SUNAT

INFORME TECNICO PREVIO DE EVALUACIÓN DE SOFTWARE N° 001-2010 / 2A2000

1. **NOMBRE DEL AREA:**

   OFICINA DE INVESTIGACIÓN Y TECNOLOGIA

2. **RESPONSABLES DE LA EVALUACION:**

   YURI CASTAÑEDA PEDROZA

3. **CARGO:**

   PROFESIONAL DE LA OFICINA DE INVESTIGACIÓN TECNOLOGICA

4. **FECHA**

   30 DE ABRIIL DEL 2010

5. **JUSTIFICACIÓN**

La Oficina de Seguridad de la Intendencia Nacional de Sistemas de Información de la SUNAT requiere dar mayor eficiencia y eficacia a la administración de reportes de alertas de intrusiones, ataques, actividades sospechosas, violaciones de políticas o accesos no autorizados que soporta nuestra infraestructura Informática, la cual permitirá mayor rapidez en la atención al presentarse eventos de seguridad a los servicios que se prestan propios del negocio y poder minimizar el riesgo.

6. **ALTERNATIVAS**

Se han seleccionado dos herramientas de análisis de eventos para brindar información centralizada de seguridad en tiempo real:

- TSOM (IBM)
- CA Enterprise Log Manager

Tivoli Security Operations Manager de IBM es una plataforma de gestión de sucesos e información que ayuda a mejorar la visibilidad de la gestión de riesgos de la información y las operaciones de seguridad, centraliza y almacena los datos de seguridad de la infraestructura de tecnológica.

CA Enterprise Log Manager es un producto de Computer Associates que recolecta, sistematiza y archiva los registros de las actividades de TI de múltiples fuentes y brinda capacidades de búsqueda, análisis y generación de reportes.

7. ANALISIS COMPARATIVO TECNICO

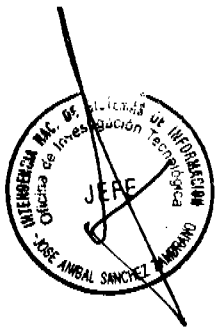
Para realizar el análisis comparativo de las herramientas se han identificado sólo las características que marcan las diferencias entre ambos productos:

REQUERIMIENTO MÍNIMO:

	Puntaje Máximo	Puntaje Mínimo	TSOM (IBM)	CA Enterprise Log Manager
PUNTAJE TOTAL	**100**	**75**	**92**	**89**
ATRIBUTOS INTERNOS	**25**	**20**	**25**	**25**
Usabilidad: ***Interoperatividad*** Enviar las alertas de seguridad por consola gráfica, Web, E-mail, beeper, tickets de help desk, etc.			5	5
Funcionalidad: ***Seguridad*** Capacidad de almacenar la información en una base de datos relacional.			5	5
Contar con mecanismos de control de accesos al sistema de seguridad.			5	5
Permitir niveles para los roles y perfiles de acceso.			5	5
Fiabilidad: ***Conformidad de la fiabilidad*** Identificar en forma precisa el recurso informático atacado, indicando los diferentes tipos de amenazas, ataques y patrones de intrusión.			5	5
ATRIBUTOS EXTERNOS	**20**	**10**	**13**	**16**
Usabilidad: ***Atracción*** Sus clientes son de uso amigable e intuitivo, y dispone de interfaces gráficas que guían al programador.			5	5
Funcionalidad: ***Adecuación*** Seguimiento para la trazabilidad de ticket para los diferentes eventos de seguridad definidos, para tener búsquedas más fáciles de realizar			3	3
Análisis de Log multidimensional (capacidad de drill down)			0	5
Compresión de log			5	3
ATRIBUTOS DE USO	**55**	**35**	**54**	**48**
Productividad Consola centralizada de seguridad, en ambiente gráfico, simple y fácil de usar con la finalidad de monitorear, ver, analizar, correlacionar y administrar todo los eventos de seguridad en tiempo real y en todo momento.			5	5
Correlacionar los eventos de la información que se está obteniendo en tiempo real.			4	2
Crear o Modificar sus reglas en busca de patrones de ataques.			4	4
Generar reportes definidos y personalizados que muestren la			4	4

INTENDENCIA NAC. DE SISTEMAS DE INFORMACION
Oficina de Investigación Tecnológica
JEFE
JOSE ANIBAL SANCHEZ ZAMBRANO

actividad de los eventos de seguridad.				
Poder sumarizar evento, explotar información de manera dinámica, creación de reportes dinámicos, Crear reglas complejas de manera visual y sencilla.			4	4
Permitir generar ticket para los diferentes eventos de seguridad en la consola.			4	4
Satisfacción Obtener y analizar en tiempo real la información generada por los diferentes equipos de la red (Firewall, Equipos de redes, Servidores, IDS, aplicaciones, etc.) mediante la revisión de archivos de anotaciones cronológicas (Logs Files) y/o mediante la recepción de traps, syslog..			4	4
Reducir el número de eventos duplicados (eventos que la única información que cambia son los segundos) o similares (eventos del tipo port scan) que son informados por los equipos que están siendo monitoreados			4	4
Mostrar en la consola solamente el equipo que está siendo atacado, filtrando los equipos por donde la trama del ataque pasó.			4	0
Procesar la información en tiempo real, a través de la correlación de eventos, para filtrar información no critica y repetitiva, eliminando falsos positivos y enviando a la consola solamente información que amerite especial atención.			5	5
Permitir a los administradores crear y/o configurar agentes o sensores propios para capturar información incluyendo nuevas reglas.			4	4
Permitir configurar los agentes o sensores para adaptarlos a requerimientos específicos, es decir adicionar, modificar reglas, poder definir acciones que deban ejecutarse en respuesta			4	4
Permitir filtrar eventos que indiquen ciertos patrones o firmas, que los administradores definan, sobre direcciones IP internas.			4	4



ANALISIS COMPARATIVO DE COSTO - BENEFICIO

El costo total de propiedad de ambas opciones es similar y va depender del nivel de descuento que ofrezcan los fabricantes, por lo que evaluaremos solo los beneficios cualitativos:

- La solución permitirá detectar en tiempo real los posibles ataques que se den contra la infraestructura tecnológica de la SUNAT, pudiendo evitar posibles daños.
- La solución implementada podrá ser accedida a través de un ambiente Web y mostrará la información de manera gráfica y fácil de entender para el analista de seguridad de la institución, permitiendo además hacer un análisis detallado de la información asociada a los ataques a la infraestructura.

8. CONCLUSIÓN

Tanto Tivoli Security Operations Manager como CA Enterprise Log Manager cumplen con los requisitos técnicos. Por lo tanto se recomienda realizar un proceso de adquisición por concurso en la que participen ambos productos, además de cualquier otro que satisfaga los requerimientos técnicos mínimos.

9. FIRMA