

	<b>LEY 28612</b> LEY QUE NORMA EL USO, ADQUISICION Y ADECUACION DEL SOFTWARE EN LA ADMINISTRACION PUBLICA	Fecha: 13/05/2021
	<b>INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE</b>	Página 1 de 5

## **INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE N°065-2021-GIN/SAT**

### **1. NOMBRE DEL ÁREA:**

Gerencia de Informática

### **2. RESPONSABLES DE LA EVALUACIÓN:**

Juan Martin Camino Leon

### **3. CARGO / ROL:**

Especialista de Seguridad informática II

### **4. FECHA DE APROBACION**

13 de mayo del 2021

### **5. JUSTIFICACIÓN**

Como parte de los controles recomendados por la NTP ISO / IEC 27001:2014 Anexo A (A.12.6.1 Gestión de vulnerabilidades técnicas), en el SAT se desarrollan actividades de identificación, evaluación y corrección de las vulnerabilidades técnicas existentes sobre los activos TI.

Para ello se cuenta con herramientas que permiten automatizar este proceso con el fin de que resulte preventivo y se realice de forma permanente, evitando así que se materialicen riesgos que afecten la seguridad de la información en el SAT. Entre las herramientas que se vienen utilizando desde el año 2013 en el SAT tenemos el scanner de vulnerabilidades Nessus Professional y la plataforma de gestión de vulnerabilidades Tenable.IO Vulnerability Management (Cloud).

Actualmente existe la necesidad de ampliar la cobertura de activos de red sobre los cuales se realiza el análisis de vulnerabilidades, por esta razón se requiere implementar e integrar con las herramientas ya existentes en el SAT, una herramienta de análisis de vulnerabilidades de activos de red que permita cubrir la brecha que se ha identificado en cuanto a cantidad de activos monitorizados.

El presente informe se elabora en cumplimiento de la Ley N° 28612 Ley que norma el Uso, Adquisición y Adecuación del software en la Administración Pública, dejándose constancia que la adquisición en cuestión responde a los principios de vigencia y neutralidad tecnológica, transparencia y eficiencia, y a los criterios de austeridad y ahorro de los recursos públicos mencionados en dicha Ley.

### **6. ALTERNATIVAS**

Considerando los requerimientos del SAT, se han tomado en cuenta las herramientas de software con mayor presencia en el mercado, que puedan cumplir con dichos requerimientos. Las alternativas que se sometieron a evaluación fueron las siguientes:

	<b>LEY 28612</b> LEY QUE NORMA EL USO, ADQUISICION Y ADECUACION DEL SOFTWARE EN LA ADMINISTRACION PUBLICA	Fecha: 13/05/2021
	<b>INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE</b>	Página 2 de 5

- a. Rapid 7 Insight Vulnerability Managent
- b. Qualys Vulnerability Management
- c. Tenable.IO Vulnerability Management

Para el análisis de la información se han recurrido a las siguientes fuentes:

- a. A través de la información disponible en la página web de los fabricantes:
- b. Información disponible en Internet.

Cabe precisar que el requerimiento se genera sobre la necesidad de renovar y ampliar la cobertura del análisis de vulnerabilidades que se realiza sobre activos de red y que esta herramienta se debe complementar e integrar con la herramienta de análisis de vulnerabilidades de activos TI y análisis de vulnerabilidades de Aplicaciones Web con que actualmente cuenta el SAT de manera que se pueda tener una visión y gestión centralizada e integral de las vulnerabilidades existentes.

## 7. ANALISIS COMPARATIVO TÉCNICO

El análisis técnico se ha realizado en conformidad con la metodología establecida en la “Guía Técnica de Evaluación de Software” aprobada por Resolución Ministerial N° 139-2004-PCM:

### a. Propósito de la Evaluación:

- Determinar los atributos o características mínimas más convenientes para asegurar que las alternativas evaluadas se ajustan a las necesidades y requerimientos del SAT.

### b. Identificar el tipo de producto

- Software para el análisis de vulnerabilidades de activos de red


### c. Especificaciones del modelo de calidad

Se aplicara el modelo de Calidad de Software Descrito en la parte I de la Guía de Evaluación de software aprobado por Resolución Ministerial N° 139-2004-PCM.

### d. Selección de Métricas

Las métricas fueron seleccionadas en base al análisis de los requerimientos del área de TI y a la información técnica de los productos de software señalados en el punto 6 Alternativas.

Del análisis realizado, se han determinado las siguientes características técnicas mínimas y sus respectivas métricas.


	<b>LEY 28612</b> LEY QUE NORMA EL USO, ADQUISICION Y ADECUACION DEL SOFTWARE EN LA ADMINISTRACION PUBLICA	Fecha: 13/05/2021
	<b>INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE</b>	Página 3 de 5

Atributos Internos y externos			
Item	Características	Descripcion	Puntaje
1	Adecuacion	Facilita la generacion de informes de vulnerabilidad estandar y de cumplimiento y provee una vista unificada	7
2	Integracion	Se integra y complementa con la plataforma de gestion de vulnerabilidades existente	7
3	Funcionalidad	Capacidad para el descubrimiento de activos	5
4		Capacidad y cobertura para la deteccion de vulnerabilidades	5
5		Deteccion de malware	5
6		Analisis de vulnerabilidades a traves de MDM	4
7		Plantillas y politicas preconfiguradas y personalizables listas para realizar escaneos	5
8		Automatizacion de tareas, permite definir parámetros de frecuencia y horario	4
9		Escaneo activo que se integra y/o complementa con servicios de escaneo pasivo	5
10		Configuracion y despliegue de agentes para escaneo y monitoreo	5
11		Escaneo por direcciones IP y nombres DNS	4
12		Integracion con soluciones de administración de parches, administración de credenciales y administración de dispositivos móviles.	4
13		Manejo de pruebas avanzadas	5
14		Conexiones concurrentes	4
15	Portabilidad	Facilidad para la instalacion, despliegue y configuracion	5
16		Actualizaciones automaticas	3
17	Fiabilidad	Proporciona disponibilidad y escalabilidad	3
18		Soporta estandares	3
19	Usabilidad	Facilidad de uso a traves una interfaz simple e intuitiva	5
20		Generacion de reportes , analisis y metricas	3
21		Licenciamiento basado en activo y no en direcciones IP	3
22	Seguridad	Acceso basado en roles	3
23		Cumplimiento de estandares de seguridad	3

