"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año de la Lucha Contra la Corrupción y la Impunidad"

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE Nº 001-2019-MINEDU/SPE-OTIC

SUSTENTO TÉCNICO PARA LA SUSCRIPCIÓN DE UN SOFTWARE DE GESTIÓN DE VULNERABILIDADES DE SERVIDORES FÍSICOS Y EQUIPOS DE RED DEL MINISTERIO DE EDUCACIÓN

1. NOMBRE DEL AREA

Oficina de Tecnologías de la Información y Comunicación.

2. RESPONSABLES DE LA EVALUACIÓN

Ing. Luis Gastulo Salazar.
Ing. Jorge Enrique Abad Jesús.

3. CARGOS

Coordinador de Seguridad de la Información UCSI – OTIC.
Especialista de Seguridad de la Información UCSI – OTIC.

4. FECHA

Enero 2019.

5. JUSTIFICACIÓN

La Unidad de Calidad y Seguridad de la Información – UCSI de la Oficina de Tecnologías de la Información y Comunicación – OTIC del Ministerio de Educación (MINEDU), requiere la suscripción de una herramienta (software) que permita detectar y gestionar vulnerabilidades técnicas de los servidores físicos y equipos de red de la infraestructura tecnológica del MINEDU, con la finalidad de detectar y reducir las vulnerabilidades técnicas y sus riesgo asociados.

Por lo expuesto y en el marco de la Ley 28612 "Ley que norma el uso, adquisición y adecuación del software en la Administración Pública", se procede a evaluar el Software de Gestión de Vulnerabilidades de servidores físicos y equipos de red del MINEDU.

6. ALTERNATIVAS

Considerando el requerimiento de la Unidad de Calidad y Seguridad de la Información – UCSI, se han buscado alternativas de software en el mercado, tomando en consideración la disponibilidad en el servicio de atención y de soporte local.

En ese sentido, la búsqueda ha dado como resultado los productos que se listan a continuación:

- Tenable IO Vulnerability Management.
- Qualys Guard Vulnerability Management.

Cabe mencionar que los productos mencionados, son productos de tipo propietario.

7. ANÁLISIS 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" (R.M. N° 139-2004-PCM) tal como se exige en el reglamento de la Ley N° 28612.

a. Propósito de evaluación
Validar que las alternativas seleccionadas sean las más convenientes técnicamente para el uso de la Unidad de Calidad y Seguridad de la Información de la OTIC del Ministerio de Educación.

b. Identificar el tipo de producto
Software de Gestión de Vulnerabilidades de Servidores Físicos y Equipos de Red del MINEDU.

c. Identificación del modelo de calidad
Se aplicará el modelo de calidad de software descrito en la parte 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 a las características técnicas descritas en el Anexo N° 01; en ella se han evaluado atributos internos, externos y de uso.

8. ANÁLISIS COMPARATIVO DE COSTO - BENEFICIO

El presente análisis tiene por objetivo seleccionar la mejor alternativa, en ese sentido, se ha decidido dar una valoración de 0.7 a la evaluación técnica y de 0.3 a la evaluación económica, con el fin de garantizar que el Software de Gestión de Vulnerabilidades de Servidores Físicos y Equipos de Red del MINEDU a suscribir, cumpla con los requerimientos técnicos solicitados.

La evaluación de estas alternativas incluyen los costos de licencias por suscripción anual y mantenimiento y/o actualizaciones de la versión del software, de los cuales el costo referencial de uno de los productos evaluados ha sido tomado desde la página web del fabricante de software.

Ver Anexo N° 03: Costos Referenciales de Licencias de Software

En el Anexo N° 02, se muestran los resultados del Análisis Comparativo de Costo – Beneficio, así como el cuadro de valoración técnica – económica.

Asimismo, en la presente evaluación se ha considerado lo siguiente:

- ***Hardware necesario para su funcionamiento de las alternativas:***
  La Unidad de Calidad y Seguridad de la Información – UCSI, cuenta con computadoras personales de escritorio, por lo que no es necesario la adquisición del hardware para el funcionamiento de los productos en mención.
- ***Soporte y mantenimiento externo***
  Con la suscripción de las licencias del Software de Gestión de Vulnerabilidades de Servidores Físicos y Equipos de Red del MINEDU, se tienen derechos de soporte, actualizaciones de los parches y actualizaciones a versiones últimas liberadas por el fabricante durante el periodo de la garantía de los productos en mención.
- ***Personal y mantenimiento interno***
  El Ministerio de Educación cuenta con soporte de Mesa de Ayuda a cargo de la Oficina de Tecnologías de la Información y Comunicación – OTIC, para realizar la instalación y configuración del software en los en los equipos informáticos

designados en coordinación con el proveedor, así como para atender incidentes que pueda ocasionar el producto durante su funcionamiento.

- ***Capacitación***
  El personal de la Unidad de Calidad y Seguridad de la Información – UCSI quienes utilizarán los productos evaluados, tiene conocimiento en el uso y manejo de los productos en mención, por lo que no es necesario considerar la capacitación.

