PROVISIÓN E IMPLEMENTACIÓN DE SOLUCION DE SEGURIDAD PERIMETRAL PARA LAS APLICACIONES WEB E INFRAESTRUCTURA DEL SENACE	
1. NOMBRE DEL ÁREA:	Oficina de Tecnologías de la Información - OTI
2. RESPONSABLE DE LA EVALUACIÓN:	Sandibel Buiza Cabello
3. CARGO:	Especialista en Soporte Técnico II
4. FECHA:	04 de mayo de 2016

- El presente informe se ha elaborado sobre la base del Decreto Supremo N° 024-2006-PCM Reglamento de la Ley N° 28612 - Ley que norma el uso, adquisición y adecuación del software en la Administración Pública.
- Las herramientas que se toman en consideración en el presente informe, son las disponibles en el mercado peruano, que cuenten con soporte local a través de una red de asociados de negocio que aseguren el adecuado soporte en el tiempo y la pluralidad de ofertas.

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN V°B° LUZ MARIA RAMOS MACHUCA JEFA

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN V°B° Sandibel Buiza Cabello Especialista en Soporte Técnico II SENACE

5. JUSTIFICACIÓN:

El SENACE tiene planificado ejecutar un proceso que contempla la adquisición de equipos de seguridad perimetral que permita la prevención de intrusos – IPS que engloba componentes de hardware, software y servicios de instalación, configuración adecuación, correlación y monitoreo de la solución, así como su integración con los equipos de seguridad perimetral existentes en la entidad (Ver Anexo 1).

El equipo de seguridad perimetral es una solución que realizará el monitoreo, la detección y el bloqueo de cualquier intento de intrusión, transmisión de código malicioso o amenazas a través de la red de manera proactiva que se dirige a los servidores y a la red interna.

Uno de los componentes de la plataforma es una consola de gestión, en el cual resida el software de administración que permite tener visibilidad y control sobre la actividad dentro de la red, las vulnerabilidades, las amenazas, las aplicaciones del lado del cliente, archivos y sitios web.

6. ALTERNATIVAS

Considerando la importancia de contar con una plataforma de administración que permita la gestión y monitoreo de los servicios, se han determinado las siguientes alternativas:

Producto	Fabricante
McAfee Network Security - IPS	McAfee
Cisco FirePower - IPS	Cisco

Para la determinación de estas herramientas, así como para la evaluación técnica, se ha tomado como referencia:

a) Presentaciones de los representantes de las empresas proveedoras de soluciones de software.
b) La información disponible en la página web de cada uno de los fabricantes.
c) Información disponible en Internet.
d) Cuadrante de Gartner, ver Anexo 2.
e) Evaluaciones similares en otras instituciones del Estado Peruano.

Es importante remarcar que los productos McAfee Network Security - IPS y Cisco FirePower - IPS, son de tipo Propietario.

7. ANÁLISIS COMPARATIVO TÉCNICO

El análisis comparativo técnico está basado en la metodología establecida en la Guía Técnica sobre Evaluación de Software para la Administración Pública, aprobada por Resolución Ministerial N° 139-2004-PCM.

7.1. Propósito de la evaluación

Identificar características de calidad mínimas de la solución de seguridad perimetral de prevención de intrusos – IPS

7.2. Tipo de producto

Software de Gestión para la Seguridad Perimetral para la Infraestructura de SENACE.

7.3. Modelo de Calidad

Se aplica el modelo establecido en la Guía Técnica sobre Evaluación de Software para la Administración Pública (R.M. N° 139-2004-PCM).

7.4. Selección de métricas

La selección de métricas se obtuvo a partir de los atributos especificados en el Modelo de Calidad, tal como se detalla en el **Anexo N°3: "Atributos de evaluación de software".**

Para cuantificar cada uno los requisitos o requerimientos se ha asignado un valor de acuerdo al siguiente cuadro:

Detalle	Valor
Cumplimiento de requisito a nivel Alto	3
Cumplimiento de requisito a nivel Medio	2
Cumplimiento de requisito a nivel Bajo	1

Considerando que la suma de los puntajes máximos es 100 para la evaluación de alternativas, se considerará la siguiente tabla de aceptación de alternativas, para la provisión de sistema de virtualización de servidores para el SENACE.

Rango de Puntaje	Descripción
[75- 100>	**Altamente Recomendable.** Cumple totalmente con los requerimientos y expectativas.
[50-74>	**Riesgoso** Cumple parcialmente con los requerimientos, pero no se garantiza su adaptación a las necesidades.
[0-49>	**No recomendable.** Software con características inadecuadas.

