INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE N° 005-2023-ANA-DSNIRH

SOFTWARE ANTIVIRUS

1. NOMBRE DEL ÁREA

Dirección del Sistema Nacional de Información de Recursos Hídricos

2. RESPONSABLES DE LA EVALUACIÓN

Nombre: Ing. Javier Eduardo Suarez Niño
Director
Dirección del Sistema Nacional de Información de Recursos Hídricos

Nombre: Tec. Pablo Demetrio Carrión Méndez
Cargo: Coordinador de la Mesa de Servicios TI

3. FECHA

18 de agosto de 2023

4. JUSTIFICACIÓN

La Autoridad Nacional del Agua - ANA 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 alterada, eliminada o copiada sin previo conocimiento del usuario responsable mediante el empleo de programas no deseados como virus informáticos, troyanos, spyware, ransomware y toda la variante de los mismos.

En base a que diariamente se crean nuevas amenazas, es necesario considerar funcionalidades específicas para mitigar los riesgos con que actúan los softwares con código malicioso (malware). Para lo cual se requiere adquirir un software antimalware con capacidades de prevención, mitigación, detección y recuperación ante amenazas cibernéticas (malware) para la institución con el fin de asegurar el tráfico de información en la red interna (LAN) y extendida (WAN).

A la fecha la ANA cuenta con un software ANTIVIRUS, que incluye licencias hasta el 20 de diciembre del 2023. Por ello, es urgente el contar con una nueva solución de protección antivirus para los equipos informáticos.

Por lo expuesto y en el marco de la ley 28612 “Ley que norma el uso, adquisición y adecuación del software de la Administración Pública”, se procede a evaluar el Software antivirus que cubre las necesidades de la institución.

Firmado digitalmente por SUAREZ NIÑO Javier Eduardo FAU 20520711865 hard
Motivo: Doy V° B°

Firmado digitalmente por CARRION MENDEZ Pablo Demetrio FAU 20520711865 hard
Motivo: Soy el autor del documento

5. ALTERNATIVAS DE EVALUACIÓN:

Considerando los requerimientos de la Autoridad Nacional del Agua, se ha buscado alternativas de software en el mercado con soporte local que cuenten con características y requerimientos de implementación semejantes que cubran las necesidades de protección que tiene la institución.

Teniendo que se debe contar con una herramienta de software que cuente como mínimo las funcionalidades que permitan mayor protección a la información que se maneja en la ANA, se ha considerado como alternativas de solución a:

Fabricante	Procedencia	Producto Evaluado
WatchGuard	Estados Unidos	WatchGuard Endpoint Security
Sophos	Inglaterra	Sophos Intercept X Advanced
Symantec	Estados Unidos	Symantec Endpoint Security Enterprise

Para la determinación de estas soluciones, así como la evaluación técnica y para la elaboración de los términos de referencia, se ha tomado información disponible en las páginas web de cada uno de los productos antivirus a evaluar.

6. ANÁLISIS COMPARATIVO TÉCNICO.

El análisis técnico ha sido realizado en conformidad con la metodología de la "Guía Técnica sobre evaluación de software en la administración pública" (R.M.Nº 139-2004-PCM) tal como se exige en el reglamento de la Ley N.º 28612.

6.1. Propósito de Evaluación

Validar que las alternativas seleccionadas sean las más convenientes para Autoridad Nacional del Agua, que permita cubrir las necesidades de prevención, mitigación, detección y recuperación ante ataques de malware. El propósito es determinar los atributos o características para el producto final.

6.2. Identificar el Tipo de Producto

Software antivirus para la protección contra todo tipo de software malicioso (malware).

6.3. Identificación del Modelo de Calidad

Para la evaluación técnica del Software antivirus se aplicará el modelo de calidad descrito en la parte I de la Guía de evaluación de software aprobada por R.M. Nº 139-2014-PCM y la Ley Nº 28612 – "Ley que norma el uso, adquisición y adecuación del software en la administración pública".

