Licitación**
Carácter del procedimiento: **Internacional Abierta**
Clave interna: **LPIA-006HHE001-016-17**
Clave electrónica: **LA-006HHE001-E74-2017**

Descripción: **Adquisición de una solución de seguridad de aplicaciones.**

Especificaciones	Cumplimiento
G. Los reportes de incidentes que se generen deberán ser capaces de mostrar campos de los CI's alojados en la CMDB	Cumple
H. En caso de requerirse modificaciones a los formularios de registro de incidentes o solicitudes, añadir nuevos estados o categorías, así como la creación o modificación de reportes, estas podrán ser realizadas sin el uso de lenguaje de programación o manipulación de código fuente y en un lapso de no mayor a 12 horas	Cumple
I. La herramienta deberá tener la capacidad de realizar en tiempo real y de manera automática o manual, un respaldo de su información para asegurar la continuidad del servicio.	Cumple
4.3. ADMINISTRADOR DE PROYECTO PARA LA IMPLEMENTACIÓN DE LA SOLUCIÓN	
El proveedor deberá designar desde la notificación del fallo y hasta que la solución sea puesta en producción y haya sido aceptada por la DGTI a un Administrador de Proyecto (PM por sus siglas en Ingles). Con objeto de garantizar la correcta ejecución de los trabajos de suministro, instalación, puesta en punto de los equipos ofertados. El PM será el punto de contacto entre la DGTI y el proveedor durante los trabajos de implementación de la solución ofertada en la propuesta técnica.	Cumple
El Administrador de Proyecto tendrá autoridad y estará facultado para tomar decisiones en todo lo relativo al cumplimiento de la implementación de la solución con todos los bienes y servicios solicitados en el presente Anexo Técnico, además conocerá el alcance de los servicios, así como las normas y especificaciones aplicables a éstos.	
Lo anterior proporcionará la certeza de contar con un profesional que identificará las fortalezas, oportunidades, debilidades y amenazas de la fase de implementación del proyecto, ayudando a eliminar los obstáculos que pudieran evitar el éxito del plan a través de la ejecución y gestión eficaz de las siguientes actividades:	
ü Administración del proyecto, desde la planeación, asignación de roles y responsabilidades de los recursos involucrados	
ü Planificación y programación de las actividades del Proyecto	
ü Control y seguimiento de actividades	
ü Facilitar el entendimiento y la comprensión de los objetivos del proyecto	
ü Incrementa la coordinación y cooperación entre el equipo de trabajo asignado al proyecto	
ü Seguimiento y aseguramiento al cumplimiento de objetivos y entregables del proyecto de acuerdo al plan de trabajo y con la calidad acordada en contrato.	
ü Seguimiento a control de cambios y solicitudes por parte la **DGTI**	
ü Ejecución del proceso de entrega (Implementación a la Operación de los bienes y servicios ofertados en la presente propuesta)	
4.4. LÍDER TÉCNICO	
El proveedor deberá designar desde la notificación del fallo y hasta que la solución sea puesta en producción y haya sido aceptada por la DGTI a un a un Líder Técnico (TL por sus siglas en Ingles). El TL será responsable de validar la arquitectura y configuración, así como supervisar la puesta en producción y correcto funcionamiento de la solución.	Cumple
El líder técnico será el encargado del seguimiento oportuno de cualquier asunto técnico, además de las siguientes actividades:	
ü Control y gestión de las actividades técnicas.	
ü Propuestas de arquitectura.	
ü Memorias técnicas.	
ü Resolución de dudas técnicas	
ü Vigilar la calidad técnica de la solución.	

ACTA DE FALLO

Procedimiento de contratación: **Licitación**
Carácter del procedimiento: **Internacional Abierta**
Clave interna: **LPIA-006HHE001-016-17**
Clave electrónica: **LA-006HHE001-E74-2017**

