INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE N°070-2024-GIN/SAT

SUSCRIPCION DE SOFTWARE PARA ANÁLISIS DE VULNERABILIDADES SOBRE ACTIVOS DE RED Y APLICACIONES WEB

1. NOMBRE DEL ÁREA:

Gerencia de Informática

2. RESPONSABLES DE LA EVALUACIÓN:

a. Juan Martin Camino Leon
b. Sandro Iván Rodriguez Romero

3. CARGO / ROL:

a. Especialista de Seguridad informática II / Oficial de Seguridad y Confianza Digital
b. Gerente de Informática

4. FECHA DE APROBACION

20 de marzo del 2024

5. JUSTIFICACIÓN

En aplicación de los controles recomendados por la NTP ISO / IEC 27001:2022 Anexo A (A.8. Gestión de vulnerabilidades técnicas), la Gerencia de Informática del SAT desarrolla actividades de detección, identificación, evaluación, análisis y corrección de las vulnerabilidades técnicas existentes sobre los sistemas y aplicaciones informáticas de la entidad.

Para cumplir de manera eficiente con las actividades mencionadas en el párrafo anterior, la Gerencia de Informática del SAT requiere contar con una herramienta de software que le permita automatizar las actividades de detección, identificación y clasificación de vulnerabilidades sobre activos TI, y de otra herramienta específicamente orientada para el análisis de aplicaciones Web. Se requiere, además, que ambas herramientas se encuentren integradas en una plataforma de gestión de vulnerabilidades cloud de un único fabricante y su uso se licencie bajo la modalidad de suscripción. Mediante el uso de estas herramientas, se busca que el proceso de Gestión de Vulnerabilidades resulte preventivo, oportuno y se realice de forma permanente, de manera que se minimicen los riesgos para la seguridad de la información en el SAT.

La Ley N° 28612, "Ley que norma el Uso, Adquisición y Adecuación del software en la Administración Pública", tiene por objeto establecer las medidas que permitan a la administración pública la contratación de licencias de software y servicios informáticos en condiciones de neutralidad, vigencia tecnológica, libre concurrencia, y trato justo e igualitario de proveedores.

El presente informe se elabora en cumplimiento del artículo 6 de la Ley N° 28612, el cual indica que el uso o adquisición de licencias de software en la administración pública requiere del Informe Previo de Evaluación del área de Informática de la entidad, el cual determine el tipo de licencias que resulte más conveniente para atender los requerimientos formulados.

6. ALTERNATIVAS

Se ha realizado una búsqueda de software que pueda cumplir con los requerimientos técnicos de la Gerencia de informática del SAT. Para elegir las alternativas que serán evaluadas, se ha tomado en consideración productos con funcionalidades similares, que cuenten con mayor presencia en el mercado, y que tengan una buena calificación y reconocimiento de la industria de TI.

Las alternativas que se sometieron a evaluación fueron las siguientes:

a. Software para análisis de vulnerabilidades sobre activos de red:

- Rapid 7 Insight Vulnerability Managent
- Qualys Vulnerability Management
- Tenable.IO Vulnerability Management

b. Software para análisis de vulnerabilidades sobre aplicaciones web:

- Rapid 7 Insight AppSec
- Tenable Web App Scanning
- Qualys Web Application Scanning

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.

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 y de aplicaciones WEB

c. **Especificaciones del modelo de calidad**

Se aplicará 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 de la Gerencia de Informática del SAT y a la información técnica de los productos de software señalados en el punto 6 Alternativas.

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

A partir de los puntajes obtenidos en la evaluación, se aplicará la siguiente **tabla de aceptación de alternativas:**

Rango de Puntaje	Descripción
[85-100>	Recomendable. Cumple totalmente con los requerimientos y expectativas
[50-84>	Riesgoso. Cumple parcialmente con los requerimientos, pero no se garantiza su adaptación a las necesidades
[0-49>	No recomendable. Software no cumple con los requerimientos y expectativas.