9. CONCLUSIÓN

De los resultados del análisis realizado, se puede verificar que el producto Tenable IO Vulnerability Management, es la que alcanza el mayor puntaje, es decir es la que mejor se adecua a las necesidades del área usuaria como Software de Gestión de Vulnerabilidades de Servidores Físicos y Equipos de red del MINEDU.

10. RECOMENDACIONES

Se recomienda la adquisición del producto que obtuvo mayor puntaje en el Análisis de Costo – Beneficio, debido a que sus características técnicas de dicho producto satisfacen la necesidad del área usuaria.

11. FIRMAS

FIRMA DIGITAL
Firmado digitalmente por: ABAD JESUS Jorge Enrique FAU 20131370998 soft
Motivo: Soy el autor del documento
Fecha: 16/01/2019 18:54:46-0500

FIRMA DIGITAL
Firmado digitalmente por: PAJUELO HUAMAN Alberto Carlos FAU 20131370998 hard
Motivo: Soy el autor del documento
Fecha: 27/03/2019 15:52:01-0500

FIRMA DIGITAL
Firmado digitalmente por: GASTULO SALAZAR Luis Miguel FAU 20131370998 soft
Motivo: Soy el autor del documento
Fecha: 17/01/2019 09:58:43-0500

FIRMA DIGITAL
Firmado digitalmente por: LUCIANO ESPINOZA Veronica Silveria FAU 20131370998 hard
Motivo: En señal de conformidad
Fecha: 17/01/2019 14:29:43-0500

ANEXO N° 01

METRICAS (ATRIBUTOS) INTERNAS Y EXTERNAS								
Nº	**Atributo**	**Descripción**	**Puntaje Máximo**	**Puntaje Mínimo**	**Criterio de calificación**	**Puntaje**	**Tenable IO Vulnerability Management**	**Qualys Guard Vulnerability Management**
1	Funcionalidad	El software debe funcionar en un entorno de la nube y debe permitir la suscripción del servicio de gestión de vulnerabilidades como mínimo para 150 Activos o Target.	5	3	Total	5	5	5
					Parcial	3		
					Ninguno	0		
		El software debe contar con agentes y escáner de vulnerabilidades para ser instalado en los equipos cliente.	5	3	Total	5	5	5
					Parcial	3		
					Ninguno	0		
		El software debe permitir analizar y detectar automáticamente las amenazas o ataques de seguridad en toda la red de datos, sistemas de información y aplicaciones web de la Entidad.	5	3	Total	5	5	5
					Parcial	3		
					Ninguno	0		
		El software debe permitir identificar las amenazas de red por niveles de gravedad a fin de tener control de las vulnerabilidades que pudieran presentarse en el entorno de la red.	5	3	Total	5	5	5
					Parcial	3		
					Ninguno	0		
		El software debe tener la capacidad de realizar escaneo de vulnerabilidades, auditoria de configuraciones y reportes.	5	3	Total	5	5	5
					Parcial	3		
					Ninguno	0		
		El software debe tener la capacidad de rastrear los activos de la red y sus vulnerabilidades.	5	3	Total	5	5	5
					Parcial	3		
					Ninguno	0		
		El software debe permitir personalizar paneles, examinar detalles de las vulnerabilidades y generar reportes, a fin de monitorear y tomar decisiones para reducir riesgos en la red.	5	3	Total	5	5	5
					Parcial	3		
					Ninguno	0		
		El software debe contar con agentes para servidores y sensores de escaneo de vulnerabilidades para ayudar a maximizar la cobertura del escáner y reducir los puntos débiles de vulnerabilidad.	5	3	Total	5	5	3
					Parcial	3		
					Ninguno	0		
		El software debe permitir el escaneo de aplicaciones web, equipos virtuales, servicios en la nube, contenedores, infraestructura virtual, entre otros.	5	3	Total	5	5	5
					Parcial	3		
					Ninguno	0		
		El software debe permitir visualizar y monitorear de manera instantánea todos los activos de TI de la red.	5	3	Total	5	5	5
					Parcial	3		
					Ninguno	0		
		El software debe tener la capacidad de escaneo de activos, tales como: - Los dispositivos de red: Firewalls / Routers / Switches (Juniper, Check Point, Cisco, Palo Alto	5	3	Total	5	5	5

