I.- Tipo de programa o proyecto

Consideradas las características y requerimientos para la adquisición de una solución de seguridad de aplicaciones, esta unidad administrativa ubica los recursos correspondientes en el programa ***G.O.: Gasto Ordinario***, partida presupuestal 51501 BIENES INFORMÁTICOS, que, según consta en el *Clasificador por Objeto del Gasto para la Administración Pública Federal*, cuya última modificación fue publicada en el Diario Oficial de la Federación (DOF) el 27 de junio de 2017, se define como:

> "***51501 BIENES INFORMÁTICOS.*** *Asignaciones destinadas a la adquisición de equipos y aparatos de uso informático, para el procesamiento electrónico de datos y para el uso de redes, tales como: servidores, computadoras, lectoras, terminales, monitores, procesadores, tableros de control, equipos de conectividad, entre otros.*"

El equipo que será adquirido se instalará en el edificio sede del INAI, sita en Insurgentes Sur Nº 3211, Col Insurgentes Cuicuilco, Delegación Coyoacán, CP. 04530, Ciudad de México.

II.- Monto total de inversión, calendario de inversiones por año y fuente de los recursos

El monto total de inversión para la adquisición de una solución de seguridad de aplicaciones se estima $2,696,500(dos millones seiscientos noventa y seis mil quinientos pesos 00/100 M.N.) IVA incluido, la presente adquisición se realizará con recursos fiscales correspondientes al ejercicio 2017.

III.- Situación actual

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) es un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento de los derechos de acceso a la información pública y de protección de datos personales, en los términos establecidos en la Constitución Política de los Estados Unidos Mexicanos y las leyes respectivas, con domicilio legal en la Ciudad de México.

El 5 de mayo de 2015 entró en vigor la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) al día siguiente de su publicación en el Diario Oficial de la Federación (DOF). Con ella, el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) cambia su nombre por el de ***Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*** (**INAI**), que se robustece con mejores y nuevas atribuciones que lo consolidan como organismo garante a nivel nacional.

La LGTAIP tiene por objeto establecer los principios, bases generales y procedimientos para garantizar el derecho de acceso a la información en posesión de cualquier autoridad, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad de la Federación, las Entidades Federativas y los municipios.

Uno de los aspectos relevantes de la LGTAIP es la creación del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, que es coordinado por el INAI y al cual concurren también los organismos garantes de las entidades federativas, el Instituto Nacional de Estadística y Geografía, la Auditoría Superior de la Federación y el Archivo General de la Nación. Del mismo modo, prevé el diseño y operación de una **Plataforma Nacional de Transparencia**, instrumento informático que permite cumplir con los procedimientos, obligaciones y disposiciones legales para los sujetos obligados y organismos garantes, pero sobre todo facilitando la accesibilidad para los usuarios.

El 10 de mayo de 2016 se publicó en el DOF el Decreto por el que se abroga la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y se expide la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP).

El INAI busca aplicar los mejores esquemas de operación, prácticas y mecanismos de seguridad de la información enfocados a incrementar el grado de confianza que sus usuarios tienen en él y paralelamente ofrecer al Pleno, la certeza de que la Institución se encuentra operando de manera segura y confiable, no solamente en cuanto a los procesos de Tecnologías de la Información y Comunicaciones (TIC), sino en todos sus ámbitos, interno y externo, con el fin de permitir abrirse a las necesidades de servicio con la tecnología actual y adaptarse a los cambios necesarios que el INAI está promoviendo para actualizarse y mantenerse a la vanguardia y cumplir con las atribuciones que le confirieron la Constitución, la LGTAIP y la LFTAIP.