7.5. Comparativo Técnico/Funcional

El siguiente cuadro describe el resultado de la evaluación por cada alternativa, agrupada desde el punto de vista del modelo de calidad sugerido por la Oficina Nacional de Gobierno Electrónico de la PCM.

Modelo/Característica/Sub Características		Alternativas	
		McAfee Network Security	Cisco FirePower
Calidad Interna y Externa		**82**	**85**
Funcionalidad	Seguridad	33	33
	Exactitud	6	6
Fiabilidad	Recuperabilidad	3	3
	Madurez	3	3
Usabilidad	Entendimiento	2	2
	Operabilidad	2	2
	Aprendizaje	5	6
	Atracción	10	12
Eficiencia	Comportamiento de tiempos	3	3
Capacidad de Mantenimiento	Capacidad de ser analizado	3	3
	Estabilidad	6	6
Portabilidad	Coexistencia	3	3
	Reemplazabilidad	3	3
Calidad de Uso		**15**	**15**
Eficacia		3	3
Productividad		3	3
Satisfacción		6	6
Seguridad		3	3
Total		**97**	**100**

El detalle de la evaluación por cada funcionalidad se describe en el **Anexo 4.**

8. ANALISIS COMPARATIVO COSTO-BENEFICIO

Costos referenciales de licencias, actualización, soporte y mantenimiento por 3 años.

ID	Producto	Licencias	Fabricante	Precio Referencia (S/.)
1	Cisco FirePower	Sí	CISCO	S/. 195,542.70 [1]
2	McAfee Network Security	Sí	MCAFEE	S/. 120,620.00 [2]

Los costos asociados a la adquisición de esta solución son mínimos comparados con el ahorro de tiempo en horas hombre para identificar, controlar y contener un Ciberataque y las perdidas tangibles por la pérdida de información y datos antes, durante y después de un Ciberataque, así como los intangibles asociados a la imagen de vulnerabilidad que estos dejan.

[1] Cotización de proveedor – IPS Cisco Fire Powerm de fecha 18 de Abril de 2016.
[2] Cotización de proveedor – IPS McAfee Network Security, de fecha 03 de Mayo de 2016.

Beneficios:

Los Principales beneficios al adquirir esta solución son los siguientes:

- Protege monitorea, detecta y bloquea cualquier intento de intrusión, transmisión de código malicioso o amenazas a través de la red de manera proactiva que se dirige a los servidores y a la red interna.
- Personal capacitado para mejorar las estrategias defensivas de la seguridad perimetral.

Nota: El costo aproximado es referencial del mercado local y fue obtenida desde ofertas publicadas en Internet. Se precisa que es potestad de la Unidad de Logística, realizar el estudio de mercado, según la normatividad vigente.

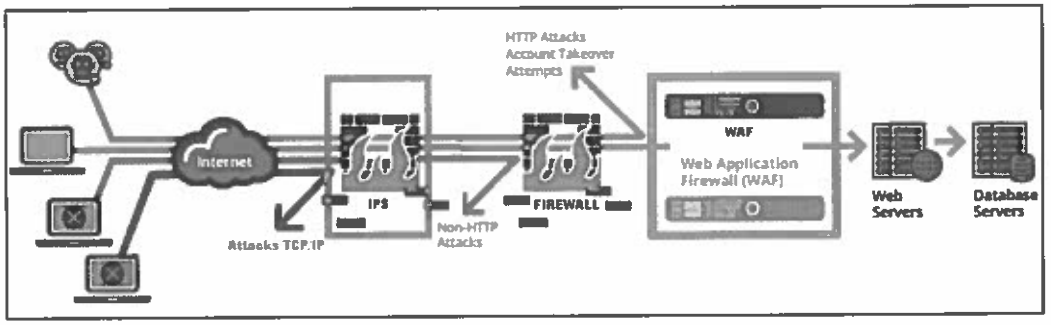
9. CONCLUSIONES

Las herramientas de software analizadas cumplen con los requisitos técnicos mínimos requeridos por la OTI; por lo que esta oficina recomienda realizar el proceso de adquisición incluyendo estas herramientas. Asimismo, si es necesario, se recomienda adquirir cualquier otra que satisfaga con los requerimientos técnicos mínimos establecidos.

10. FIRMAS

ELABORADO POR: Sandibel Buiza Cabello Especialista en Soporte Técnico II	APROBADO POR: Luz Maria Ramos Macavilca Jefa (e) de Oficina de Tecnologías de la Información
FIRMA :	FIRMA :

ANEXO 1: ESQUEMA TECNOLÓGICO DE LA SOLUCIÓN



ANEXO 2: CUADRANTE DE GARTNER[3]

[3] Gartner Inc. es una empresa consultora y de investigación de las tecnologías de la información a nivel mundial.

