"Año del Buen Servicio al Ciudadano"

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE N° 001-2017-MINEDU/VMGI/PRONIED-OTI

LICENCIA DE HERRAMIENTA DE SOFTWARE CORRELACIONADOR DE EVENTOS

1. **NOMBRE DEL ÁREA**
   Oficina de Tecnologías de la Información (OTI)

2. **RESPONSABLE DE LA EVALUACIÓN**
   Ing. Ronald Angel Cornejo Benavente

3. **CARGO**
   Especialista de Seguridad de la Información

4. **FECHA**
   28 de abril de 2017

5. **JUSTIFICACIÓN**
   El Programa Nacional de Infraestructura Educativa - PRONIED es una institución pública que para cumplir adecuadamente con sus actividades y ejecutar eficientemente sus procesos, requiere de una herramienta de software correlacionador de eventos permita centralizar los diferentes eventos que suceden en la infraestructura tecnológica de la institución.

   Asimismo de acuerdo al Decreto Supremo N° 013-2003-PCM y el Decreto Supremo N° 037-2005-PCM, establecen las disposiciones referidas al licenciamiento de software en entidades públicas, haciendo necesaria la adquisición formal y legal de las licencias de los productos utilizados.

6. **ALTERNATIVAS**
   Considerando los requerimientos del PRONIED, se ha buscado alternativas de herramienta de software correlacionador de eventos.

   Se analizarán las siguientes alternativas:

   - SolardWinds SIEM Log & Event Manager
   - ManageEngine EventLog Analyzer Premium Edition

7. **ANÁLISIS COMPARATIVO TÉCNICO**
   Se realiza una evaluación técnica de acuerdo a lo dispuesto en la parte 3 "Proceso de Evaluación de Software" de la "Guía Técnica sobre Evaluación de Software en la Administración Pública", aprobado mediante Resolución Ministerial Nº 139-2004-PCM.

   a. Propósito de la Evaluación
   Determinar los atributos o características mínimas de la licencia de herramienta de software correlacionador de eventos.

   b. Identificador de tipo de producto
   Licencia de herramienta de software correlacionador de eventos.

c. Especificaciones de Modelo de Calidad

Se aplicará el modelo de calidad de software descrito en la parte 1 de la guía de evaluación de software mencionada y se determinan los atributos relacionados con la funcionalidad y usabilidad que aprobado por resolución Ministerial Nº 139-2004-PCM.

d. Selección de Métricas

Las Métricas fueron seleccionadas en base al análisis de información de los productos señalados en el punto "Alternativas".

ITEM	ATRIBUTOS	DESCRIPCIÓN
1	**ATRIBUTOS INTERNOS Y EXTERNOS**	
1.1	Interfaz	Interfaz de tipo web, intuitiva, con tablero de control
1.2	Recolección de Log y eventos	Permite la recolección de log y eventos desde cualquier dispositivo de red
1.3	Análisis de Log en tiempo real	Permite el análisis se efectué en tiempo real vía procesamiento de memoria
1.4	Unificación de eventos	Permite la unificación de eventos de diferentes fabricantes
1.5	Ejecuta acciones de respuesta de incidentes críticos	Permite programar tareas automatizadas como poner en cuarentena maquinas infectadas, bloqueo de direcciones IPs, reinicio de servicios
1.6	Protección de Datos sensibles	Protege los datos sensibles con políticas que impidan manipulación dispositivos USB, conexión remota no autorizada
1.7	Rastreo de dispositivos USB	Permite el rastreo de dispositivos USB en tiempo real, incluyendo los archivos y procesos que sea accedido por estos.
1.8	Reglas Pre-Configuradas	Permite tener al menos 600 reglas pre-configuradas de correlación para seguridad y monitoreo de red
1.9	Reportes	Realiza reportes en forma automática y programada, envíos de correo e-mail, o almacenados en disco
1.10	Exportación	Permite exportar en formatos HTML, Crystal Report, PDF, Excel
1.11	Personalización de reportes	Permite personalizar a detalle, agrupar de acuerdo a las necesidades de un dispositivo determinado
1.12	Cumplimiento	Permite generar reportes de cumplimiento, con al menos 200 plantillar integradas para cumplimiento de PCI, DSS, SOC, entre otros.
1.13	Tablero de Mando	Proporciona una visión total e inmediata de la seguridad de la red
1.14	Manipulación de consola	Permite arrastrar y soltar, así como depuración constante de objetos del tablero de mando
1.15	Compresión de datos de registro	Permite realizar compresión con al menos 95% de capacidad del mismo, programación de archivado

