

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”
“Año de la Universalización de la Salud”

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE Nº 007-2020

“Solución de Ciberseguridad”

1. NOMBRE DEL ÁREA

Oficina General de Tecnologías de la Información - OGTI

2. RESPONSABLES DE LA EVALUACIÓN

Tobias Paul García Campos

Julio César Mamani Amanca

3. CARGO

Especialista en Seguridad de la Información

Coordinador de Gobierno Digital y Seguridad de la Información

4. FECHA

08 de Junio - 2020

5. JUSTIFICACION:

El Ministerio de la Producción requiere adquirir una solución de ciberseguridad conformada por licencias bajo la modalidad de suscripción que comprenderá el monitoreo de cuatrocientos (400) equipos de la red informática para protección proactiva con capacidad de auto aprendizaje, adaptándose de forma automática y en tiempo real a las nuevas formas de amenazas tanto conocidas como desconocidas que pudieran presentarse en los equipos informáticos de la infraestructura tecnológica de la institución.

6. ALTERNATIVAS:

Actualmente en el mercado existen diferentes soluciones correspondientes a ciberseguridad para equipos informáticos de la entidad, en merito a ello se toman en cuenta aquellas que sean compatibles e instalables en la plataforma tecnológica de usuario final.

Tomando en consideración las necesidades y requerimientos del Ministerio de la Producción, tomando en cuenta los nuevos esquemas relacionados con protección ante amenazas no solo conocidas, sino también desconocidas, se ha buscado alternativas de soluciones de Ciberseguridad en el mercado local que cumplan dichas necesidades y cuenten con soporte técnico local.

Se considera conveniente evaluar las siguientes soluciones a fin de definir una de ellas:

- DARKTRACE.
- TENABLE.IO.

Para la determinación de las soluciones seleccionadas, así como la evaluación técnica, se ha tomado como referencia:

- Información disponible en la página web de cada uno de los fabricantes.
- Información disponible en internet.

7. ANALISIS COMPARATIVO TÉCNICO:

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”
“Año de la Universalización de la Salud”

El análisis técnico ha sido realizado según los lineamientos establecidos en la "Guía técnica sobre evaluación de software para la administración pública" aprobado por R.M. N° 139-2004-PCM tal como exige el reglamento de la ley N° 28612 -"Ley que norma el uso, adquisición y adecuación del software en la administración pública":

7.1 Propósito de la Evaluación:

Validar que las alternativas seleccionadas sean las más convenientes para el Ministerio de la Producción.

7.2 Identificar el tipo de solución

Solución de Ciberseguridad para equipos informáticos.

7.3 Especificación del Modelo de Calidad.

La evaluación de la solución de Ciberseguridad se ha realizado bajo los parámetros establecidos en la RM 139-2004-PCM "Guía Técnica sobre Evaluación de Software en la Administración Pública".

7.4 Selección de métricas

Las métricas fueron identificadas de acuerdo a las funcionalidades que ofrecen las soluciones señaladas en el punto "6". Alternativas del presente informe

Cuadro comparativo de métricas

Cuadro N°01: Cuadro comparativo técnico

N°	Atributos	Descripción	Puntaje Máximo	DARKTRACE	TENABLE.IO
Atributos Internos y Externos					
1	Funcionalidad	Capacidad de adaptarse de forma automática a los cambios del entorno en tiempo real	6	6	6
		La tecnología de identificación de amenazas debe estar puramente basada en algoritmos avanzados de Machine Learning e Inteligencia Artificial	6	6	0
		No debe requerir la instalación de agentes en los equipos a monitorear	6	6	0
		Cumplir con las políticas de seguridad y acceso institucionales.	6	6	6
		Debe proporcionar visibilidad completa de la red, incluidas las TI tradicionales y no tradicionales.	6	6	6
		Debe poder identificar cualquier comportamiento anómalo en el entorno y resaltar estos comportamientos en tiempo real.	5	5	5
		Debe ser capaz de identificar	5	5	0

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”
“Año de la Universalización de la Salud”

		cualquier dispositivo nuevo insertado en la red.			
2	Fiabilidad	Capacidad de modelar el comportamiento normal del usuario, dispositivos y red, a partir de éste, identificar las anomalías correspondientes a brechas de seguridad	5	5	0
3	Usabilidad	Capacidad de aprendizaje autónomo del comportamiento normal de la red sin requerir conocimiento previo del historial de comportamiento anómalo	4	4	4
		Proporcionar una interfaz gráfica intuitiva, amigable, consistente y de fácil uso	4	4	4
		Disponibilidad de manuales y capacitación a cargo de especialistas calificados por el fabricante	4	4	4
4	Eficiencia	Debe mostrar las amenazas que se van identificando en la red en tiempo real y el detalle de logs de cada una de ellas	5	5	5
5	Portabilidad	Deberá poder identificar amenazas conocidas desde el primer día de instalada	5	5	5
6	Capacidad de mantenimiento	Registro de los incidentes de seguridad detectados para tener un claro entendimiento de éstas	5	5	5
		Permanentemente actualización de la solución, incluyendo el suministro de nuevas versiones y parches	5	5	5
		Soporte directo del fabricante	5	5	5
		Sub Total	82	82	60
1	Eficacia	Capacidad de detectar amenazas tanto internas como externas	8	8	8
2	Productividad	Debe ser centralizada, con una única interfaz de administración y visualización para toda la solución	5	5	5
3	Seguridad	Permite conservar los datos analizados sin alteraciones ni eliminaciones y capacidad de investigación forense	5	5	5
		Sub Total	18	18	18
		Total	100	100	78

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”
“Año de la Universalización de la Salud”

8. ANALISIS COMPARATIVO DE COSTO – BENEFICIO:

8.1 Licenciamiento

Se debe incluir licencias con mantenimiento de software (cambios de versión, actualización) por el tiempo del contrato.