Descripción: **Adquisición de una solución de seguridad de aplicaciones.**

Especificaciones	Cumplimiento
ü Validar la seguridad de la solución.	
5. ENTREGABLES.	
Documento | Fecha de entrega | Tipo	
Inventario de equipos | Diez días naturales después de la entrega de los equipos. | Físico/Electrónico	Cumple
Memoria técnica de la instalación que incluya: Plan de trabajo, Documentación de proceso de instalación, Diagramas de conexión físico, Diagrama lógico de conexión, Configuración de los equipos, Resultados de pruebas de alta disponibilidad, Reporte fotográfico | Diez días naturales después de la entrega de los equipos | Físico / Electrónico	Cumple
Carta garantía del equipo que forme parte de la solución de seguridad de aplicaciones, por un periodo de tres años en todos sus componentes físicos y de software. | Diez días naturales después de la entrega e instalación de los equipos, junto con memoria técnica | Físico / Electrónico	Cumple
Documento del proceso de la mesa de ayuda para levantamiento y escalación de incidentes | Diez días naturales después de la entrega e instalación de los equipos, junto con memoria técnica | Físico / Electrónico	Cumple
Registros con evidencias de la trasferencia de conocimiento | Diez días naturales después de la entrega e instalación de los equipos, junto con memoria técnica | Físico / Electrónico	Cumple
6. TIEMPOS DE ENTREGA	
El equipamiento solicitado deberá estar entregado e instalado a más tardar el **5 de diciembre de 2017**. Los entregables diez días naturales después de la entrega e instalación del equipamiento. El contrato de esta adquisición tendrá vigencia hasta el 31 de diciembre de 2017.	Cumple
El equipamiento se considera entregado e instalado en la fecha que sean recibidos a satisfacción de la DGTI.	Cumple
9. INFORMACIÓN ADMINISTRATIVA	
· La adquisición de la presente convocatoria se adjudicará en una sola partida. Los licitantes deberán cumplir al 100% con los requisitos indicados.	Cumple
El Licitante deberá incluir en su propuesta técnica, una carta firmada por su representante legal, en la que se mencione que todo el equipamiento informático para el balanceo de aplicaciones, certificados SSL y Firewall de aplicaciones Web que oferta es nuevo y con soporte dentro de la República Mexicana.	Cumple
El Licitante deberá incluir en su propuesta técnica, una carta firmada por su representante legal, en la que se mencione que, en caso de resultar adjudicado en el presente procedimiento, entregará a la DGTI una carta garantía del equipo que forme parte de la solución de seguridad de aplicaciones, por un periodo de tres años en todos sus componentes físicos y de software.	Cumple
El Licitante deberá incluir en su propuesta técnica, una carta firmada por su representante legal, en la que se mencione el número de personal certificado en los equipos de la solución propuesta.	Cumple
El Licitante deberá presentar en su propuesta técnica, una carta del fabricante que lo acredite como distribuidor autorizado. La carta del fabricante deberá estar dirigida a la convocante mencionando la presente convocatoria.	Cumple
El Licitante deberá presentar en su propuesta técnica, una carta del fabricante donde confirme la disponibilidad de refacciones por al menos los próximos 3 (tres) años, para los equipos ofertados.	Cumple

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO
A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES
DIRECCIÓN GENERAL DE ADMINISTRACIÓN
DIRECCIÓN DE RECURSOS MATERIALES Y SERVICIOS GENERALES
SUBDIRECCIÓN DE ADQUISICIONES Y CONTROL PATRIMONIAL

ACTA DE FALLO

Procedimiento de contratación: **Licitación**
Carácter del procedimiento: **Internacional Abierta**
Clave interna: **LPIA-006HHE001-016-17**
Clave electrónica: **LA-006HHE001-E74-2017**

Descripción: **Adquisición de una solución de seguridad de aplicaciones.**

Debe señalarse que de acuerdo con lo establecido en la convocatoria, el puntaje mínimo requerido para ser consideradas las propuestas solventes técnicamente es de **37.5 puntos** de los **50** a otorgarse----------
---

Derivado del dictamen antes referido se obtuvo el puntaje siguiente: ----------
---

La propuesta del licitante **GRUPO DE TECNOLOGIA CIBERNETICA, S.A. DE C.V.**, obtuvo **44.5 puntos** por lo que **fue considerada solvente** y pasó a ser evaluada económicamente.----------
---

Evaluación económica:

No	Licitante	Montos propuestos		Puntos a otorgar	Puntos otorgados
		con IVA	sin IVA		
1	GRUPO DE TECNOLOGIA CIBERNETICA, S.A. DE C.V.	2´640,480.00	2´276,275.86	50	50

Por lo anterior, los totales generales resultan de la siguiente forma:

N°	Licitante	Puntaje Evaluación Técnica	Puntaje Evaluación Económica	Resultado final de la puntuación
1	GRUPO DE TECNOLOGIA CIBERNETICA, S.A. DE C.V.	44.5	50	94.5

---

4. Derivado de lo anterior, con fundamento en los Artículos 35 fracción I y 36 del Reglamento y apartado 5.2 de la Convocatoria, se adjudica la contratación de la **"Adquisición de una solución de seguridad de aplicaciones"**, al licitante **GRUPO DE TECNOLOGIA CIBERNETICA, S.A. DE C.V.**, en virtud de que cumple con todos los requisitos solicitados por la Convocante para este procedimiento de contratación y obtuvo una ponderación técnico-económica de **94.5** puntos, a través de un contrato cerrado, por un monto total de **$2´640,480.00 (Dos Millones Seiscientos Cuarenta Mil Cuatrocientos Ochenta Pesos 00/100 M.N.),** con I.V.A. incluido y por una vigencia a comprendida partir del **27 de noviembre al 31 de diciembre de 2017**---------
---