Luego de determinar las características técnicas mínimas y las métricas aplicables, se procedió al análisis comparativo técnico, para lo cual se aplicó el modelo de calidad de software descrito en la Parte I Guía Evaluación de Software por Resolución Ministerial N° 139-2004 PCM.

Un aspecto importante que se ha tomado en cuenta al momento de la evaluación, es la integración con la plataforma de gestión de vulnerabilidades y gestión de vulnerabilidades de aplicaciones web que actualmente se encuentra en uso y con periodo de suscripción vigente en el SAT.

Se tomaran en consideración para la evaluación costo – beneficio, aquellas alternativas que obtengan un puntaje igual o superior a 85 en el análisis comparativo técnico:

	<b>LEY 28612</b> LEY QUE NORMA EL USO, ADQUISICION Y ADECUACION DEL SOFTWARE EN LA ADMINISTRACION PUBLICA	Fecha: 13/05/2021
	<b>INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE</b>	Página 4 de 5

ITEM	CARACTERISTICAS	Rapid 7 Insight VM	Tenable IO VM	Qualys VM
1	Facilita la generacion de informes de vulnerabilidad estandar y de cumplimiento y provee una vista unificada	4	6	5
2	Se integra y complementa con la plataforma de gestion de vulnerabilidades existente	4	7	4
3	Capacidad para el descubrimiento de activos	5	5	4
4	Capacidad y cobertura para la deteccion de vulnerabilidades	4	5	5
5	Deteccion de malware	3	4	3
6	Analisis de vulnerabilidades a traves de MDM	2	4	1
7	Plantillas y politicas preconfiguradas y personalizables listas para realizar escaneos	3	5	4
8	Automatizacion de tareas, permite definir parámetros de frecuencia y horario	4	4	3
9	Escaneo activo que se integra y/o complementa con servicios de escaneo pasivo	4	5	3
10	Configuracion y despliegue de agentes para escaneo y monitoreo	3	4	3
11	Escaneo por direcciones IP y nombres DNS	4	4	3
12	Integracion con soluciones de administración de parches, administración de credenciales y administración de dispositivos móviles.	3	3	3
13	Manejo de pruebas avanzadas	4	3	3
14	Conexiones concurrentes	4	3	4
15	Facilidad para la instalacion, despliegue y configuracion	3	4	4
16	Actualizaciones automaticas	2	3	3
17	Proporciona disponibilidad y escalabilidad	2	3	3
18	Soporta estandares	3	3	3
19	Facilidad de uso a traves una interfaz simple e intuitiva	3	5	4
20	Generacion de reportes , analisis y metricas	1	3	2
21	Licenciamiento basado en activo y no en direcciones IP	2	3	2
22	Acceso basado en roles	3	3	3
23	Cumplimiento de estandares de seguridad	3	3	3
<b>PUNTAJES TOTALES</b>		<b>73</b>	<b>92</b>	<b>75</b>


## 8. ANALISIS COSTO - BENEFICIO

### Costos

Se requiere la suscripción de software para el análisis de vulnerabilidades de activos de red por un periodo de 12 meses, además de capacitación y entrenamiento en el uso de la herramienta y el despliegue de la misma de modo tal que permitan obtener un mejor aprovechamiento de su uso.

No se ha realizado un análisis comparativo de costos, debido a que lo que se pretende es determinar técnicamente la herramienta más adecuada para atender los requerimientos de la institución. En ese sentido solo una alternativa (Tenable.IO Vulnerability Management) ha logrado alcanzar el puntaje mínimo establecido (85).

Las herramientas evaluadas no requieren de adquisición de hardware adicional para su explotación en el SAT.

	<b>LEY 28612</b> LEY QUE NORMA EL USO, ADQUISICION Y ADECUACION DEL SOFTWARE EN LA ADMINISTRACION PUBLICA	Fecha: 13/05/2021
	<b>INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE</b>	Página 5 de 5

### **Beneficio**

La suscripción del software para el análisis de vulnerabilidades de activos de red, permitirá incorporar al proceso de gestión de vulnerabilidades una mayor cantidad de activos identificados como críticos. El despliegue previsto permitirá maximizar la cobertura, automatizar las tareas de identificación y análisis de vulnerabilidades y por consecuencia, los tiempos de corrección y respuesta a las mismas, lo cual permitirá mitigar los riesgos asociados con ataques, explotación y uso indebido o no autorizado de los activos de TI.

## **9. CONCLUSIONES**

A partir de los resultados del análisis comparativo técnico desarrollado, se concluye que el software Tenable.IO Vulnerability Management, es el producto que mejor se ajusta a las necesidades de la entidad.

## **10. FIRMAS**

-----  
**Juan Martin Camino Leon**  
**Especialista de Seguridad informática II**  
**SERVICIO DE ADMINISTRACION TRIBUTARIA DE LIMA**