INFORME TÉCNICO DE EVALUACIÓN DE SOFTWARE PARA ANÁLISIS DE VULNERABILIDADES DE LOS SERVIDORES DEL MINISTERIO DE TRANSPORTES Y COMUNICACIONES

INFORME TÉCNICO N° 0019-2017-MTC/10.06.LRBS

1 NOMBRE DEL ÁREA

OFICINA DE TECNOLOGÍA DE INFORMACIÓN

2 RESPONSABLE DE LA EVALUACIÓN

PATRICK JAVIER MUÑANTE LOAYZA
LUIS ROBERTO BLAS SERNAQUE

3 CARGO

ADMINISTRADOR DE SEGURIDAD INFORMÁTICA
ESPECIALISTA NORMATIVO Y REGULACIÓN DE TI

4 FECHA

06/06/2017

5 JUSTIFICACIÓN

Durante el mes de mayo del año en curso, se detectaron nuevas amenazas que explotan vulnerabilidades encontradas en los sistemas operativos Windows para secuestrar la información y pedir un pago para su rescate. Además se incrementó el número de ataques de organizaciones delictivas hacia entidades del gobierno provocando la exposición de información confidencial y perdida de servicios.

Actualmente, antes que un servidor entre en producción, se realiza el análisis de vulnerabilidades de los servidores utilizando software libre, implementado por el área de seguridad de la OTI, el cuál no tiene una base de datos de conocimiento amplia para la biblioteca de vulnerabilidades y remediación.

6 ALTERNATIVAS

Considerando la importancia de contar con una plataforma que permita la gestión y remediación de las vulnerabilidades de los servidores, se han determinado las siguientes alternativas.

Ítem	Producto
1	Qualys Vulnerability Management Express Edition
2	Nessus Professional

Para la evaluación técnica, se tiene los siguientes supuestos:

a) Presentaciones de las empresas proveedoras de soluciones de software.
b) La información disponible en la página web de cada uno de los fabricantes.
c) Información disponible en Internet.
d) Evaluaciones similares en otras instituciones del Estado Peruano.

Es importante remarcar que los productos Qualys y Nessus son de tipo propietario.

7 ANÁLISIS COMPARATIVO TÉCNICO

El análisis comparativo técnico está basado en la metodología establecida en la Guía Técnica sobre evaluación de Software para la Administración Pública, aprobada por Resolución Ministerial N° 139-2004-PCM.

7.1 Propósito de la Evaluación

Identificar características de calidad mínima de soluciones para análisis de vulnerabilidad.

7.2 Identificar el tipo de software

Se aplica el modelo establecido en la Guía Técnica sobre Evaluación de Software para la Administración Pública (R.M. N° 139-2004-PCM).

7.3 Especificación del Modelo de Calidad

Se aplicará el modelo de calidad de software descrito en la parte 1 de la Guía de evaluación de software aprobada por R.M N° 139-2004-PCM y la Ley N° 28612 -"Ley que norma el uso, adquisición y adecuación del software en la administración pública".

7.4 Selección de métricas

La selección de métricas se obtuvo a partir de los atributos especificados en el Modelo de Calidad, tal como se detalla en el **Anexo N°1:** "Atributos de evaluación de software".

Para cuantificar cada uno los requisitos o requerimientos se ha asignado un valor de acuerdo al siguiente cuadro:

Detalle	Valor
Cumplimiento de requisito a nivel Alto	5
Cumplimiento de requisito a nivel Medio	4
Cumplimiento de requisito a nivel Bajo	3

Considerando que la suma de los puntajes máximos es 100 para la evaluación de alternativas, se considerará la siguiente tabla de aceptación de alternativas, para la provisión del sistema de seguridad evaluado para el MTC.

Rango de Puntaje	Descripción
[75- 100>	**Altamente Recomendable.** Cumple totalmente con los requerimientos y expectativas.
[50-74>	**Riesgoso** Cumple parcialmente con los requerimientos, pero no se garantiza su adaptación a las necesidades.
[0-49>	**No recomendable.** Software con características inadecuadas.