1.16	Rastreo de eventos maliciosos	Correlaciona datos de eventos de múltiples fuentes en tiempo real mediante reglas
1.17	Integración de factores de autenticación	Permite la integración de factores de autenticación como, contraseña, tarjeta inteligente, dispositivo biométrico
1.18	Alertas	Permite envío de alertas en tiempo real sobre eventos der seguridad
1.19	Sistema Operativo Soportado	La solución ofertada deberá soportar los Sistemas Operativos Windows 7 (32 y 64 bits), Windows 8 y 8.1 (32 y 64 bits), Windows 10, Windows 2008 Server (64 bits), Windows 2012 Server (64 bits) y
2	**ATRIBUTOS DE USO**	
2.1	Facilidad de uso e instalación	El uso de interface debe ser fácil y amigable e intuitiva.
2.2	Soporte local	Cuenta con un representante local, el cual debe proporcionar el soporte respectivo.
2.3	Capacitación	Requiere capacitación

e. Niveles, escalas para las métricas

ITEM	ATRIBUTOS	NIVEL
1	ATRIBUTOS INTERNOS Y EXTERNOS	91
1.1	Interfaz	5
1.2	Recolección de Log y eventos	5
1.3	Análisis de Log en tiempo real	5
1.4	Unificación de eventos	5
1.5	Ejecuta acciones de respuesta de incidentes críticos	4
1.6	Protección de Datos sensibles	4
1.7	Rastreo de dispositivos USB	5
1.8	Reglas Pre-Configuradas	5
1.9	Reportes	4
1.10	Exportación	5
1.11	Personalización de reportes	5
1.12	Cumplimiento	5
1.13	Tablero de Mando	5
1.14	Manipulación de consola	5
1.15	Compresión de datos de registro	5
1.16	Rastreo de eventos maliciosos	5
1.17	Integración de factores de autenticación	5
1.18	Alertas	5
1.19	Sistema Operativo Soportado	4

2	ATRIBUTOS DE USO	9
2.1	Facilidad de uso e instalación	3
2.2	Soporte local	3
2.3	Capacitación	3
	TOTAL	100

El análisis técnico y calificación de las métricas realizado a las tres (03) alternativas de software se muestra a continuación:

ITEM	ATRIBUTOS	NIVEL	ALTERNATIVAS	
1	ATRIBUTOS INTERNOS Y EXTERNOS	91	SOLARDWINDS SIEM LOG & EVENT MANAGER	MANAGEENGINE EVENTLOG ANALYZER PREMIUM EDITION
1.1	Interfaz	5	5	5
1.2	Recolección de Log y eventos	5	5	4
1.3	Análisis de Log en tiempo real	5	5	4
1.4	Unificación de eventos	5	5	4
1.5	Ejecuta acciones de respuesta de incidentes críticos	4	4	4
1.6	Protección de Datos sensibles	4	4	4
1.7	Rastreo de dispositivos USB	5	5	4
1.8	Reglas Pre-Configuradas	5	4	4
1.9	Reportes	4	4	4
1.10	Exportación	5	5	4
1.11	Personalización de reportes	5	5	4
1.12	Cumplimiento	5	5	3
1.13	Tablero de Mando	5	5	4
1.14	Manipulación de consola	5	5	3
1.15	Compresión de datos de registro	5	5	4
1.16	Rastreo de eventos maliciosos	5	4	4

1.17	Integración de factores de autenticación	5	5	4
1.18	Alertas	5	5	4
1.19	Sistema Operativo Soportado	4	4	4
2	**ATRIBUTOS DE USO**	**9**	**9**	**9**
2.1	Facilidad de uso e instalación	3	3	2
2.2	Soporte local	3	3	3
2.3	Capacitación	3	3	3
TOTAL		**100**	**98**	**84**

Este análisis tiene un peso del 80%.

8. ANÁLISIS COSTO BENEFICIO

Para el análisis de costo – beneficio se ha tomado en cuenta los criterios solicitados en el punto 8, del reglamento de la Ley Nº 28612

Nº	CRITERIOS A EVALUAR	SOLARDWINDS SIEM LOG & EVENT MANAGER	MANAGEENGINE EVENTLOG ANALYZER PREMIUM EDITION
1	Costo Referencial	Costo de 1 licencia: S/.20,000.00.	Costo de 1 licencia: S/. 11,358.00.

Este análisis tiene un peso del 20%.

Fórmula del cálculo del puntaje:
Puntaje de menor costo (mc) = 100 puntos.
Puntaje de Mayor Costo (MC) = (mc/MC)*100

A continuación se presenta el resultado global del análisis técnico y el análisis costo – beneficio:

ATRIBUTOS	SOLARDWINDS SIEM LOG & EVENT MANAGER	MANAGEENGINE EVENTLOG ANALYZER PREMIUM EDITION
Análisis Comparativo Técnico	73.1	70.9
Análisis Costo Beneficio	18.3	17.7
TOTAL	**91.4**	**88.6**

9. CONCLUSIONES

Por lo expuesto, y considerando los resultados del Análisis Comparativo Técnico y Análisis Costo Beneficio, se concluye que la licencia de SolardWinds SIEM Log & Event Manager es el que mejor se adecua a las necesidades del PRONIED.

10. FIRMAS

Abog. Wilson Vara Mallqui
Jefe (e) de la Oficina de Tecnologías de la Información – OTI
PRONIED

Ing. Ronald Angel Cornejo Benavente
Especialista de Seguridad de la Información
PRONIED