Informe Técnico Previo de Evaluación de Software N° 001 -2023
Sustento Técnico para la Adquisición de Licencias de Software Antivirus Empresarial

1. NOMBRE DEL ÁREA

Oficina de Tecnología de la Información y la Comunicación - OTI

2. RESPONSABLE DE LA EVALUACIÓN

Nombre	:	Jesús Miguel Rojas Hernández
Cargo	:	Coordinador Unidad Funcional de Infraestructura
Nombre	:	Hammerly Scoot Ruiz Cayao
Cargo	:	Especialista en Administración de Base de Datos.

3. FECHA

24/01/2023

4. JUSTIFICACIÓN

Actualmente el Servicio Nacional de Meteorología e Hidrología del Perú – SENAMHI, es un organismo público ejecutor adscrito al Ministerio del Ambiente, tiene como propósito generar y proveer información y conocimiento meteorológico, hidrológico y climático de manera confiable, oportuna y accesible en beneficio de la sociedad peruana, con el ánimo de difundir información confiable y de calidad, el SENAMHI opera, controla, organiza y mantiene la Red Nacional de más de 900 Estaciones Meteorológicas e Hidrológicas de conformidad con las normas técnicas de la Organización Meteorológica Mundial (OMM).

El Servicio Nacional de Meteorología e Hidrología del Perú - SENAMHI necesita contar con una solución que garantice la adecuada protección de la información almacenada en los equipos y de los sistemas informáticos de la institución, de ser modificada, borrada o afectada por programas no deseados como virus informáticos, troyanos, spyware y nuevas variantes de los mismos.

En base a las nuevas amenazas es necesario considerar funcionalidades específicas para mitigar los riesgos con que actúen los softwares de código malicioso-malware. Por lo cual se requieren software antivirus robustos por ser una institución de impacto nacional.

Actualmente el Servicio Nacional de Meteorología e Hidrología del Perú – SENAMHI cuenta con un software ANTIVIRUS, que incluyen licencias hasta el 01 de marzo del 2023. Por ello, es crucial contar con una nueva solución de protección antivirus para los equipos informáticos (End Point) debido al nivel de tráfico de información en la red interna (LAN) y extendida (WAN).

Por lo expuesto y en el marco de la ley 28612 "Ley que norma el uso, adquisición y adecuación del software del a Administración Pública", se procede a evaluar el Software antivirus corporativo.

5. ALTERNATIVAS DE EVALUACIÓN

Considerando los requerimientos del Servicio Nacional de Meteorología e Hidrología del Perú - SENAMHI, se han buscado diversos softwares en el medio local que cumplan con los requerimientos.

Es por ello, que la herramienta de software que sea seleccionada debe contener como mínimo las funcionalidades que permitan mayor protección a la información que se maneja en el SENAMHI.

Por lo mencionado, se ha establecido parámetros en base a la experiencia y a las mejores prácticas en el SENAMHI, estableciendo criterios que fortalezcan la seguridad en las T.I. obteniendo disponibilidad, integridad y confidencialidad, como factores que conlleven a una mejor evaluación.

En base a estas premisas y la información encontrada se está evaluando las siguientes soluciones:

- McAfee
- Kaspersky
- Eset NOD
- Sophos

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

- ✓ Información disponible en las páginas web de cada uno de los fabricantes.
- ✓ Información disponible en Internet.
- ✓ Cuadrante de Gartner, anexo 1.
- ✓ Evaluaciones similares en otras instituciones del Estado Peruano.

6. ANALISIS COMPARATIVO TÉCNICO

El análisis técnico ha sido realizado en conformidad con la metodología establecida en la "Guía Técnica sobre evaluación de software en la administración Pública RM 139-2004 - PCM".

Propósito de la Evaluación:
Validar que las alternativas seleccionadas sean las más convenientes para el SENAMHI.

Determinar las características del software de protección para servidores y equipos de escritorio líder en el sector, seleccionando aquellas que satisfagan la necesidad de gestionar eficientemente los procesos de protección.

Identificador de tipo de producto:
Software antivirus corporativo para servidores y equipo de escritorio.

Selección de Métricas:

Las métricas fueron identificadas de acuerdo con los Términos de Referencia del SENAMHI y a los antecedentes de evaluación para este tipo de software en el sector público peruano.

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 una solución de software para la entidad.

Puntaje	Descripción
[90-100]	**Altamente recomendado** Cumple con los requerimientos y expectativas
[45-89]	**Riesgoso.** Cumple parcialmente con los requerimientos, no se garantiza su adaptación a las necesidades.
[0-44]	**No recomendable.** Solución informática con características inadecuadas.