METRICAS (ATRIBUTOS) INTERNAS Y EXTERNAS								
Nº	**Atributo**	**Descripción**	**Puntaje Máximo**	**Puntaje Mínimo**	**Criterio de calificación**	**Puntaje**	**Tenable IO Vulnerability Management**	**Qualys Guard Vulnerability Management**
		Networks), impresoras y dispositivos de almacenamiento. - Auditoría de configuración sin conexión de dispositivos de red. - Virtualización: VMware ESX, ESXi, vSphere, vCenter. - Sistemas operativos: Windows, Mac, Linux, Solaris, BSD, Cisco IOS, IBM iSeries. - Bases de datos: Oracle, SQL Server, MySQL, DB2, Informix / DRDA, PostgreSQL. - Nube: Desplegado como AWS IAM.			Parcial	3		
					Ninguno	0		
		El software debe tener la capacidad de enumerar iOS, Android y dispositivos que acceden a la red y detecta vulnerabilidades de dispositivos móviles.	5	3	Total	5	5	5
					Parcial	3		
					Ninguno	0		
		El software debe ser compatible con navegadores de internet: Ghrome, Firefox, Internet Explorer, entre otros.	5	3	Total	5	5	5
					Parcial	3		
					Ninguno	0		
2	Fiabilidad	El software debe de tener la capacidad para evaluar y reaccionar ante posibles ataques informaticos sobre los equipos donde se encuentran los agentes instalados mediante la correlación de eventos.	5	3	Si	5	5	5
					No	0		
3	Usabilidad	Permite rastrear los activos y sus vulnerabilidades con mayor precisión.	5	3	Total	5	5	5
					Parcial	3		
		Permite sin costo para el cliente, agentes para servidores y sensores de escaneo de vulnerabilidades para ayudar a maximizar la cobertura del escáner y reducir los puntos débiles de vulnerabilidades.	5	3	Total	5	5	3
					Parcial	3		
4	Capacidad de mantenimiento	Tiene la capacidad de adaptarse a nuevos requerimientos de la organización y fácil actualización de la solución en futuras nuevas versiones.	4	2	Total	4	4	4
					Parcial	2		
					Ninguno	0		
			84	50			84	80
METRICAS (ATRIBUTOS) DE USO								
1	Eficacia	Permite realizar el escaneo de seguridad de forma sólida, administra su seguridad de manera sistemática y hace que se cumplan las normativas continuamente sin necesidad de hacer cambios en la arquitectura, preservar su rendimiento, y la continuidad de las operaciones.	4	2	Total	4	4	4
					Parcial	2		
					Ninguno	0		
2	Productividad		4	2	Total	4	4	4

METRICAS (ATRIBUTOS) INTERNAS Y EXTERNAS								
Nº	**Atributo**	**Descripción**	**Puntaje Máximo**	**Puntaje Mínimo**	**Criterio de calificación**	**Puntaje**	**Tenable IO Vulnerability Management**	**Qualys Guard Vulnerability Management**
		Permite una fácil administración mediante las herramientas intuitivas propias de la solución.			Parcial	2		
					Ninguno	0		
3	Accesibilidad	Permite garantizar la seguridad de la infraestructura tecnológica y aplicaciones web mediante la gestión transparente en la nube con los niveles de seguridad adecuados.	4	2	Total	4	4	4
					Parcial	2		
					Ninguno	0		
4	Satisfacción	Permite la generación de reportes fiables de vulnerabilidades técnicas asociando valores de riesgo que permitan gestionarlos de acuerdo a su criticidad.	4	2	Total	4	4	4
					Parcial	2		
					Ninguno	0		
		Sub Total	16	8			16	16
		Total	100	58			100	96

"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año de la Lucha Contra la Corrupción y la Impunidad"

ANEXO N° 02

COSTOS REFERENCIALES DE SUSCRIPCIÓN DE SOFTWARE DE GESTIÓN DE VULNERABILIDADES DE SERVIDORES FÍSICOS Y EQUIPOS DE RED

Ítem	Software	Costo Total (S/.)*
1	Tenable I.O Vulnerability Management	16,444.51
2	Qualys Guard Vulnerability Management	55,000.00
* Expresados en Nuevos Soles (S/.), incluye el 18% de IGV		
Fecha: 14/01/2019		
Tiempo de suscripción: 12 meses		

ANÁLISIS COSTO - BENEFICIO

Ítem	Software	Costos S/.	Beneficio	Costo / Beneficio
1	Tenable I.O Vulnerability Management	16,444.51	100	100.00%
2	Qualys Guard Vulnerability Management	55,000.00	96	76.17%

"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año de la Lucha Contra la Corrupción y la Impunidad"

ANEXO N° 03

COSTOS REFERENCIALES DE LICENCIAS DE SOFTWARE

a) Software Tenable IO Vulnerability Management

https://store.tenable.com/1479/purl-tenableio?quantity=150, Fecha: 14/01/2019, Hora: 11:00 am.

b) Software Qualys Guard Vulnerability Management

Referencia/Concepto:	SUSCRIPCION DE SOFTWARE PARA ANALISIS DE VULNERABILIDADES			
II. DETALLE DE LA COTIZACION				
ITEM	DESCRIPCION	PRECIO UNITARIO	CANTIDAD	SUB TOTAL
01	Qualys Guard Vulnerability Management. Licencia para 150 activos por 12 meses	55,000.00	01	**55,000.00**
			PRECIO FINAL S/.(INCLUYE IGV)	**55,000.00**
III. CONSIDERACIONES				