5. La disponibilidad presupuestal está validada por la Dirección de Recursos Financieros, mediante Reserva No. 230/128, según de fecha 6 de octubre de 2017. ----------
---

6. El Lic. Ibo Brito Brito, hace saber al licitante adjudicado, que en cumplimiento de lo establecido en el numeral 4.1 *"Documentación que deberá presentar el Proveedor"* de la Convocatoria, deberá entregar en la Subdirección de Adquisiciones y Control Patrimonial del INAI a más tardar dos días hábiles posteriores a la notificación de este fallo, la siguiente documentación en original y copia para su cotejo. La omisión en la entrega de los documentos siguientes que se tienen como obligatorios será motivo para no suscribir el contrato correspondiente por causas

ACTA DE FALLO

Procedimiento de contratación: **Licitación**
Carácter del procedimiento: **Internacional Abierta**
Clave interna: **LPIA-006HHE001-016-17**
Clave electrónica: **LA-006HHE001-E74-2017**

Descripción: **Adquisición de una solución de seguridad de aplicaciones.**

imputables al licitante adjudicado: ----------

Persona moral

a) Registro Federal de Contribuyentes.
b) Inscripción ante la SHCP (Formato R1).
c) Cambio de domicilio fiscal o razón social (Formato R2), en su caso.
d) Escritura pública en la que conste que fue constituida conforme a las leyes mexicanas y sus modificaciones, en su caso.
e) Escritura Pública mediante la cual acredite ser representante legal y/o contar con facultades para suscribir el contrato y/o pedido.
f) Comprobante de domicilio legal en territorio nacional no mayor a tres meses.
g) Respuesta positiva emitida por el SAT en el que se señale que se encuentra al corriente respecto del cumplimiento de las obligaciones fiscales del artículo 32- D del Código Fiscal de la Federación.
h) Manifestación de no encontrarse en el supuesto de conflicto de intereses, según artículo 49 fracción IX de la Ley General de Responsabilidades Administrativas.

Se hace del conocimiento del licitante adjudicado que el contrato correspondiente se suscribirá el **15 de diciembre de 2017**, a las **18:00 horas**, en la Subdirección de Adquisiciones y Control Patrimonial, ubicada en el domicilio de la Convocante, Planta Baja (tel. 5004-2400 ext. 2553); si por causas imputables al licitante no se suscribe dentro del término antes señalado, (por no entregar la documentación en los términos antes referidos, entre otras causas), será sancionado por el Órgano Interno de Control del INAI, en términos del Artículo 62 del Reglamento.----------

Asimismo, el licitante ganador deberá entregar una garantía de cumplimiento por el importe equivalente del 10% del monto total del contrato, sin incluir I.V.A., dentro de los diez días naturales siguientes a la firma del mismo en la Dirección de Recursos Materiales, ubicada en el domicilio de la Convocante; de no entregar la garantía en el plazo establecido se procederá a la rescisión del contrato, con fundamento en el artículo 54 del Reglamento.-----

7. Conforme a lo establecido en el artículo 37 del Reglamento y en el numeral 3.3.6 de la Convocatoria, se fijará una copia de la presente acta en los estrados de la Planta Baja del domicilio de la convocante, por un término no menor de cinco días hábiles a partir de este día, mismo que estará a disposición de cualquier interesado. ---------

No habiendo más asuntos que tratar se da por concluido el presente acto siendo las **19:00** horas del día de su fecha, levantándose la presente acta como constancia y firmando un original de conformidad al margen o al calce quienes en ella intervinieron. ----------

POR LA DIRECCIÓN GENERAL DE TECNOLOGIAS DE LA INFORMACIÓN
ÁREA TÉCNICA Y REQUIRENTE

Mtro. Guillermo Preciado López
Director de Soluciones Tecnológicas

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO
A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES
DIRECCIÓN GENERAL DE ADMINISTRACIÓN
DIRECCIÓN DE RECURSOS MATERIALES Y SERVICIOS GENERALES
SUBDIRECCIÓN DE ADQUISICIONES Y CONTROL PATRIMONIAL

ACTA DE FALLO

Procedimiento de contratación: **Licitación**
Carácter del procedimiento: **Internacional Abierta**
Clave interna: **LPIA-006HHE001-016-17**
Clave electrónica: **LA-006HHE001-E74-2017**

Descripción: **Adquisición de una solución de seguridad de aplicaciones.**

POR EL ÓRGANO INTERNO DE CONTROL

Lic. Marco Antonio Contreras Uribe
Auditor

POR LA CONVOCANTE

Lic. Ibo Brito Brito
Subdirector de Adquisiciones y Control Patrimonial

Última hoja del acta de fallo de la Licitación Pública de carácter Internacional Abierta, con clave interna LPIA-006HHE001-016-17 y clave electrónica LA-006HHE001-E74-2017.