ANEXO 3: CRITERIOS PARA LA EVALUACION DE SOFTWARE

3.1 TABLA RESUMEN DE PUNTAJES MÁXIMOS POR CARACTERISTICAS

Características	Puntaje Máx.
	100
Calidad Interna y Externa	**85**
Funcionalidad	39
Fiabilidad	6
Usabilidad	22
Eficiencia	3
Capacidad de mantenimiento	9
Portabilidad	6
Calidad de Uso	**15**
Eficacia	3
Productividad	3
Satisfacción	6
Seguridad	3

3.2 TABLA DETALLADA DE PUNTAJES MÁXIMOS POR CARACTERISTICAS/SUB-CARACTERISTICAS

CALIDAD INTERNA Y EXTERNA PUNTAJE MAXIMO: 85		
Característica	**Sub Característica**	**Puntaje Máximo**
Funcionalidad La capacidad del producto de software para proveer las funciones que satisfacen las necesidades explícitas e implícitas cuando el software se utiliza bajo condiciones Específicas. **Puntaje máximo: 39**	**Seguridad** La capacidad del producto de software para proteger la información y los datos de modo que las personas o los sistemas o autorizados no puedan leerlos o modificarlos, y a las personas o sistemas autorizados no se les niegue el acceso a ellos. La seguridad en un sentido amplio se define como característica de la calidad en uso, pues no se relaciona con el software solamente, sino con todo un sistema.	33
	Exactitud La capacidad del producto de software para proveer los resultados o efectos acordados con un grado necesario de precisión.	6
Fiabilidad La capacidad del producto de software para mantener un nivel específico de funcionamiento cuando se está utilizando bajo condiciones especificadas. **Puntaje máximo: 6**	**Recuperabilidad** La capacidad del producto de software para restablecer un nivel especificado de funcionamiento y recuperar los datos afectados directamente en el caso de una falla.	3
	Madurez La capacidad del producto de software para evitar fallas como resultado de errores en el software.	3
Usabilidad La capacidad del producto de software de ser entendido, aprendido, usado y atractivo al usuario, cuando es utilizado bajo las condiciones especificadas. **Puntaje máximo: 22**	**Entendimiento** La capacidad del producto de software para permitir al usuario entender si el software es adecuado, y cómo puede ser utilizado para las tareas y las condiciones particulares de la aplicación.	2
	Operabilidad La capacidad del producto de software para permitir al usuario operarlo y controlarlo.	2
	Aprendizaje La capacidad del producto de software para permitir al usuario aprender su aplicación. Un aspecto importante a considerar aquí es la documentación del software.	6
	Atracción La capacidad del producto de software de ser atractivo al usuario.	12
Eficiencia La capacidad del producto de software para proveer un desempeño adecuado, de acuerdo a la cantidad de recursos utilizados y bajo las condiciones planteadas. Los recursos pueden incluir otros productos de software,, la configuración de hardware y software del sistema, y materiales (Ej: Papel de impresión o diskettes). **Puntaje máximo: 3**	**Comportamiento de tiempos** La capacidad del producto de software para proveer tiempos adecuados de respuesta y procesamiento, y ratios de rendimiento cuando realiza su función bajo las condiciones establecidas.	3

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN – V°B° – LUZ MARIA RAMOS MACAHUCA – JEFA – SENACE

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN – V°B° – Sandro Luiza Cabello – Especialista en Soporte Técnico II – SENACE

Capacidad de mantenimiento Capacidad del producto de software para ser modificado. Las modificaciones pueden incluir correcciones, mejoras o adaptación del software a cambios en el entorno, y especificaciones de requerimientos funcionales.y software del sistema, y materiales (Ej: Papel de impresión o diskettes). **Puntaje máximo: 9**	**Capacidad de ser analizado** La capacidad del producto de software para atenerse a diagnósticos de deficiencias o causas de fallas en el software o la identificación de las partes a ser modificadas.	3
	Estabilidad La capacidad del producto de software para evitar efectos inesperados debido a modificaciones del software.	6
Portabilidad La capacidad del software para ser trasladado de un entorno a otro. El entorno puede incluir entornos organizacionales, de hardware o de software. **Puntaje máximo: 6**	**Coexistencia** La capacidad del producto de software para coexistir con otros productos de software independientes dentro de un mismo entorno, compartiendo recursos comunes.	3
	Reemplazabilidad La capacidad del producto de software para ser utilizado en lugar de otro producto de software, para el mismo propósito y en el mismo entorno.	3

