



Decenio de la Igualdad de Oportunidades para mujeres y hombres"
"Año de la Universalización de la Salud"

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE N° 001-2020- ANA-DSNIRH

SOFTWARE ANTIVIRUS

1. NOMBRE DEL ÁREA

Dirección del Sistema Nacional de Información de Recursos Hídricos

2. RESPONSABLES DE LA EVALUACIÓN

Lic. Edwin Dante Quispe Soto
Director

Dirección del Sistema Nacional de Información de Recursos Hídricos

Nombre: Tec. Pablo Demetrio Carrión Méndez
Cargo: Coordinador de Soporte Técnico

3. FECHA

04 de setiembre de 2020

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 07 de diciembre del 2020. 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.





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
Panda Security	España	Panda Fusion 360
Bitdefender	Rumania	Bitdefender Ultra Plus
Gdata	Alemania	Gdata Endpoint Protection Business

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:





CUADRO 1
METRICAS: ATRIBUTOS INTERNOS Y EXTERNOS

N°	ATRIBUTO	DESCRIPCIÓN	PUNTAJE MAXIMO	PUNTAJE MINIMO	GDATA	PANDA	BITDEFENDER
1	Funcionalidad	Brindar un sistema de gestión centralizado híbrido para entornos OnPremise y Cloud lográndose integrar al directorio activo en los dos escenarios	3	1	3	3	3
		Compatibilidad con sistemas operativos Windows, Linux, Mac, iOS y Android	3	1	3	3	3
		Debe incluir inventario de hardware y software con reconocimiento de vulnerabilidades a nivel parches	3	1	3	3	1
		Debe incluir la gestión de parches de actualización multiplataforma	3	1	3	3	3
		Debe incluir módulo de control de aplicaciones basado en listas blancas y listas negras	3	1	3	3	1
		Debe incluir módulo de control de dispositivos con capacidad de configurar listas blancas basadas en ID del hardware	3	1	3	3	1
		Deber incluir módulo de control de contenido web con capacidad de filtrar páginas web basadas en categorías	3	1	3	3	3
		Debe incluir tecnología de detección basado en firmas, supervisión de conducta, inteligencia artificial y machine learning.	3	1	3	3	3
		Debe incluir funcionalidades que permitan explorar el performance de la red y tomar acciones preventivas ante comportamientos anómalos.	3	1	3	3	3
2	Fiabilidad	Sistema de generación de informes y programación de envío de alertas	3	1	3	3	3
		Debe contar con soporte local 24x7 para asistencias presenciales y/o remotas por parte del postor o integrador	6	0	6	0	6
		Debe contar con soporte local 24x7 para asistencias presenciales y/o remotas por parte del postor o integrador	6	0	6	6	6
3	Usabilidad	Debe incluir un sistema de acceso a la consola de administración basado en perfiles	4	0	4	4	4





		Consola de administración portable para acceso de técnicos en diferentes ubicaciones	4	0	4	0	0
		Configuración especial para equipos de bajo performance	4	0	4	0	0
		Posibilidad de solicitar permisos de acceso a web, aplicaciones y dispositivos desde el usuario	4	0	4	0	0
		Posibilidad de enviar mensajes de alertas en las pantallas de los usuarios	4	0	4	0	0
4	Adaptabilidad	Adaptabilidad a trabajos específicos sin necesidad de conocimientos previos avanzados de software	8	1	6	6	8
		Fácil recuperación y/o migración de infraestructura (Respaldo de base de datos)	8	1	8	8	8
5	Adecuación	Se adecua plenamente a las funciones requeridas	8	1	8	4	6
					84	58	62



METRICAS: ATRIBUTOS DE USO

	ATRIBUTO	DESCRIPCIÓN	PUNTAJE MAXIMO	PUNTAJE MINIMO	GDATA	PANDA	BITDEFENDER
1	Capacitación	Se dispone con cursos estándares con evaluación y certificación técnica emitida por el fabricante o representante oficial único en el país	4	0	4	4	4
	Seguridad	La solución no debe estar observada ni investigada en temas de posible filtración de información de cliente o incorporación de backdoors en sus sistemas	5	0	5	5	5
3	Satisfacción	El usuario interactúa con familiaridad con el producto	5	0	5	0	0
SUBTOTAL					14	9	9
TOTAL					98	67	71

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

6.5. Análisis Comparativo Técnico/Funcional

ATRIBUTOS/CARACTERISTICAS	GDATA	PANDA	BITDEFENDER
Brindar una consola de administración remota para los diferentes escenarios de gestión de estaciones de trabajo y servidores (OnPremise y nube)	SI	SI	SI



Contar con diversas estrategias para la gestión, sincronización y actualización de firmas para estaciones de trabajo, laptops, servidores y móviles.	SI	SI	SI
Cubrir la protección de las diferentes plataformas utilizadas en la institución Windows, Linux, Mac, iOS, Android, VMWare y Hyper-V.	SI	SI	SI
Incluir funcionalidades que permitan implementar estrategias de prevención de ejecución de software malicioso como control de aplicaciones, control de dispositivos, control de navegación web basada en categorías y similares.	SI	SI	SI
Incluir funcionalidades que permitan implementar estrategias de mitigación de software malicioso como sistemas de análisis de vulnerabilidades, gestión de parches, firewalls, analizadores de red que respondan al comportamiento anómalo.	SI	SI	SI
Incluir funcionalidades que permitan implementar estrategias de detección avanzada para la detección de malware conocido y desconocido, las tecnologías incluidas deben ser capaces de analizar la totalidad de programas ejecutándose en la red evidenciando que estos comprometidos con algún malware, sistemas de detección basados en inteligencia artificial y sistemas de autoaprendizaje (Machine Learning).	SI	SI	SI
Incluir funcionalidades que permitan implementar estrategias de recuperación ante ataques de malware, desinfectando programas, ejecutables y/o carpetas completas además de poder cifrar y respaldar información y/o archivos críticos para la operatividad del sistema o trabajo diario.	SI	SI	SI
Contar con sistema de informes centralizados que permitan automatizar la publicación y envío del performance de la herramienta al personal técnico responsable.	SI	SI	SI
Compatibilidad comprobada con aplicaciones propias del estado peruano (SIAF, SIGA, SPIJ, etc.)	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.

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
GDATA ENDPOINT PROTECTION BUSINESS	520,000.00	3
PANDA FUSION 360	550,000.00	2
BITDEFENDER GRAVITYZONE ULTRA PLUS	630,592.00	1



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 GDATA, por lo que se recomienda su adquisición no obstante las soluciones seleccionadas con PANDA y BITDEFENDER también podrían participar del proceso de selección.

9. FIRMAS

Nombre	Cargo	Firma
Lic. Edwin Dante Quispe Soto	Director de la Dirección del Sistema Nacional de Información de Recursos Hídricos.	
Tec. Pablo Demetrio Carrión Méndez	Coordinador de Soporte Técnico	

10. ANEXOS

- ✓ Cotización de PANDA
- ✓ Cotización GDATA.
- ✓ Cotización BITDEFENDER