En el INAI las TIC han sido fundamentales para el desarrollo institucional, pues le han permitido obtener notables logros y alcanzar reconocimiento internacional y prestigio institucional entre la sociedad mexicana. Los instrumentos tecnológicos concebidos por el INAI para el acceso a la información y la protección de datos personales, con los que la sociedad ejerce estos derechos y permite a los sujetos obligados atender de forma expedita los requerimientos de información de las personas, han logrado mayores niveles de eficiencia y calidad a fin de generar mayor valor público en beneficio de la sociedad mexicana.

Ahora bien, de acuerdo a la *ficha de alineación a fines institucionales, objetivos, metas, acciones y proyectos*, que se deriva de la planeación estratégica institucional, las actividades de la Dirección General de Tecnologías de la Información, están alineadas al objetivo estratégico institucional para *Coordinar el Sistema Nacional de Transparencia y de Protección de Datos Personales, para que los órganos garantes establezcan, apliquen y evalúen acciones de acceso a la información pública, protección y debido tratamiento de datos personales*. A su vez, entre las actividades para el logro de este objetivo estratégico están la: *Provisión de servicios integrales en materia de TIC*, que se han implementado para: *Medir la operación del CPD donde se encuentran albergados los servidores de aplicativos, bases de datos, enlaces de telecomunicaciones, etc. que permiten que operen los Sistemas sustantivos institucionales, así como los servicios básicos de telefonía,*

internet, entre otros. El indicador de gestión de esta actividad es el *Porcentaje de disponibilidad de los servicios del Centro de Procesamiento de Datos*, entendiendo la disponibilidad como el servicio que garantiza que los usuarios autorizados tengan acceso a la información y a otros activos de información asociados en el lugar, momento y forma en que es requerido. Los sistemas seguros, deben mantener la información disponible para sus usuarios. Es decir que, tanto hardware como software, debe mantenerse funcionando eficientemente y ser capaz de recuperarse rápidamente en caso de fallo.

En ese orden de ideas, el artículo 48 del Estatuto Orgánico del INAI, fracción V, mandata que la Dirección General de Tecnologías de la Información tendrá la función de: *Establecer los mecanismos de seguridad de la información, a efecto de garantizar la disponibilidad, integridad y confidencialidad de la Plataforma Nacional de Transparencia.*

De los párrafos precedentes se desprende que, por su naturaleza, el INAI opera en forma cotidiana diversos temas de seguridad y protección de la información, involucrados en su objetivo primordial que es el de garantizar a la sociedad el ejercicio de sus derechos de acceso a la información pública por los mecanismos establecidos en la LGTAIP y la LFTAIP, así como la protección de sus datos personales, dentro del marco de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).

Actualmente, los grandes cambios e innovaciones que ha traído la era de las tecnologías de la información y comunicaciones (TIC), han propiciado la necesidad de incrementar los niveles de seguridad sobre cada uno de ellos, y principalmente en los elementos de tecnología y de sistemas, sin olvidar aquellos componentes como la alta disponibilidad y los tiempos de acceso hacia múltiples redes de datos y aplicaciones.

Por lo anterior, es necesario salvaguardar, administrar y proteger el activo más valioso del Instituto después del recurso humano: su información; para lograr esto, es necesario disponer de infraestructura de seguridad adecuada.

En este orden de ideas la Dirección General de Tecnologías de la Información del INAI, justifica la adquisición de una solución de balanceo de cargas y seguridad para las aplicaciones en alta disponibilidad, que permita mantener disponibles y seguras sus aplicaciones. Esta solución está conformada por diversos componentes de software, hardware, así como servicios profesionales para su implementación y soporte técnico durante un período de tres años.

Los requerimientos de la solución están integrados por dispositivos que técnicamente ejecutan funciones de balanceo de cargas de trabajo. Un equipo balanceador de carga, es un dispositivo conformado por hardware y software que se coloca al frente de un conjunto de servidores que atienden una o varias aplicaciones, y que asigna las solicitudes que llegan de los usuarios a los servidores, mediante diversos algoritmos de optimización de los flujos de datos. La función de estos dispositivos es distribuir la carga de trabajo en varias computadoras separadas o agrupadas en un clúster que, en el caso del INAI, se trata de la Plataforma Nacional de Transparencia.