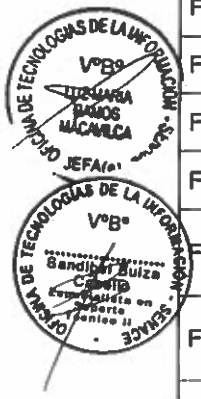
CALIDAD DE USO **PUNTAJE MAXIMO: 15**	
Característica	**Puntaje Máximo**
Eficacia La capacidad del producto de software para permitir a los usuarios lograr las metas especificadas con exactitud e integridad, en un contexto especificado de uso. **Puntaje máximo: 3**	**3**
Productividad La capacidad del producto de software para permitir a los usuarios emplear cantidades apropiadas de recursos, en relación a la eficacia lograda en un contexto especificado de uso. **Puntaje máximo: 3**	3
Satisfacción La satisfacción es la respuesta del usuario a la interacción con el producto, e incluye las actitudes hacia el uso del producto. **Puntaje máximo: 6**	6
Seguridad La capacidad del producto de software para lograr niveles aceptables de riesgo de daño a las personas, institución, software, propiedad (licencias, contratos de uso de software) o entorno, en un contexto especificado de uso. **Puntaje máximo: 3**	3

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN V°B° LUZ MARIA RAMOS MACAVILCA JEFA(e) SENACE

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN V°B° Bandel Ruiza Caballo Especialista en Soporte Técnico II SENACE

ANEXO 4. EVALUACION DETALLADA DE LAS HERRAMIENTAS DE SOFTWARE

Característica [1]	Sub Categoría	Métrica	Puntaje Máx.	Alternativas	
				McAfee Network Security	Cisco FirePower
CALIDAD INTERNOS Y EXTERNOS (PUNTAJE MÁXIMO: 85)					
Funcionalidad	Seguridad	Prevención de pérdida de datos (claves y códigos de seguridad) e información de identificación personal (cuentas, contraseñas, otros.)	Alto	Alto	Alto
Funcionalidad	Seguridad	Previene de manera razonable los ataques a los servidores públicos y la red interna.	Alto	Alto	Alto
Funcionalidad	Seguridad	Envío de alertas y eventos en tiempo real sobre intrusion, discovery, malware, correlation, connection events, health status change).	Alto	Alto	Alto
Funcionalidad	Seguridad	Permite la creación de reglas para el bloqueo específico de ataques (SQL, DoS, Executables, otros)	Alto	Alto	Alto
Funcionalidad	Seguridad	Protección y detección proactiva de amenazas provenientes de Internet conocidas y desconocidas.	Alto	Alto	Alto
Funcionalidad	Seguridad	Permitir detectar anomalías en protocolos de red, minimizando los falsos positivos y falsos negativos en la identificación de ataques	Alto	Alto	Alto
Funcionalidad	Seguridad	Dispone de la opción de consulta, donde se realiza la búsqueda del histórico de los eventos sucedidos en los equipos ofertados desde la consola principal, con el fin de realizar análisis forense.	Alto	Alto	Alto
Funcionalidad	Seguridad	Soportar reglas de contenido con al menos los siguientes parámetros: Message; Reference; Action; Protocol; SID; GID; Direction, Source IP, Destination IP, Source port; Destination port; Rule overhead, Metadata.	Alto	Alto	Alto
Funcionalidad	Seguridad	Soportar reglas por plataforma tal como: Apple; Cisco; Compaq; HP; IBM; Juniper; Microsoft; Nokia; RedHat; Suse; Sun; Juniper.	Alto	Alto	Alto
Funcionalidad	Seguridad	Permite el bloqueo de ataque, tráfico malicioso o tráfico no deseado.	Alto	Alto	Alto
Funcionalidad	Seguridad	Permite realizar excepciones en el filtro de protocolos TCP, UDP, ICMP que no serán analizados	Alto	Alto	Alto
		Sub total Seguridad	**33**	**33**	**33**
Funcionalidad	Exactitud	Actualización automáticas (programadas) y manuales de seguridad y de firmas	Alto	Alto	Alto
Funcionalidad	Exactitud	La actualización de vulnerabilidades y mantenimiento (parches y actualizaciones) se efectuará desde el sitio Web del fabricante y ser automático.	**Alto**	Alto	Alto
		Sub total Exactitud	**6**	**6**	**6**



