"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año del Dialogo y la Reconciliación Nacional"

MINISTERIO DE EDUCACIÓN
SPE - OTIC
Folio Nº 3

INFORME TECNICO PREVIO DE EVALUACIÓN DE SOFTWARE DE MONITOREO Y AUDITORIA DE BASE DE DATOS DEL MINISTERIO DE EDUCACIÓN

INFORME Nº 303-2018-MED-SPE-OTIC

1. **NOMBRE DEL AREA:**
   Oficina de Tecnologías de la Información y Comunicación

2. **RESPONSABLE DE LA EVALUACIÓN:**
   - Lic. Jaime Ccanto Crispín
   - Ing. Julio Enrique Álvarez Guizado

3. **CARGO:**
   Especialistas en Especificaciones Técnicas - OTIC

4. **FECHA**
   Julio de 2018

5. **JUSTIFICACIÓN**

La Unidad de Calidad y Seguridad de la Información – UCSI de la Oficina de Tecnologías de la Información y Comunicación – OTIC del Ministerio de Educación, requiere la adquisición de un "software para el monitoreo y auditoria de base de datos", con la finalidad de reducir el riesgo de fuga de información sensible del Ministerio de Educación.

Por lo expuesto y en el marco de la Ley 28612 "Ley que norma el uso, adquisición y adecuación del software en la Administración Pública", se procede a evaluar el Software para el monitoreo y auditoria de base de datos.

6. **ALTERNATIVAS**

Considerando los requerimientos de la Unidad de Calidad y Seguridad de la Información de la OTIC, se han buscado alternativas de software en el mercado, tomando en consideración la disponibilidad en el servicio de atención y de soporte local.

En ese sentido, la búsqueda ha dado como resultado los productos que se listan a continuación:

- McAfee Database Security.
- SecureSphere Database Activity Monitoring.
- Security Guardium Data Activity Monitor.

7. **ANÁLISIS COMPARATIVO TÉCNICO**

El análisis técnico ha sido realizado en conformidad con la metodología establecida en la "Guía Técnica sobre evaluación de software en la administración pública" (R.M. N° 139-2004-PCM) tal como se exige en el reglamento de la Ley N° 28612.

a. **Propósito de evaluación**
   Validar que las alternativas seleccionadas sean las más convenientes para el uso de la Unidad de Calidad y Seguridad de la Información de la OTIC del Ministerio de Educación.

b. **Identificar el tipo de producto**
   Software de monitoreo y auditoria de base de datos.

c. Identificación del modelo de calidad
Se aplicará el Modelo de Calidad de Software descrito en la parte I de la Guía de evaluación de software aprobado por Resolución Ministerial N° 139-2004-PCM.

d. Selección de métricas.
Las métricas fueron identificadas de acuerdo a los criterios de las especificaciones técnicas del Ministerio de Educación. Ver Anexo 01; en ella se han evaluado atributos internos, externos y de uso.

8. ANÁLISIS COMPARATIVO DE COSTO - BENEFICIO

El presente análisis tiene por objetivo seleccionar la mejor alternativa, para lo cual se ha optado por dar un peso a la evaluación técnica de 0.7 y a la evaluación económica de 0.3, con el fin de garantizar que el software a adquirir cumpla con los requerimientos solicitados. Ver Anexo 02.

La implementación de estas alternativas incluye el costo de una (01) Licencia de productos seleccionados. Ver Anexo 03 - Costos referenciales de licencias de software.

El producto ofrecido debe corresponder a la última versión liberada en el mercado.

9. CONCLUSIÓN

De los resultados del análisis realizado, se puede verificar que el producto McAfee Database Security, es la que alcanza el mayor puntaje, es decir es la que mejor se adecua a las necesidades del área usuaria como Software de Monitoreo y Auditoria de Base de Datos.

10. RECOMENDACIÓN

Se recomienda la adquisición del producto que obtuvo mayor puntaje en el Análisis de Costo – Beneficio, debido a sus características técnicas de dicho producto satisface la necesidad del área usuaria.

11. FIRMAS

Lic. Jaime Ccanto Crispín
Especialista en Especificaciones Técnicas GTI - OTIC
Ministerio de Educación

Especialista en Especificaciones Técnicas OTIC MINEDU V°B°

Ing. Julio Álvarez Guizado
Especialista en Especificaciones Técnicas GTI - OTIC
Ministerio de Educación

MINISTERIO DE EDUCACIÓN - REPÚBLICA DEL PERÚ - Oficina de Tecnologías de la Información y Comunicación

Alberto Carlos Pajuelo Huamán
Jefe de la Oficina de Tecnologías de la Información y Comunicación - Ministerio de Educación