Con la adquisición de esta solución de balanceo de cargas y seguridad para las aplicaciones, se podrán minimizan los tiempos de respuesta de la PNT, en particular para los módulos de carga y consulta del SIPOT, con lo que se pretende mejorar el desempeño del servicio que ofrece la PNT y evitar la saturación en el acceso de sus diversos usuarios.

Adicionalmente, la solución de balanceadores de carga permitirá implementar los certificados de seguridad tipo SSL para la Plataforma Nacional de Transparencia y otras aplicaciones institucionales.

Derivado de estas ventajas y los requerimientos de seguridad de las aplicaciones sustantivas, es que se propone la adquisición de una solución para balanceo de cargas y seguridad en las aplicaciones del INAI. Esta solución de balanceo y seguridad de aplicaciones está dimensionada en un esquema de alta disponibilidad, pues con esta arquitectura se va a permitir asegurar y mantener la conectividad de los usuarios a las aplicaciones del INAI. Así mismo, se va a mejorar el nivel de seguridad, a través del uso de certificados SSL y el uso de políticas a sus aplicaciones web.

La solución consiste en dos balanceadores que funcionaran en alta disponibilidad, es decir que se eliminan los puntos únicos de fallo, pues se configuran los dos equipos de tal forma que comparten las funciones de balanceo, para asegurar un cierto grado absoluto de continuidad operacional de las aplicaciones del INAI.

La adquisición de una solución de balanceo de cargas y seguridad para las aplicaciones, se justifica plenamente como una mejora tecnológica tendiente a potencializar los procesos sustantivos, alineada a las estrategias instituciones, diseñada para reforzar los mecanismos de seguridad de la información, necesarios para incrementar los niveles de disponibilidad, y confidencialidad de la Plataforma Nacional de Transparencia y otras aplicaciones que son activos de información de misión crítica para el INAI.

Por lo anteriormente expuesto, el INAI requiere la adquisición de una solución de seguridad de aplicaciones, misma que se ha dimensionado de acuerdo a requerimientos mínimos, basados en las necesidades de operación del INAI, para el desempeño eficiente de las labores institucionales y responder eficazmente a los requerimientos de disponibilidad de los servicios que ofrece el Instituto, en el cumplimiento a sus mandatos de Ley.

IV.- Alternativas de solución

Para atender necesidad de una solución para balanceo de cargas y seguridad en las aplicaciones del INAI, se propone adquirir los equipos mediante un procedimiento de licitación pública. Una alternativa para solucionar los requerimientos, es el arrendamiento sin opción a compra de equipo de para balanceo de cargas y seguridad en las aplicaciones.

En las circunstancias actuales la adquisición de una solución de seguridad de aplicaciones para el INAI, es la opción más viable para resolver la problemática planteada. Las principales razones son las siguientes:

En términos de lo previsto en el artículo 23, sexto párrafo, del *Reglamento de Adquisiciones, Arrendamientos y Servicios del Instituto Federal de Acceso a la Información y Protección de Datos*; así como el Capítulo VI, numeral 2, de las *Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*, se elaboró una investigación de mercado para identificar la existencia de bienes y servicios en las condiciones solicitadas por el INAI, así como las existencia de proveedores a nivel nacional o internacional, y el

precio estimado a efecto de obtener cotizaciones actualizadas, y documentar el esquema de aprovisionamiento más conveniente para el Instituto.