Característica [1]	Sub Categoría	Métrica	Puntaje Máx.	Alternativas	
				McAfee Network Security	Cisco FirePower
Fiabilidad	Recuperabilidad	Permite realizar backup de la configuración, mediante un menú de Respaldo y Restauración.	Alto	Alto	Alto
		Sub total Recuperabilidad	**3**	**3**	**3**
Fiabilidad	Madurez	Reconocido como líder o challenger en el cuadrante de Gartner a la fecha del comparativo.	Alto	Alto	Alto
		Sub total Madurez	**3**	**3**	**3**
Usabilidad	Entendimiento	Dispone de manuales y base de conocimiento para la solución de problemas específicos.	Medio	Medio	Medio
		Sub total Entendimiento	**2**	**2**	**2**
Usabilidad	Operabilidad	Permitir la administración de manera centralizada a través de conexiones SSH, CLI y HTTPS.	Medio	Medio	Medio
		Sub total Operabilidad	**2**	**2**	**2**
Usabilidad	Aprendizaje	Realiza el análisis dinámico y en tiempo real para crear un mapa de la red monitoreada considerando: Redes existentes; Host activos; Host o servers en la red; MAC address en la red; Máquinas virtuales; Sistema operativo de cada uno de los host; Servicios activos, Aplicaciones activas; vulnerabilidades de cada uno de los host identificados	Alto	Alto	Alto
Usabilidad	Aprendizaje	Fácil y rápido de comprender para la gestión y operatividad (tareas) del administrador de TI.	Alto	Medio	Alto
		Sub total Aprendizaje	**6**	**5**	**6**
Usabilidad	Atracción	Debe contar con una interface de administración vía web amigable para el administrador de TI .	Alto	Alto	Alto
Usabilidad	Atracción	Cuenta con una visión general que visualice los Top de intrusos, información de aplicaciones, geolocalización de Ip´s en tiempo real.	Alto	Medio	Alto
Usabilidad	Atracción	Permite elaborar reportes (cuenta con plantilla predefinidas)	Alto	Alto	Alto
Usabilidad	Atracción	Permite visualizar la trayectoria del dispositivo mediante gráfica de línea de tiempo y brindar información del origen de un ataque.	Alto	Medio	Alto
		Sub total Atracción	**12**	**10**	**12**
Eficiencia	Comportamiento de tiempos	Alto rendimiento para realizar el análisis (velocidad de procesamiento)	Alto	Alto	Alto
		Sub total Comportamiento de tiempos	**3**	**3**	**3**
Capacidad de mantenimiento	Capacidad de ser analizado	Dispone de un registro (logs) detallado de errores en el funcionamientos y operatividad de la solución	Alto	Alto	Alto

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - SENACE
V°B°
LUZMINDA RAMOS MACAVILCA
JEFA
OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - SENACE
V°B°
Sandra Ruiza Cadelle
Especialista en Soporte Técnico II

Característica [1]	Sub Categoría	Métrica	Puntaje Máx.	Alternativas	
				McAfee Network Security	Cisco FirePower
		Sub total Capacidad de ser analizado	**3**	**3**	**3**
Capacidad de mantenimiento	Estabilidad	Cuenta con soporte local, vía telefónico o correo electrónico.	Alto	Alto	Alto
Capacidad de mantenimiento	Estabilidad	Dispone de parches y actualizaciones de version.	Alto	Alto	Alto
		Sub total Estabilidad	**6**	**6**	**6**
Portabilidad	Coexistencia	Compatible con la solución de seguridad permetral - firewall existente.	Alto	Alto	Alto
		Sub total Coexistencia	**3**	**3**	**3**
Portabilidad	Reemplazabilidad	Permite la actualización de versiones superiores, actualización de firmas manuales y automáticas.	Alto	Alto	Alto
		Sub total Reemplazabilidad	**3**	**3**	**3**
CALIDAD DE USO (PUNTAJE MÁXIMO: 15)					
Eficacia	Capacidad de alcanzar metas operativas.		Alto	Alto	Alto
		Sub total Eficacia	**3**	**3**	**3**
Productividad	La configuración se realiza en un tiempo adecuado.		Alto	Alto	Alto
		Sub total Productividad	**3**	**3**	**3**
Satisfacción	El usuario interactúa con familiaridad con el producto y en total conformidad.		Alto	Alto	Alto
Satisfacción	Permite reducir significativamente el esfuerzo del administrador de TI, mediante la aceleración de respuesta a las amenazas.		Alto	Alto	Alto
		Sub total Satisfacción	**6**	**6**	**6**
Seguridad	Capacidad de ser software confiable.		Alto	Alto	Alto
		Sub total Seguridad	**3**	**3**	**3**
PUNTAJE TOTAL			**100**	**97**	**100**

Puntaje de adecuación: (Nivel Alto: 3, Nivel Medio: 2, Nivel Bajo: 1)