CUADRO N°01 – METRICAS
SOFTWARE PARA ANALISIS DE VULNERABILIDADES SOBRE ACTIVOS DE RED

Atributos Internos, externos y de uso			
Ítem	**Características**	**Descripción**	**Puntaje**
1	FUNCIONALIDAD	Consola de administración web, para la gestión centralizada de usuarios, roles, perfiles y grupos de activos o aplicaciones.	4
2		El acceso a la consola de administración es mediante interface web segura	4
3		Descubrimiento de vulnerabilidades con y sin credenciales	4
4		Permite escanear redes híbridas IPV4/IPv6	4
5		Permite identificar y priorizar las vulnerabilidades de acuerdo con su impacto o riesgo.	4
6		Capacidad de realizar escaneo de vulnerabilidades, auditoria de configuraciones y reportes.	4
7		Capacidad de descubrir activos en la red y en ambientes virtualizados.	4
8		Capacidad de descubrir vulnerabilidades en bases de datos	4
9		Debe clasificar las vulnerabilidades por CVE / CVSS e identificar los últimos parches y recomendaciones para su remediación.	4
10		El software debe ser compatible con navegadores de internet: Chrome, Firefox, Internet Explorer, entre otros.	4
11		Evaluación de configuración segura	4
12		Generar informes / reportes personalizados	4
13		Soporte de evaluación de hipervisores y nube	4
14	FIABILIDAD	Informes, análisis y métricas confiables	4
15	USABILIDAD	Facilidad de administración y operación a través una interfaz simple e intuitiva	4
16		Facilidad de integración utilizando API y herramientas estándar	4
17		Personalización	4
18	EFICIENCIA	Licenciamiento basado en activos	4
19		Despliegue/instalación y uso combinado de escáneres y/o agentes y/o sensores y/o conectores, sin que representen costo adicional.	4
20	CAPACIDAD DE MANTENIMIENTO	Calidad de la comunidad de usuarios	4
21		Calidad del soporte técnico	4
22	PORTABILIDAD	Facilidad de instalación y despliegue	4
23		Escalabilidad	4
24	EFICACIA	Métodos de evaluación	4
25		Calidad y cobertura de la firma	4
			100

CUADRO N°02 – METRICAS
SOFTWARE PARA ANALISIS DE VULNERABILIDADES SOBRE APLICACIONES WEB

Atributos Internos, externos y de uso			
Ítem	**Características**	**Descripción**	**Puntaje**
1	FUNCIONALIDAD	Programar y ejecutar las actividades de escaneo/análisis de manera centralizada desde la interfaz web de la plataforma de gestión de vulnerabilidades cloud del fabricante, del mismo modo la visualización de los resultados y los reportes deben centralizarse en la misma plataforma.	4
2		Debe realizar escaneo de aplicaciones web HTML tradicionales y web creadas con HTML 5 y AJAX.	4
3		Solución dinámica de prueba de seguridad de aplicaciones (DAST)	4
4		Detecta existencia de certificados SSL / TLS por caducar o emitidos incorrectamente	4
5		Permite un escaneo externo seguro para evitar que aplicaciones en produccion no se vean interrumpidas o demoradas a causa del escaneo	4
6		Permite excluir partes de la aplicación web que se analizara	4
7		Escanea desde los 10 principales riesgos de OWASP hasta los componentes vulnerables de las aplicaciones web en una única plataforma.	4
8		Detecta configuraciones incorrectas en el servidor web.	4
9		Capacidad de escaneo con y sin autenticación.	4
10		Permite la identificación de servicios corriendo en puertos que no son estándar	4
11		Clasificar por nivel de riesgo de las vulnerabilidades, en base a la explotabilidad y de acuerdo a CVSS (Common VulnerabilityScoring System).	4
12		Plantillas de escaneo y permitir generar nuevas plantillas en base a las que vienen por defecto.	4
13		Permite generar reportes de cumplimiento	4
14	FIABILIDAD	Informes, análisis y métricas confiables	4
15		Certificaciones	
16	USABILIDAD	Facilidad de administración y operación a través una interfaz simple e intuitiva	4
17		Facilidad de integración utilizando API y herramientas estándar	4
18		Automatización y recuperación	4
19	EFICIENCIA	Escaneo de seguridad de contenedores	4
20		Fuzzing	4
21	CAPACIDAD DE MANTENIMIENTO	Calidad de la comunidad de usuarios	4
22		Calidad del soporte técnico	4
23	PORTABILIDAD	Facilidad de instalación y despliegue	4
24	EFICACIA	Análisis de composición de software	4
25		API Security Testing	4
			100

A continuación, se procede con la evaluación de cada alternativa de software, considerando las características técnicas mínimas y las métricas definidas.