A continuación, se presenta un resumen de dicha cotización en la tabla 1:

Tabla 1: Arrendamiento puro sin opción a compra de una solución para balanceo de cargas y seguridad en las aplicaciones (36 meses)

Nombre del proveedor	Monto arrendamiento
MCSec, S.C.	$4,055,072.46
EDE Consulting Services, S.A. de C.V.	$4,533,333.33
Sirius Electrónicos, S.A. de C.V.	$3,929,967.06
Consultores Asociados en Informática y Telecomunicaciones, S.A. de C.V.	$4,054,769.23
Grupo de Tecnología Cibernética, S.A. de C.V.	$3,793,000.00
Monto promedio de arrendamiento	**$4,073,228.35**

Tabla 2: Adquisición de una solución de seguridad de aplicaciones para el INAI

Nombre del proveedor	Monto adquisición
MCSec, S.C.	$2,798,000.02
EDE Consulting Services, S.A. de C.V.	$2,720,000.02
Sirius Electrónicos, S.A. de C.V.	$2,672,377.61
Consultores Asociados en Informática y Telecomunicaciones, S.A. de C.V.	$2,635,600.04
Grupo de Tecnología Cibernética, S.A. de C.V.	$2,655,100.01
Monto promedio de adquisición	**$2,696,215.54**

De los datos de las tablas 1 y 2, se desprende que el costo promedio del arrendamiento puro sin opción a compra de equipo de cómputo y periférico durante 36 meses es de $4,073,228.35, en tanto que la opción de adquirir el equipo de cómputo y periférico con las mismas características, tiene un costo promedio de $2,696,215.54 incluyendo impuestos.

Se adjuntan los términos de referencia y las peticiones de oferta de la investigación de mercado cuyos resultados se presentan en ambas tablas.

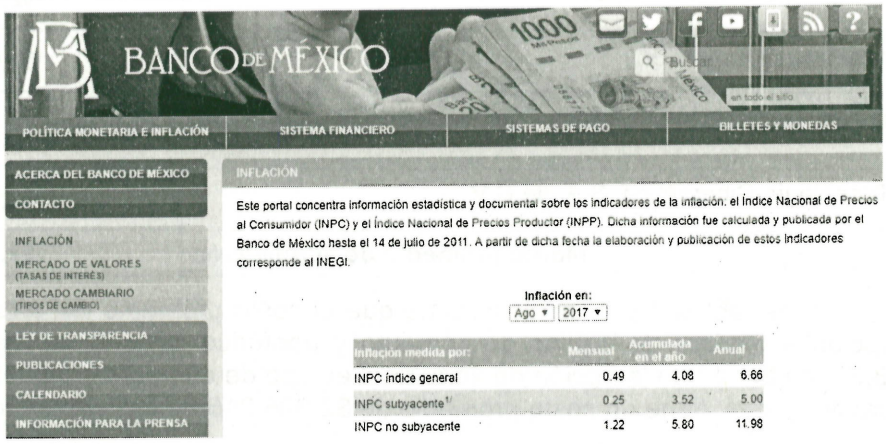
La opción de arrendamiento puro sin opción a compra de una solución para balanceo de cargas y seguridad en las aplicaciones, objeto de esta justificación, excede en costo directo a la opción de compra, principalmente por el importe causado por los intereses añadidos por los proveedores al costo de venta, para amortizar el costo de financiamiento de la inversión de los equipos arrendados y la utilidad adicional que se genera para los intermediarios del mercado sobre el importe de los intereses.

En el caso del arrendamiento, el plazo de 36 meses es el que ofrece mejores condiciones tanto para el Instituto, como para los posibles proveedores, en virtud de que una de las ventajas del arrendamiento de Tecnologías de la Información y Comunicación (TIC), consiste en convertir la inversión en un gasto; es decir, que el proveedor financie el desarrollo, construcción y operación de la infraestructura TIC. Difícilmente un proveedor va ofrecer equipo nuevo en arrendamiento en un periodo menor de 36 meses, pues el costo de las rentas mensuales sería elevado, toda vez que la inversión inicial tendría que recuperarse en corto tiempo. Otra ventaja del arrendamiento a mediano plazo, es la modernidad de la tecnología utilizada, pues se evita la obsolescencia del equipo ya que, cuando se cumple el plazo del servicio aproximadamente cada 36 a 48 meses, con la renovación del contrato se renuevan todos los aparatos por equipo reciente y de tecnología de punta.

