INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE

N°007-2019-1U0100

1. NOMBRE DEL AREA:

Oficina de Seguridad Informática

2. RESPONSABLE DE LA EVALUACIÓN:

Hipólito Alejandro Alférez Meza

CARGO

Técnico 5 - Oficina de Seguridad Informática

3. FECHA:

09 de agosto de 2019

4. JUSTIFICACIÓN:

La Intendencia Nacional de Sistemas de Información requiere contar con una solución tecnológica de protección proactiva y mitigación de amenazas informáticas que permita la utilización de tecnologías con la capacidad de auto aprendizaje adaptándose de forma autónoma y en tiempo real a las nuevas formas de amenazas que pudieran presentarse en la infraestructura institucional.

5. ALTERNATIVAS:

En la exploración tecnológica del mercado se analizó la siguiente solución:

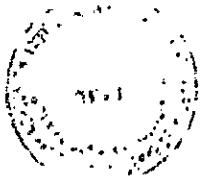
DARKTRACE Enterprise Immune System

6. ANÁLISIS COMPARATIVO TÉCNICO

Para el producto seleccionado se ha evaluado los atributos mínimos que la solución debe contemplar, en el siguiente cuadro se muestran los puntajes de cada atributo:

	Puntaje Max 100 puntos	DARKTRACE Immune System
ATRIBUTOS INTERNOS	**50**	**50**
Funcionalidad: Adecuación Capacidad de adaptarse de forma automática a los cambios del entorno en tiempo real	7	7
Funcionalidad: Exactitud La tecnología de identificación de amenazas debe estar puramente basada en algoritmos avanzados de Machine Learning e Inteligencia Artificial	7	7
Funcionalidad: Interoperabilidad No debe requerir la instalación de agentes en los equipos a monitorear	7	7
Funcionalidad: Seguridad Cumplir con las políticas de seguridad y acceso institucionales.	5	5
Fiabilidad: Madurez Capacidad de modelar el comportamiento normal del usuario, dispositivos y red, y a partir de éste identificar las anomalías correspondientes a brechas de seguridad	6	6

Usabilidad: Entendimiento Capacidad de aprendizaje autónomo del comportamiento normal de la red sin requerir conocimiento previo del historial de comportamiento anómalo	5	5
Usabilidad: Atracción Proporcionar una interfaz gráfica intuitiva, amigable, consistente y de fácil uso.	5	5
Eficiencia: Comportamiento de tiempos 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
Portabilidad: Facilidad de instalación Deberá poder identificar amenazas conocidas desde el primer día de instalada	3	3
ATRIBUTOS EXTERNOS	**20**	**20**
Usabilidad: Aprendizaje Disponibilidad de manuales y capacitación a cargo de especialistas calificados por el fabricante	5	5
Capacidad de mantenimiento: Capacidad de ser Analizado Registro de los incidentes de seguridad detectados para tener un claro entendimiento de éstas	5	5
Capacidad de mantenimiento: Cambiabilidad Permanente actualización de la solución, incluyendo el suministro de nuevas versiones y parches.	5	5
Capacidad de mantenimiento: Estabilidad Soporte directo del fabricante.	5	5
ATRIBUTOS DE USO	**30**	**30**
Productividad: Debe ser centralizada, con una única interfaz de administración y visualización para toda la solución	7	7
Eficacia: Capacidad de detectar amenazas tanto internas como externas	8	8
Satisfacción: El análisis del tráfico debe basarse en algoritmos avanzados de Machine Learning e Inteligencia Artificial	8	8
Seguridad: Permite conservar los datos analizados sin alteraciones ni eliminaciones, y capacidad de investigación forense	7	7
PUNTAJE TOTAL	**100**	**100**



7. CONCLUSIONES

La solución tecnológica analizada cumple con las características y los requisitos mínimos requeridos. Por lo tanto, se recomienda realizar un proceso de adquisición por concurso en la que participe esta solución tecnológica, además de cualquier otra que satisfaga los requerimientos exigidos.

Hipólito Alejandro Alférez Meza
Registro 7120