6.4. Selección de Métricas

Las métricas fueron identificadas de acuerdo a la información técnica de los productos de software ofertados, la cual consiste en características del producto, requerimientos de información entre otros:

ANA Firmado digitalmente por SUAREZ NIÑO Javier Eduardo FAU 20520711865 hard Motivo: Doy V° B°

ANA Firmado digitalmente por CARRION MENDEZ Pablo Demetrio FAU 20520711865 hard Motivo: Soy el autor del documento

CUADRO N° 1							
METRICAS: ATRIBUTOS INTERNOS Y EXTERNOS							
N°	**ATRIBUTO**	**DESCRIPCIÓN**	**PUNTAJE MAXIMO**	**PUNTAJE MINIMO**	**WatchGuard**	**Sophos**	**Symantec**
1	Funcionalidad	Adecuación: Soporta Sistema Operativo de estaciones de trabajo: Windows 7/8/10 de 32 y 64 bits y Sistema Operativo de Servidores: Windows 2003 Server 32/64 bits, Windows 008/2012/2012R2/2016 server y Linux.	5	1	5	5	5
		Exactitud: Protección contra amenazas: virus, gusanos, troyanos, keyloggers, dialers, adware, spyware, hacktools, rootkits, bots, phishing, herramientas de control remoto y todo tipo de programa malicioso (malware) incluyendo la protección contra ransomware.	5	1	5	5	5
		Interoperabilidad: Interacción con bases de datos SQL, así como herramientas de Microsoft Office, navegadores de internet, integración con el Directorio Activo.	5	1	5	5	5
		Integración con herramientas de threat intelligent y plataformas de gestión de superficie de ataque y SIEMs.	5	1	5	5	5
		Seguridad: • Capacidad para proteger información y datos. Proteger con contraseña la configuración del antivirus para que no sea alterada además de blindar las aplicaciones que corren sobre los sistemas.	5	1	5	5	5
		• Capacidad de detectar malware sin archivos y ataques combinados.	5	1	5	5	5
		• Capacidad de remediar ataque de ransomware	5	1	5	5	5
2	Fiabilidad	Madurez:	5	1	5	5	5

Firmado digitalmente por SUAREZ NINO Jaime Eduardo FAU 20520711865 hard
Motivo: Doy V° B°

Firmado digitalmente por CARRION MENDEZ Pablo Demetrio FAU 20520711865 hard
Motivo: Soy el autor del documento

		Deberá incluir la protección contra Vulnerabilidades de día cero y alertas de Actualizaciones de software centralizado. Deberá trabajar en simultaneo con gestores de parches, tecnologías SIEM, XDRs y plataformas de Sandboxing.					
		Tolerancia a errores: Deberá permitir la instalación y desinstalación remota del software en el Endpoint centralizadamente, entregando un diagnóstico de las operaciones realizadas.	5	1	5	5	5
3	Eficiencia	Uso de recursos: Reducir el uso de recursos como Memoria, CPU y espacio en disco en máquinas virtuales.	5	1	5	5	5
		Comportamientos de tiempos: Alto rendimiento para análisis y procesos (velocidad de procesamiento)	5	1	5	5	5
4	Mantenimiento	Actualización: • Facilidad para migrar a versiones Superiores, Actualización de firmas manuales y automáticas.	5	1	5	5	5
		• Capacidad de uso de repositorios distribuidos.	5	1	5	5	5
		Soporte: • Servicio técnico local con bolsa de horas ilimitadas.	5	1	5	5	5
		• Soporte del fabricante en casos de amenazas de día cero.	5	1	5	5	5
5	Portabilidad	Coexistencia: La consola centralizada de tener la capacidad de operar en la nube	5	1	3	4	3
				SUBTOTAL	**78**	**79**	**78**

METRICAS: ATRIBUTOS DE USO

	ATRIBUTO	DESCRIPCIÓN	PUNTAJE MAXIMO	PUNTAJE MINIMO	WatchGuard	Sophos	Symantec
1	Eficacia	Capacidad del alcanzar metas	5	1	5	5	5

Firmado digitalmente por SUAREZ NINO Jose Antonio FAU 20520711865 hard
Motivo: Soy V° B°

Firmado digitalmente por CARRION MENDEZ Pablo Demetrio FAU 20520711865 hard
Motivo: Soy el autor del documento

		Operativas/indicadores del usuario en contexto especifico de uso.	5	1	5	5	5
2	Seguridad	La solución como mínimo deberá permitir proteger la navegación de los usuarios a sitios de banco y sitios confiables que se definan mediante el protocolo HTTPS con la finalidad de evitar el phishing o robo de datos a los usuarios.	5	1	5	5	5
3	Satisfacción	Capacidad para cubrir requerimientos con total conformidad del usuario.	5	1	5	5	4
				SUBTOTAL	**20**	**20**	**19**
				TOTAL	**98**	**99**	**97**