7.5 Comparativo Técnico/Funcional

El siguiente cuadro describe el resultado de la evaluación por cada alternativa, agrupada desde el punto de vista del modelo de calidad sugerido por la Oficina Nacional de Gobierno Electrónico de la PCM.

Modelo/Característica/Sub Características		Alternativas	
		Qualys	Nessus
Calidad Interna y Externa			
Funcionalidad	Interoperabilidad	20	20
	Seguridad	20	25
	Adecuación	5	4
	Exactitud	5	5
Usabilidad	Entendimiento	3	5
	Operabilidad	8	8
Fiabilidad	Tolerancia a errores	5	5
Capacidad de Mantenimiento	Cambiabilidad	3	5
Portabilidad	Facilidad de instalación	4	5
	Reemplazabilidad	5	5
Calidad de Uso			
Satisfacción		4	5
Seguridad		4	5
Total		**86**	**97**

El detalle de la evaluación por cada funcionalidad se describe en el **Anexo 3.**

8 ANALISIS COMPARATIVO COSTO - BENEFICIO

Costos referenciales de licencias, actualización, soporte y mantenimiento por 1 año.

ID	Software	Licencias	Fabricante	Precio Referencial (S/.)
1	Qualys Vulnerability Management Express Edition	Sí	Qualys	S/. 3500.00
2	Nessus Professional	Sí	Tenable	S/.7665.00

Nota: El costo aproximado es referencial del mercado local y fue obtenida desde ofertas publicadas en Internet. Se precisa que es potestad de la Unidad de Logística, realizar el estudio de mercado, según la normatividad vigente.
Fuente:
http://searchsecurity.techtarget.com/feature/Comparing-the-top-vulnerability-management-tools

9 CONCLUSIONES

La Oficina de Tecnologías de Información, requiere software de análisis de vulnerabilidades para escanear los servidores que están en producción y los que serán puestos en producción a fin de mitigar las falencias de seguridad de los sistemas del MTC.

Uno de los factores a tener en cuenta y que favorece a la alternativa de adquisición del software Nessus, es el valor intangible del nivel de conocimientos (know how) que poseen los usuarios en el manejo del software en mención.

Se recomienda la adquisición de la licencia legalmente emitida, la cual deberá ser solicitada a distribuidores o representantes autorizados de dicho producto.

Se recomienda la provisión de un software análisis de vulnerabilidades, en conformidad al informe de evaluación presentado con el objeto de proteger la información ante las amenazas provenientes de internet con código malicioso, virus, spyware, malware, ransomware, etc.

En base a lo expuesto, Nessus es el software seleccionado para la adquisición de un escáner de vulnerabilidades de los servidores del MTC.

10. FIRMAS

SERVICIOS TI V°B° Seg. Informática OTI - OGA - MTC

Patrick Javier Muñante Loayza
Analista de Seguridad Informática
Oficina de Tecnología de Información

Luis Roberto Blas Sernaque
Especialista normativo y regulación de TI
Oficina de Tecnología de Información

Oficina de Tecnología de Información V°B° IN Y GOB. TI - OGA - MTC

ANEXO 1: ATRIBUTOS DE EVALUACION DE SOFTWARE

1.1 TABLA RESUMEN DE PUNTAJES MÁXIMOS POR CARACTERISTICAS

Características	Puntaje Máximo
	100
Calidad Interna y Externa	**90**
Funcionalidad	55
Usabilidad	15
Fiabilidad	5
Capacidad de mantenimiento	5
Portabilidad	10
Calidad de Uso	**10**
Eficacia	5
Satisfacción	5