Si se comparan los costos en arrendamiento por tres años ($4,073,228.35) con los de adquisición ($2,696,215.54) se obtiene que la diferencia es de $1,377,012.81. De acuerdo con las "Perspectivas Económicas de Mediano Plazo" de la Secretaría de Hacienda y Crédito Público (SHCP), en el próximo ejercicio presupuestal del 2018 la inflación se ubica en un nivel que, en el año 2014, el Banco de México estimó en 3 por ciento anual con un intervalo de variabilidad de más/menos un punto porcentual. *("Criterios Generales de Política Económica 2014", página 161, 3er párrafo, el documento completo se puede consultar en:*

http://www.shcp.gob.mx/POLITICAFINANCIERA/FINANZASPUBLICAS/finanzas_publicas_criterios/cgpe_2014_vf_c_accesibilidad.pdf

En agosto del 2017, la inflación anual acumulada en el año es de 4.08, y la estimación anual, es de 6.66%; los datos de pueden consultar en el vínculo electrónico: http://www.banxico.org.mx/portal-inflacion/index.html



Ahora bien, con base en la *Encuesta sobre las Expectativas de los Especialistas en Economía del Sector Privado: Septiembre de 2017*, publicada por el Banco de México el 2 de octubre de 2017, disponible en su portal en la liga:

http://www.banxico.org.mx/informacion-para-la-prensa/comunicados/resultados-de-encuestas/expectativas-de-los-especialistas/%7BF432882D-DC86-6A73-7FD1-3C1C97AA731F%7D.pdf

se obtienen estadísticas básicas de los pronósticos recabados en las encuestas de septiembre de 2016 a septiembre de 2017, como la inflación general promedio para los próximos cuatro años. Con base en esas fuentes oficiales de datos, se estima que la inflación anual será, en promedio, del 3.5% anual. Por tanto, el impacto inflacionario para el periodo de arrendamiento, del 2018 al 2020, tal como se presenta en la tabla 3.

Tabla 3 Impacto inflacionario

Período	Inflación Anual	Inflación Acumulada
2018e	3.50	3.50%
2019e	3.50	7.00%
2020e	3.50	10.50%

Fuente: Criterios Generales de Política Económica 2014 SHCP PEF.pdf, pág. 162, Encuesta sobre las Expectativas de los Especialistas en Economía del Sector Privado: Septiembre de 2017, pág. 22

Con la alternativa de adquisición de los equipos los costos de reposición en tres años, periodo de tiempo que permite comparar en condiciones equivalentes con la opción de arrendamiento, se estima que el monto de la diferencia más la inflación acumulada del 10.5% del costo actual, en términos monetarios el impacto inflacionario sería de $566,205.26, es decir, que actualizar el equipo mediante una nueva adquisición en el año 2020, equivale en costo al 41% de la diferencia del costo adicional ($1,377,012.81) del arrendamiento por tres años.

La estimación del impacto inflacionario en el periodo 2018-2020, se presenta en la tabla 4, los datos del costo anual se obtuvieron a través de la investigación de mercado, como se define en el artículo 2 fracción XVI del *Reglamento de Adquisiciones, Arrendamientos y Servicios del Instituto Federal de Acceso a la Información y Protección de Datos (RAAS-IFAI), publicado en el Diario Oficial de la Federación* el 31 de marzo de 2015, así como el Capítulo VI, Numeral 2 de las *Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*, con el objeto de identificar la existencia de servicios en las condiciones solicitadas por el INAI, los proveedores a nivel nacional o internacional y los precios estimados.