Realizando las evaluaciones respectivas para los productos, se obtiene la siguiente tabla:

DESCRIPCIÓN	CARACTERÍSTICAS	Puntaje Máximo	SOPHOS	McAfee	KASPERSKY	ESET NOD
FUNCIONALIDAD	Detección y bloqueo de software no autorizado, de forma automática. Capturar amenazas que todavía no tienen firma, incluyendo las amenazas de día cero. Debe permitir escaneos programados. Manejo flexible de las licencias, permitiendo la reasignación en caso suceda cambio de equipo servidor o de escritorio.	**15**	13	13	14	13

FIABILIDAD	Pertenecer o estar dentro del grupo líder en el cuadrante de Gartner. Los análisis, revisiones y escaneos que la solución haga NO debe afectar el rendimiento ni la performance de los equipos. Alto rendimiento para realizar el análisis (velocidad de procesamiento). Sistema basado en la reputación de sitios web.	**10**	10	9	9	9
COMPATIBILIDAD	Microsoft Windows Server 2008 Microsoft Windows Server 2012 Microsoft Windows 7 y superior	**10**	10	9	9	10
	Linux MAC					
USABILIDAD	Cuenta con una única consola de administración para administrar todas las funcionalidades. Disminuye la superficie de ataque de servidores físicos y virtuales, y equipos de escritorio con filtrado preciso, políticas por la red y notificación de ubicación para los protocoles basados en IP y tipos de tramas.	**15**	14	14	13	14
EFICACIA	Análisis proactivo de amenazas en base a comportamientos sospechosos. Protege frente a ataques sofisticados en entornos virtuales aislando los malware de componentes de seguridad y sistemas operativos críticos.	**15**	13	13	14	15
PRODUCTIVIDAD	La solución actualiza sus firmas por lo menos una vez al día. Optimiza operaciones de seguridad para evitar tormentas de antivirus vistas habitualmente en exploraciones de sistemas completo y actualizaciones de patrones de prestaciones de seguridad tradicionales.	**10**	10	10	10	10

SATISFACCION	Permitir tomar distintas acciones cuando sea detectado un virus o un ataque. Mantener un buen performance con los aplicativos institucionales, permitiendo una correcta operatividad con los mismos.	**10**	8	9	9	9
SEGURIDAD	Examina todo tráfico entrante y saliente en busca de desviaciones de protocolos, infracciones de políticas o contenido que haga sospechar de un ataque. La solución cuenta con tecnología de detección de intrusos o prevención de intrusos. Identifica y analiza objetos sospechosos a través del análisis en recinto aislado.	**15**	14	15	15	15
TOTAL		**100**	92	92	93	95

7. ANALISIS DE COSTO BENEFICIO

Licenciamiento:

Se realiza un análisis de costos referenciales de 675 + 25 licencias adicionales por un año:

Software	Licencia	Fabricante	Precio REFERENCIAL
Sophos Intercept X Advanced	SI	Sophos	S/ 46.000.00
McAfee	SI	McAfee	S/ 53.000.00
Kaspersky Select	SI	Kaspersky	S/ 46.000.00
ESET NOD	SI	ESET	S/ 46 000.00

Hardware necesario para su funcionamiento:

La herramienta funciona en la plataforma informática con la que cuenta el SENAMHI sin necesidad de hacerse de inversión adicional.

Soporte y Mantenimiento externo:

No se requiere hacer gastos adicionales con respecto a este componente, pues cada uno de los proveedores garantiza soporte para su producto.

Capacitaciones:

El SENAMHI cuenta con personal técnico que tiene conocimiento del manejo de productos antivirus empresariales, por lo que la capacitación en esta herramienta sería adoptada de manera fácil y rápida. Así mismo el proveedor deberá dar la capacitación respectiva para el área técnica correspondiente, la misma que no generará sobrecostos en la adquisición de la solución.

Los costos referenciales se obtendrán del estudio de mercado realizado por el área especializada de la Unidad de Abastecimiento del SENAMHI.

8. CONCLUSIONES

En base al análisis de la evaluación técnica y el análisis costo beneficio, se precisa que el Software Antivirus que con igual o mayor puntaje de noventa (90) deben ser tomados en cuenta para la adquisición.

9. FIRMAS

Jesús Miguel Rojas Hernandez Coordinador Unidad Funcional de Infraestructura - OTI	Firma Digital Senamhi Firmado digitalmente por ROJAS HERNANDEZ Jesus Miguel FAU 20131366028 soft Motivo: Soy el autor del documento Fecha: 24.01.2023 15:47:44 -05:00
Hammerly Scoot Ruiz Cayao Especialista en Administración de Base de Datos - OTI	Firma Digital Senamhi Firmado digitalmente por RUIZ CAYAO Hammerly Scoot FAU 20131366028 hard Motivo: Soy el autor del documento Fecha: 24.01.2023 15:46:52 -05:00

ANEXO 1

Cuadrante de Gartner – Antivirus