ESCALA	DESCRIPCIÓN
1	Deficiente: La tecnología empleada no funciona correctamente y existen reportes de problemas por los usuarios
2	Regular: Tecnología con algunas limitaciones en las características
3	Bueno: Tecnología con algunas limitaciones en desempeño y funcionalidad
4	Muy Bueno: Tecnología con buen desempeño y funcionalidad
5	Excelente: Tecnología de gran desempeño y funcionalidad aprobada a nivel mundial

Del CUADRO N°1, se muestra los resultados de evaluación de los productos considerados para la adquisición de software antimalware el **SOPHOS** como el más adecuado para los fines de la institución.

6.5. Análisis Comparativo Técnico/Funcional

ATRIBUTOS/CARACTERITICAS	WatchGuard	Sophos	Symantec
Deberá contar con una primera exploración automática después de la instalación del programa, lo que permite asegurar que el equipo se encuentre protegido desde el comienzo.	SI	SI	SI
Deberá proteger contra amenazas: virus, gusanos, troyanos, keyloggers, dialers, adware, spyware, hacktools, rootkits, bots, phishing, herramientas de control remoto y todo tipo de programa malicioso (malware) incluyendo la protección contra ransomware	SI	SI	SI
Deberá incluir consola de administración centralizada con funcionalidades de despliegue y gestión híbridos permitiéndose adecuar a diferentes escenarios de red	SI	SI	SI
Deberá poder trabajar en simultaneo con plataformas de gestión de superficie de ataques basada en gestión de parches, cumplimiento y gestión avanzada de anomalias sin impactar en el consumo de recursos y errores de compatibilidad	SI	SI	SI

Se ha observado que en la evaluación las 3 soluciones cumplen con los requerimientos técnico funcional que se requiere en la Entidad.

ANA Firmado digitalmente por SUAREZ NINO Jaime Eduardo FAU 20520711865 hard Motivo: Doy V° B°

ANA Firmado digitalmente por CARRION MENDEZ Pablo Demetrio FAU 20520711865 hard Motivo: Soy el autor del documento

7. ANÁLISIS COMPARATIVO DE COSTO-BENEFICIO.

Análisis Costo – Beneficio de licencias, implementación, actualización, soporte y mantenimiento por 3 años para 2170 licencias.

SOFTWARE	COSTO	VALORACIÓN
WatchGuard	715,552.00	1
Sophos	652,540.00	3
Symantec	705,000.00	2

VALORACION DEL COSTO DE LICENCIAMIENTO:

COSTO	PUNTAJE
Alto Costo	1
Costo Medio	2
Costo Bajo	3

NOTA: Las cotizaciones de referencia se adjuntan al presente en los Anexos

8. CONCLUSIONES

Se determinaron los atributos y/o características mínimas que deben ser considerados para una evaluación de software, para cubrir el requerimiento de la Autoridad Nacional del Agua.

De acuerdo a la evaluación realizada, se sugiere que la mejor alternativa de software antivirus es el SOPHOS, por lo que se recomienda su adquisición no obstante las soluciones seleccionadas con WATCHGUARD y SYMANTEC también podrían participar del proceso de selección.

9. ANEXOS

- ✓ Anexo 01: Cotización WATCHGUARD.
- ✓ Anexo 02: Cotización SOPHOS.
- ✓ Anexo 03: Cotización SYMANTEC.

10. FIRMAS

Nombre	Cargo	Firma
Ing. Javier Eduardo Suarez Niño	Director de la Dirección del Sistema Nacional de Información de Recursos Hídricos.	ANA Firmado digitalmente por SUAREZ NIÑO Javier Eduardo FAU 20520711865 hard Motivo: En señal de Conformidad
Tec. Pablo Demetrio Carrión Méndez	Coordinador de la Mesa de Servicios TI	ANA Firmado digitalmente por CARRION MENDEZ Pablo Demetrio FAU 20520711865 hard Motivo: Doy V° B°

ANA Firmado digitalmente por SUAREZ NIÑO Javier Eduardo FAU 20520711865 hard Motivo: Doy V° B°

ANA Firmado digitalmente por CARRION MENDEZ Pablo Demetrio FAU 20520711865 hard Motivo: Soy el autor del documento