Tabla 4 Estimación del impacto inflacionario en el periodo 2018-2020

Período	Costo del equipo en 2017	Impacto Inflacionario	Inflación Acumulada
2018 (Ene-Dic)	$2,696,215.54	$94,367.54	3.50%
2019 (Ene-Dic)		$188,735.09	7.00%
2020 (Ene-Oct)		$283,102.63	10.50%
Total acumulado		**$566,205.26**	

Fuente: Investigación de mercado realizada por la DGTI en términos del Artículo 23, párrafo sexto del Reglamento de Adquisiciones, Arrendamientos y Servicios del Instituto Federal de Acceso a Información y Protección de Datos.

Desde el punto de vista económico, se concluye que, en el esquema de adquisición de una solución de seguridad de aplicaciones, se aseguran al Estado las mejores condiciones disponibles en cuanto a precio, calidad, financiamiento y oportunidad, por lo que se considera la alternativa más viable. Desde la perspectiva técnica ambas opciones son viables.

Esta adquisición de una solución de seguridad de aplicaciones permite proporcionar una respuesta adecuada en términos de costos de oportunidad y tiempo de respuesta en materia de servicios de infraestructura tecnológica para cubrir los requerimientos para mejorar el desempeño del servicio que ofrece la PNT, minimizan los tiempos de respuesta en los módulos de carga y consulta del SIPOT evitar la saturación en el acceso de sus diversos usuarios, así como incrementar los niveles de disponibilidad, y confidencialidad de la Plataforma Nacional de Transparencia entre otras aplicaciones sustantivas.

Con base en lo anterior, se concluye que, en el esquema de adquisición de una solución de seguridad de aplicaciones para el INAI, se aseguran al Estado las mejores condiciones disponibles en cuanto a precio, calidad, financiamiento y oportunidad, por lo que se considera la alternativa más viable técnica y económicamente.

V.- Componentes

DESCRIPCIÓN DE LOS EQUIPOS 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*).

Los equipos y componentes de la solución propuesta deberán cumplir como mínimo con los siguientes requerimientos:

- Debe soportar su implementación en modo transparente, actuando como un Bridge L2.
- 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).
- Debe contar con la funcionalidad de Firewall stateful incluyendo IPv4 e IPv6.
- 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).
- 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).
- 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.

- 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.
- 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.
- 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.
- 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.
- 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.
- Debe ser posible de aplicar excepciones a la inspección del tráfico, mediante las políticas de firewall de aplicaciones web.
- Debe ser posible aplicar políticas basadas en firmas que identifiquen ataques basados en las cabeceras HTTP, HTTP Request Body, y HTTP Response body.
- Las firmas deben ser actualizadas por el fabricante de forma automática sin la necesidad de intervención por parte del administrador de la solución.
- Las firmas deben tener niveles de severidad basado en Open Web Application Security Project (OWASP) Risk Rating Methodology.
- Las firmas deben ser organizadas en categorías y subcategorías.
- Debe ser posible implementar políticas de protección URL para permitir la detección de patrones o strings en los URL o extensiones de archivo.
- 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).
- Las URLs y extensiones de archivos configuradas para bloquear, deben poder identificarse mediante el uso de expresiones regulares o strings.
- Debe permitir, a través de políticas de HTTP, el control de: parámetros y métodos de HTTP request y códigos de respuesta HTTP.
- 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.
- 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.

- 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.
- Debe contar con políticas para identificar y bloquear ataques de Cross Site Scripting (XSS) e inyección de SQL.
- 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.
- 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.
- 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.
- 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.
- Debe tener mecanismo para prevenir ataques SYN Flood.
- Debe permitir el cambiar los puertos HTTP, HTTPS, Telnet y SSH para fines de acceso remoto del equipo por el administrador.
- Debe ser compatible con la sincronización de hora a través de NTP.
- 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).
- Debe permitir la actualización a través de la línea de comandos o de la interfaz gráfica.
- Debe permitir que el proceso de upgrade en diferentes particiones.
- 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.
- Debe permitir la actualización programada de la base de datos de suscripción, donde se indique los días de la semana y hora del día.
- Debe ser compatible con la configuración de un servidor de correo para el envío de alertas por correo electrónico.
- Debe contar con servicio de agente SNMP v1, V2c y 3 (RFC 3414).
- Debe permitir la configuración de eventos SNMP al menos en lo relacionado con niveles de uso de CPU, memoria y disco.
- 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).