El puntaje resultante de la evaluación de cada alternativa de software se comparará con los rangos definidos en la tabla de aceptación de alternativas.

Para continuar con el proceso de evaluación, se tomarán en consideración solo aquellas alternativas que obtengan un puntaje igual o superior a 85 en el análisis comparativo técnico. Las alternativas con puntajes menores a 85 se considera que no cumplen con las necesidades y requisitos o los cumplen de manera parcial por lo que resultaría riesgosa su implementación.

CUADRO N°03 – EVALUACION
SOFTWARE PARA ANALISIS DE VULNERABILIDADES SOBRE ACTIVOS DE RED

ITEM	CARACTERISTICAS	SOFTWARE		
		Rapid 7 Insight Vulnerability Managent	Qualys Vulnerability Management	Tenable.IO Vulnerability Management
1	Cuenta con consola de administración web, para la gestión centralizada de usuarios, roles, perfiles y grupos de activos o aplicaciones.	3	4	4
2	El acceso a la consola de administración es mediante interface web segura	3	4	4
3	Descubrimiento de vulnerabilidades con y sin credenciales	4	4	4
4	Permite escanear redes hibridas IPV4/IPv6	4	4	4
5	Permite identificar y priorizar las vulnerabilidades de acuerdo con su impacto o riesgo.	4	4	3
6	Capacidad de realizar escaneo de vulnerabilidades, auditoria de configuraciones y reportes.	3	4	4
7	Capacidad de descubrir activos en la red y en ambientes virtualizados.	4	4	4
8	Capacidad de descubrir vulnerabilidades en bases de datos	4	4	4
9	Clasifica las vulnerabilidades por CVE / CVSS e identifica los últimos parches y recomendaciones para su remediación.	3	4	4
10	El software debe ser compatible con navegadores de internet: Chrome, Firefox, Internet Explorer, entre otros.	4	4	4
11	Evaluación de configuración segura	3	3	4
12	Generar informes / reportes personalizados	4	4	4
13	Soporte de evaluación de hipervisores y nube	3	3	4
14	Informes, análisis y métricas confiables	3	3	4
15	Facilidad de administración y operación a través una interfaz simple e intuitiva	3	4	3
16	Facilidad de integración utilizando API y herramientas estándar	2	3	4
17	Personalización	2	4	3
18	Licenciamiento basado en activos	4	4	4
19	Despliegue/instalación y uso combinado de escáneres y/o agentes y/o sensores y/o conectores, sin que representen costo adicional.	4	4	4
20	Calidad de la comunidad de usuarios	3	4	4
21	Calidad del soporte técnico	3	3	4
22	Facilidad de instalación y despliegue	3	3	4
23	Escalabilidad	4	4	4
24	Métodos de evaluación	3	3	4
25	Calidad y cobertura de la firma	3	3	4
	PUNTAJES TOTALES	**83**	**92**	**97**

Resultados:

SOFTWARE	PUNTAJE	EVALUACION
Rapid 7 Insight Vulnerability Managent	**83**	Riesgoso.
Qualys Vulnerability Management	**92**	Recomendable.
Tenable.IO Vulnerability Management	**97**	Recomendable.