La solución ofrecida debe corresponder a las últimas versiones

8.2 Software

Los sistemas operativos instalados en los computadores de trabajo desplegadas (Ms Windows, Linux, Android, IOS), cumplen con los requisitos exigidos por las soluciones de software evaluados.

8.3 Hardware necesario para su funcionamiento

El conjunto de equipos (FlexSystem x240 IBM, IBM Storwize V7000) que componen el Centro de Dato del Ministerio de la Producción, cumplen con los requisitos necesarios para la instalación de las soluciones evaluadas.

8.4 Soporte y mantenimiento externo

El fabricante de las soluciones ofertadas debe poseer Oficina de representación en Perú, así como personal de soporte técnico que garantice la adecuada y oportuna prestación de la garantía y de servicios. Este servicio debe ser 24x7.

El proveedor deberá prestar su asesoría presencial en la instalación y configuración del software.

8.5 Costo

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 la solución de ciberseguridad, cumpla con los requerimientos técnicos solicitados.

La evaluación estas alternativas incluyen los costos de licencias por suscripción anual y soporte y actualizaciones de la versión de las soluciones.

En el **Anexo N° 01**, se muestran los resultados del Análisis Comparativo de Costo – Beneficio, así como el cuadro de valoración técnica – económica.

En el **Anexo N° 02**, se muestra Costos Referenciales de Licencias de Software.

9. CONCLUSIONES Y RECOMENDACIONES

De acuerdo a la evaluación técnica de las métricas de las soluciones evaluadas: “DARKTRACE” y “TENABLE.IO” han obtenido puntajes aceptables.

En base al análisis realizado, se evidencia que la solución DARKTRACE es que alcanza el mayor puntaje, es decir, es la que mejor solución se adecua a las necesidades del área usuaria como solución de ciberseguridad para los equipos del parque informático que se necesita para el Ministerio de la Producción.



PERÚ

Ministerio
de la Producción

| OFICINA GENERAL DE TECNOLOGIAS DE LA INFORMACION

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”
“Año de la Universalización de la Salud”

10. FIRMA

Tobias Paul García Campos
Especialista en Seguridad
de la Información

Julio César Mamani Amanca
Coordinador de Gobierno Digital
y Seguridad de la Información



“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”
“Año de la Universalización de la Salud”

ANEXO 01

Costos referenciales de la solución de ciberseguridad

N°	Solución	Costo Total (S/.)(*)
1	Darktrace	34,400.00
2	Tenable.io	51,720.00




(*) Expresado en soles (S/.) incluye el 18% de IGV.

Análisis Costo – Beneficio

N°	Solución	Costo Total (S/.)(*)	Beneficio	Costo / Beneficio
1	Darktrace	34,400.00	100	100%
2	Tenable.io	51,720.00	78	74.55%

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”
“Año de la Universalización de la Salud”

ANEXO 02**Costos referenciales de soluciones****a) Darktrace**

DARKTRACE - AGT / PRODUCE										
										
 Propuesta Económica 1: Precios expresados en Soles Periodo: 12 meses Si incluye IGV. Pago ANUAL único Pago a 30 días.	<table border="1"><thead><tr><th>Alcance del servicio</th><th>SUPER OFERTA ABRIL</th></tr></thead><tbody><tr><td>400 dispositivos</td><td rowspan="6">S/ 34,400</td></tr><tr><td>Modulo (EIS) Enterprise Immune Systems</td></tr><tr><td>NO Módulo Antigena (respuesta autónoma)</td></tr><tr><td>Capacitación Pública</td></tr><tr><td>Instalación Remota</td></tr><tr><td>Soporte anual de HW y SW</td></tr></tbody></table>	Alcance del servicio	SUPER OFERTA ABRIL	400 dispositivos	S/ 34,400	Modulo (EIS) Enterprise Immune Systems	NO Módulo Antigena (respuesta autónoma)	Capacitación Pública	Instalación Remota	Soporte anual de HW y SW
Alcance del servicio	SUPER OFERTA ABRIL									
400 dispositivos	S/ 34,400									
Modulo (EIS) Enterprise Immune Systems										
NO Módulo Antigena (respuesta autónoma)										
Capacitación Pública										
Instalación Remota										
Soporte anual de HW y SW										

b) Tenable.io

MINISTERIO DE LA PRODUCCION									
 Propuesta Económica: Precios en soles Incluye IGV Pago único anual. Pago a 30 días.	<table border="1"><thead><tr><th>Alcance del servicio</th><th>Precio Total</th></tr></thead><tbody><tr><td>400 dispositivos</td><td rowspan="5">S/ 51,720</td></tr><tr><td>Modulo descubrir</td></tr><tr><td>Módulo evaluar</td></tr><tr><td>Modulo Priorizar</td></tr><tr><td>Soporte 1 año</td></tr></tbody></table> 	Alcance del servicio	Precio Total	400 dispositivos	S/ 51,720	Modulo descubrir	Módulo evaluar	Modulo Priorizar	Soporte 1 año
Alcance del servicio	Precio Total								
400 dispositivos	S/ 51,720								
Modulo descubrir									
Módulo evaluar									
Modulo Priorizar									
Soporte 1 año									