- Throughput de al menos 20.0 Gbps
- Throughput L7 RPS (Request per second) de al menos 1.5 M
- Compresión de al menos 12 Gbps
- Debe incluir instancias virtuales
- Debe contar con al menos 8 interfaces gigabit ethernet RJ-45
- Debe contar con al menos 4 interfaces 10 gigabit ethernet SFP
- 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
- Debe ser compatible con PPPoE.
- Debe ser compatible con CDP (Cisco Discovery Protocol).
- Debe soportar el protocolo IEEE 802.3ad para el balanceo de tráfico entre los puertos.
- Debe soportar VLAN y ser compatible con el protocolo IEEE 802.1Q.
- Debe permitir el enrutamiento entre VLAN diferentes.
- Debe soportar la configuración de rutas estáticas incluyendo la distancia administrativa de la misma para decidir el enrutamiento de paquetes.
- Debe ser posible configurar políticas de enrutamiento basado en direcciones IP de origen y / o destino.
- Debe ser compatible con OSPF v2 - RFC 2328.
- 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).
- Debe asignar políticas de ancho de banda, teniendo en cuenta la dirección de origen, destino y el servicio (puertos TCP y UDP).
- 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.
- 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.
- Debe soportar balanceo de Capa 7 para los siguientes protocolos HTTP, HTTPs, RADIUS, RDP, SIP, TCPs, DNS, SMTP, RTMP, RTSP, MySQL.
- Debe balancear el tráfico entre los servidores reales utilizando algoritmos propios y utilizando información de salud de los servidores.
- Cuando existe comunicación cifrada, esta debe ser controlada por los protocolos SSL / TLS y la lista protocolos de cifrado.
- Debe ser compatible con el protocolo SSL (v2 y v3) y TLS (v1.0, v1.1, v1.2).

- 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.
- Debe ser capaz de reutilizar las sesiones SSL
- 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).
- 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.
- 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.
- Debe ser capaz de re escribir la cookie desde el servidor real para su utilización en las reglas de persistencia.
- Debe poder configurar timeouts de conexión sobre las persistencias
- El sistema debe permitir la selección del servidor real basado en la información de cabecera de paquetes TCP / IP y HTTP.
- 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);
- La selección de los campos de cabecera HTTP para fines de enrutamiento debe hacerse a través expresiones regulares o match completo.
- El sistema debe permitir la reescritura de mensajes de HTTP request, HTTP repsonse y cabecera HTTP.
- 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.

- 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.
- El sistema debe permitir la compresión de datos incluyendo: aplicaciones (Java Script, XML, SOAP, X-Javascript, XML) y texto (CSS, HTML, JavaScript, Plano, XML).
- 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.
- 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).
- 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).
- El sistema debe permitir la personalización de las páginas de error enviadas a los clientes en caso de fallo en los servidores vía HTML.
- Debe poderse implementar NAT, NAT64 y NAT46 (los dos últimos para permitir NAT en IPv4 e IPv6 entre clientes y servidores).
- Ha de implementar el esquema de autenticación Basic (RFC 2617).
- 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.
- Debe contar con funciones de redundancia y alta disponibilidad en cluster del mismo modelo en modo activo-pasivo y activo-activo.
- La formación del clúster debe permitir la sincronización de la versión del SO y de la configuración entre los participantes.
- 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.
- Los participantes en el clúster deben ser del mismo modelo y tener la misma versión del sistema operativo.
- 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.