CUADRO N°04 – EVALUACION
SOFTWARE PARA ANALISIS DE VULNERABILIDADES SOBRE APLICACIONES WEB

ITEM	CARACTERISTICAS	SOFTWARE		
		Rapid 7 Insight AppSec	Qualys Web Application Scanning	Tenable Web App Scanning
1	Programar y ejecutar las actividades de escaneo/análisis de manera centralizada desde la interfaz web de la plataforma de gestión de vulnerabilidades cloud del fabricante, del mismo modo la visualización de los resultados y los reportes deben centralizarse en la misma plataforma.	3	4	4
2	Debe realizar escaneo de aplicaciones web HTML tradicionales y web creadas con HTML 5 y AJAX.	4	4	4
3	Solución dinámica de prueba de seguridad de aplicaciones (DAST)	4	3	2
4	Detecta existencia de certificados SSL / TLS por caducar o emitidos incorrectamente	4	3	4
5	Permite un escaneo externo seguro para evitar que aplicaciones en produccion no se vean interrumpidas o demoradas a causa del escaneo	3	4	4
6	Permite excluir partes de la aplicación web que se analizara	4	4	4
7	Escanea desde los 10 principales riesgos de OWASP hasta los componentes vulnerables de las aplicaciones web en una única plataforma.	4	4	4
8	Detecta configuraciones incorrectas en el servidor web.	3	4	3
9	Capacidad de escaneo con y sin autenticación.	4	4	4
10	Permite la identificación de servicios corriendo en puertos que no son estándar	4	4	4
11	Clasificar por nivel de riesgo de las vulnerabilidades, en base a la explotabilidad y de acuerdo a CVSS (Common VulnerabilityScoring System).	4	4	4
12	Plantillas de escaneo y permitir generar nuevas plantillas en base a las que vienen por defecto.	3	3	4
13	Permite generar reportes de cumplimiento	4	4	4
14	Informes, análisis y métricas confiables	3	4	4
15	Certificaciones	4	4	4
16	Facilidad de administración y operación a través una interfaz simple e intuitiva	3	4	4
17	Facilidad de integración utilizando API y herramientas estándar	4	3	4
18	Automatización y recuperación	2	3	4
19	Escaneo de seguridad de contenedores	2	2	4
20	Fuzzing	2	3	4
21	Calidad de la comunidad de usuarios	3	3	4
22	Calidad del soporte técnico	3	3	4
23	Facilidad de instalación y despliegue	3	4	4
24	Análisis de composición de software	3	3	4
25	API Security Testing	3	4	3
	PUNTAJES TOTALES	**83**	**89**	**96**

Resultados:

SOFTWARE	PUNTAJE	EVALUACION
Rapid 7 Insight AppSec	**83**	Riesgoso.
Qualys Web Application Scanning	**89**	Recomendable.
Tenable Web App Scanning	**96**	Recomendable.

SAT Servicio de Administración Tributaria de Lima
Sandro Rodriguez Romero
Gerencia de Informática

8. ANALISIS COSTO - BENEFICIO

Costos

Se requiere la suscripción de software para el análisis de vulnerabilidades sobre activos de red y sobre aplicaciones Web por el periodo de 12 meses, además de capacitación y entrenamiento en el uso de la herramienta y el despliegue de la misma en las instalaciones de la entidad.

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 entidad. En ese sentido solo se toman en consideración las alternativas que han logrado alcanzar el puntaje mínimo aceptable (85).

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

Beneficio

Mediante la suscripción del software el uso de estas herramientas, se busca ampliar la cobertura de análisis y que el proceso de Gestión de Vulnerabilidades resulte preventivo, oportuno y se realice de forma permanente, de manera que se minimicen los riesgos para la seguridad de la información en el SAT.

9. CONCLUSIONES

A partir de los resultados del análisis comparativo técnico desarrollado, se concluye que las alternativas de software recomendadas para atender las necesidades y requerimientos d ela entidad son las siguientes:

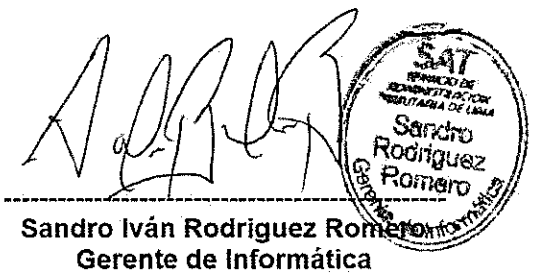
a. Software para análisis de vulnerabilidades sobre activos de red:

- Qualys Vulnerability Management
- Tenable.IO Vulnerability Management

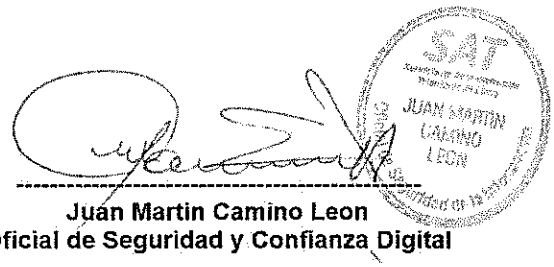
b. Software para análisis de vulnerabilidades sobre aplicaciones web:

- Qualys Web Application Scanning
- Tenable Web App Scanning

10. FIRMAS



Sandro Iván Rodriguez Romero
Gerente de Informática



Juan Martin Camino Leon
Oficial de Seguridad y Confianza Digital