SERVICIOS TI V°B° Informática OTI - OGA - MTC

Oficina de Tecnología de Información V°B° IN Y GOB. TI OGA - MTC

1.2 TABLA DETALLADA DE PUNTAJES MÁXIMOS POR CARACTERISTICAS/SUB-CARACTERISTICAS

CALIDAD INTERNA Y EXTERNA PUNTAJE MAXIMO: 90		
Característica	**Sub Característica**	**Puntaje Máximo**
Funcionalidad La capacidad del producto de software para proveer las funciones que satisfacen las necesidades explícitas e implícitas cuando el software se utiliza bajo condiciones Específicas. **Puntaje máximo: 55**	**Interoperabilidad** La capacidad del producto de software de interactuar con uno o más sistemas especificados. La interoperabilidad se utiliza en lugar de compatibilidad para evitar una posible ambigüedad con la reemplazabilidad.	20
	Seguridad La capacidad del producto de software para proteger la información y los datos de modo que las personas o los sistemas o autorizados no puedan leerlos o modificarlos, y a las personas o sistemas autorizados no se les niegue el acceso a ellos. La seguridad en un sentido amplio se define como característica de la calidad en uso, pues no se relaciona con el software solamente, sino con todo un sistema.	25
	Adecuación La capacidad del producto de software para proveer un adecuado conjunto de funciones para las tareas y objetivos especificados por el usuario.	5
	Exactitud La capacidad del producto de software para proveer los resultados o efectos acordados con un grado necesario de precisión.	5
Usabilidad La capacidad del producto de software de ser entendido, aprendido, usado y atractivo al usuario, cuando es utilizado bajo las condiciones especificadas. **Puntaje máximo: 15**	**Entendimiento** La capacidad del producto de software para permitir al usuario entender si el software es adecuado, y cómo puede ser utilizado para las tareas y las condiciones particulares de la aplicación.	5
	Operabilidad	10

SERVICIOS TI - V°B° Sec. Informática - OTI - OGA - MTC

Oficina de Tecnología de Información - V°B° INT GOB. TI - OGA - MTC

	La capacidad del producto de software para permitir al usuario operarlo y controlarlo.	
Fiabilidad La capacidad del producto de software para proveer un desempeño adecuado, de acuerdo a la cantidad de recursos utilizados y bajo las condiciones planteadas. Los recursos pueden incluir otros productos de software, la configuración de hardware y software del sistema, y materiales (Ej: Papel de impresión o diskettes). **Puntaje máximo: 5**	**Tolerancia a errores** La capacidad del producto de software para mantener un nivel especificado de funcionamiento en caso de errores del software o de incumplimiento de su interfaz especificada.	5
Capacidad de mantenimiento Capacidad del producto de software para ser modificado. Las modificaciones pueden incluir correcciones, mejoras o adaptación del software a cambios en el entorno, y especificaciones de requerimientos funcionales.y software del sistema, y materiales (Ej: Papel de impresión o diskettes). **Puntaje máximo: 5**	**Cambiabilidad** La capacidad del software para permitir que una determinada modificación sea implementada.	5
Portabilidad La capacidad del software para ser trasladado de un entorno a otro. El entorno puede incluir entornos organizacionales, de hardware o de software. **Puntaje máximo: 10**	**Facilidad de instalación** La capacidad del producto de software para ser instalado en un ambiente especificado.	5
	Reemplazabilidad La capacidad del producto de software para ser utilizado en lugar de otro producto de software, para el mismo propósito y en el mismo entorno.	5

SERVICIOS TI - OTI - OGA - MTC V°B° Seg. Informática

Oficina de Tecnología de Información V°B° IN Y GOB. TI OGA - MTC

CALIDAD DE USO PUNTAJE MAXIMO: 10	
Característica	**Puntaje Máximo**
Eficacia La capacidad del producto de software para permitir a los usuarios lograr las metas especificadas con exactitud e integridad, en un contexto especificado de uso. **Puntaje máximo: 5**	5
Satisfacción La satisfacción es la respuesta del usuario a la interacción con el producto, e incluye las actitudes hacia el uso del mismo. **Puntaje máximo: 5**	5

PUNTAJE TOTAL	
CALIDAD INTERNA Y EXTERNA	= 90 puntos
CALIDAD DE USO	= 10 puntos
TOTAL	**= 100 puntos**