- 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.
- 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.
- En la configuración activo-activo todos los miembros del clúster deben reenviar el tráfico.
- En la configuración activo-activo, el clúster debe poder contener dos o más miembros de la misma familia. Permitiendo hasta 8 dispositivos.
- 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.
- De ser necesario, se pueden aplicar configuraciones en cualquier miembro del clúster, sin importar si este es primario o secundario.
- La sincronización de la configuración del clúster, puede ser realizada a través de puertos agregados.
- 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.
- En el caso de appliances, debe soportar la configuración de varias instancias del sistema.
- Debe permitir el aprovisionamiento de diferentes administradores para cada uno instancias del sistema.
- 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).
- 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.
- 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);
- Deben soportar al menos cifrados: RSA, PFS, ECDHE y eNull para SSL Offload.
- Debe permitir la configuración del cifrado para SSL Offload.
- Debe soportar la creación de cuentas de administrador con diferentes perfiles y derechos de acceso basado en roles (RBAC).
- El perfil de los administradores debe definirse sobre la base de los derechos a las diferentes funcionalidades del sistema.
- Los derechos de acceso deben ser: Lectura, Escritura (y Lectura) y Sin acceso.

- 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.
- 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.
- 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.
- 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.
- Debe contar con filtros que permitan la visualización de eventos de administración: las acciones realizadas por los administradores.
- 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.
- 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.
- 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.
- 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.
- Debe contar con filtros que permitan la visualización de eventos del Firewalls: la política relacionada con el evento.
- 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.
- 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.
- 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.

- 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.
- 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).
- 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.
- Debe ser posible almacenar los registros en el propio sistema.
- Debe permitir la selección del nivel de log que se guardará localmente (Emergencia, Alerta, crítico, error, advertencia, notificación, información y Debug).
- Debe permitir seleccionar el tipo de log a ser almacenados localmente (Eventos, Seguridad y Tráfico) para evitar el uso excesivo de disco.
- Debe ser posible enviar notificaciones y logs a un servidor syslog
- Debe permitir seleccionar el nivel más bajo de log que se enviará al servidor syslog (Emergencia, Alerta, crítico, error, advertencia, notificación, información y Debug).
- Debe permitir el envío de registros al servidor syslog en formato CSV.
- Debe permitir seleccionar el tipo de registro para ser enviados al servidor syslog.
- 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.
- 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.
- Debe permitir y generar informes por demanda o programados.
- Debe permitir el envío por correo electrónico de los informes programados en formato PDF.

GARANTÍAS

- Todo equipo mencionado en este documento deberá de tener garantía por un periodo de tres años en todos sus componentes físicos y de software. Además, 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 duración antes mencionado.

TRANSFERENCIA DE CONOCIMIENTOS.

Deberán proporcionarse al menos tres sesiones de transferencia de conocimiento formales para que tres personas dominen la configuración, operación y manejo de problemas de la plataforma ofertada.

SERVICIOS DE INSTALACIÓN Y SOPORTE TÉCNICO.

El licitante como parte de su propuesta 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:

- 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 contrato el Licitante 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.

VI.- Lugar y fecha de emisión

México, Ciudad de México a 9 de octubre de 2017.

Guillermo Preciado López	INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN FECHA DE RECEPCIÓN: 9-oct-17 AUTORIZA: José Luis Hernández S. REVISO: Guillermo Preciado López REF: DGTI: INAI/SE/DGTI/769/17
Responsable del proyecto	**Sello DGTI**

Presenta:

JOSÉ LUIS HERNÁNDEZ SANTANA
Director General de Tecnologías de la Información

Autoriza:

JOSÉ DE JESÚS RAMÍREZ SÁNCHEZ
Secretario Ejecutivo

ÚLTIMA PÁGINA DE LA JUSTIFICACIÓN ECONÓMICA PARA EL PROGRAMA DE ADQUISICIÓN DE UNA SOLUCIÓN DE SEGURIDAD DE APLICACIONES PARA EL INAI ----------