SERVICIOS TI - V°B° Seg. Informática - OTI - OGA - MTC

Oficina de Tecnologías de Información - V°B° INFOGOB. TI - OGA - MTC

ANEXO 2. EVALUACION DETALLADA DE LAS HERRAMIENTAS DE SOFTWARE

Característica [1]	Sub Categoría	Métrica	Puntaje Máx.	Alternativas	
				Qualys	Nessus
CALIDAD INTERNOS DE EXTERNOS (PUNTAJE MÁXIMO: 90)					
Funcionalidad	Adecuación	Capacidad de integrar tareas programadas para crear exclusiones, búsquedas avanzadas, cambio de nivel heurístico de seguridad.	5	5	4
Sub Total Adecuación			**5**	**5**	**4**
Funcionalidad	Interoperabilidad	Interfaz capaz de integrarse a aplicaciones de cumplimiento de seguridad	5	5	5
Funcionalidad	Interoperabilidad	Contar con una gestión centralizada que permitirá gestionar el estado de la solución y monitorear los equipos informáticos.	5	5	5
Funcionalidad	Interoperabilidad	Capacidad de uso en nube	5	5	5
Funcionalidad	Interoperabilidad	Interfaz simplificada HTML5	5	5	5
Sub Total Interoperabilidad			**20**	**20**	**20**
Funcionalidad	Exactitud	Permite detectar con exactitud las vulnerabilidades y brinda la remediación específica para la vulnerabilidad.	5	5	4
Sub Total Exactitud			**5**	**5**	**4**
Funcionalidad	Seguridad	Provee servicio de seguridad en capas.	5	4	5
Funcionalidad	Seguridad	Continuas actualizaciones de seguridad	5	4	5
Funcionalidad	Seguridad	Escáner con mayor índice de detección de vulnerabilidades	5	4	5
Funcionalidad	Seguridad	Capacidad de auditar servidores Linux y Windows	5	4	5
Funcionalidad	Seguridad	Análisis avanzado de Seguridad	5	4	5
Sub Total Seguridad			**25**	**20**	**25**
Usabilidad	Entendimiento	Descripción detallada de la vulnerabilidad encontrada	5	3	5
Sub Total Entendimiento			**5**	**3**	**5**
Usabilidad	Operabilidad	Capacidad de gestión desde diferentes equipos (móviles y PC)	5	4	4
Usabilidad	Operabilidad	Elementos de navegación intuitivos y fáciles de usar	5	3	4
Sub Total Operabilidad			**10**	**7**	**8**

SERVICIOS TI - OTI - OGA - MTC — V°B° Seg. Informática

V°B° IN Y GOB. TI — OGA - MTC

Característica [1]	Sub Categoría	Métrica	Puntaje Máx.	Alternativas	
				Qualys	Nessus
Fiabilidad	Tolerancia a errores	La consola de administración centralizada debe soportar actualizaciones desatendidas y remotas para descargar y desplegar las actualizaciones.	5	5	5
Sub Total Madurez			**5**	**5**	**5**
Capacidad de Mantenimiento	Cambiabilidad	Capacidad del software de implementar actualizaciones de vulnerabilidades en su base de datos de conocimiento.	5	3	5
Sub Total Conformidad de Facilidad de mantenimiento			**5**	**3**	**5**
Portabilidad	Facilidad de instalación	Capacidad de instalación en modo local o solución basada en nube.	5	4	5
Sub Total Facilidad de instalación			**5**	**4**	**5**
Portabilidad	Reemplazabilidad	Control de actualizaciones de manera incremental y automática desde la solución de seguridad.	5	5	5
Sub Total Reemplazabilidad			**5**	**5**	**5**
CALIDAD DE USO (PUNTAJE MÁXIMO: 10)					
Eficacia	Permite encontrar la máxima cantidad de vulnerabilidades en el servidor analizado.		5	4	5
Sub Total Eficacia			**5**	**4**	**5**
Satisfacción	Dar un soporte que impulse al usuario la comunicación proactiva para la prevención de errores, riesgos y fallas.		5	4	5
Sub Total Satisfacción			**5**	**4**	**5**
PUNTAJE TOTAL			**100**	**85**	**97**

Puntaje de adecuación: (Nivel Alto: 5, Nivel Medio: 4, Nivel Bajo: 3)