ANEXO 01

METRICAS (ATRIBUTOS) INTERNAS Y EXTERNAS										
N°	Atributos	Descripción	Puntaje Máximo:	Puntaje Mínimo:	Criterio de calificación	Puntaje	McAfee Database Security	SecureSphere Database Activity Monitoring	Security Guardium Data Activity Monitor
1	Funcionalidad	Permitir la mayor escalabilidad posible a nivel de crecimiento futuro sin requerir cambios mayores en la arquitectura y/o componentes de la misma.	4	2	Total	4	4	2	2
					Parcialmente	2			
		Permite monitorear en tiempo real varios servidores de base de datos.	4	2	Total	4	4	4	4
					Parcialmente	2			
		Permite monitorear varias instancias de bases de datos en un servidor de base de datos.	4	2	Total	4	4	4	4
					Parcialmente	2			
		La consola de administración permite virtualizarse y estar en capacidad de procesar el manejo de instancias ilimitadas de bases de datos.	4	2	Total	4	4	4	4
					Parcialmente	2			
		Permite que la arquitectura no sea intrusiva con la capa de datos de la base de datos .	4	2	Total	4	4	4	4
					Parcialmente	2			
		Permite monitorear el 100% de las actividades, incluyendo las de los DBA.	4	2	Total	4	4	4	4
					Parcialmente	2			
		Permite que las políticas definidas generen alertas de seguridad en tiempo real, bloqueo de software o conexiones no autorizadas que intenten acceder a la base de datos, bloqueo automático de cuentas, etc.	4	2	Total	4	4	4	4
					Parcialmente	2			
		Permite leer la memoria compartida, para evitar intrusiones sobre los datos de la base de datos.	4	2	Total	4	4	4	4
					Parcialmente	2			
		Permite el bloqueo y la configuración de cuarentenas, mientras se analiza el incidente presentado.	4	2	Total	4	4	4	4
					Parcialmente	2			
		Permite instalar en los servidores sensores de monitoreo, no deberán requerir reinicio.	4	2	Total	4	4	4	4
					Parcialmente	2			
		Permite contar con la funcionalidad de parcheo virtual, para brindar seguridad al ambiente de bases de datos y conocer el impacto cuando el fabricante de la base de datos no haya liberado el parche aún.	4	2	Total	4	4	4	4
					Parcialmente	2			
		Permite integrar los datos de auditoría recolectados con data de algunas tablas de la base de datos a fin de poder enriquecer los reportes de auditoría.	4	2	Total	4	4	4	4
					Parcialmente	2			
		Permite soportar diversas fuentes de información tales como: Oracle, DB2, Mcrosoft SQL Server, Informix, My SQL entre otros.	4	2	Total	4	4	4	4
					Parcialmente	2			
		Permite soportar diferentes servidores de aplicaciones tales como Oracle application server, web logic Webspghere application server, Jboss.	4	2	Total	4	4	4	4
					Parcialmente	2			
		Permite supervisar las actividades de las bases de datos de los diferentes sistemas operativos sin necesidad de encender el log nativo de auditoría o cambiando las configuraciones o puertos de las bases de datos.	4	2	Total	4	4	4	4
					Parcialmente	2			
		Debe permitir contar con un agente en cada servidor de BD para realizar el monitoreo; la herramienta deberá tener la capacidad de alertar en tiempo real si es que el agente es desactivado.	4	2	Total	4	4	4	4
					Parcialmente	2			
2	Fiabilidad	Capacidad para evaluar y reaccionar ante identificar posibles ataques sobre la base de datos a través de la correlación de eventos (múltiples intentos fallidos de conexión denotarían ataques de fuerza bruta, consultas sobre objetos inexistentes parecerían ataques de SQL-Injection).	4	2	Total	4	4	4	4
					Parcialmente	2			
3	Usabilidad	Permite la creación de backups de reglas configuradas.	4	2	Total	4	4	4	4
					Parcialmente	2			
		Permite una arquitectura no intrusiva que no precisa tiempo de inactividad para su instalación, actualización o desinstalación	4	2	Total	4	4	4	4
					Parcialmente	2			
4	Capacidad de Mantenimiento	Tiene la capacidad de adaptarse a nuevos requerimientos de la organización y fácil actualización del de la solución en futuras nuevas versiones	4	2	Total	4	4	4	4
					Parcialmente	2			
Sub Total			80	40			80	78	78
METRICAS (ATRIBUTOS) DE USO									
1	Eficacia	Permite proteger las bases de datos de forma sólida, administra su seguridad de manera sistemática y hace que se cumplan las normativas continuamente sin necesidad de hacer cambios en la arquitectura, preservar su rendimiento, y la continuidad de las operaciones.	5	3	Total	5	5	5	5
					Parcialmente	3			
2	Productividad	Permite una fácil administración mediante las herramientas intuitivas propios de la solución.	5	3	Total	5	5	5	5
					Parcialmente	3			
3	Seguridad	Permite la protección en tiempo real de las bases de datos cruciales de la institución frente a todo tipo de amenazas: externas, internas e incluso exploits internos de las bases de datos.	5	3	Total	5	5	5	5
					Parcialmente	3			
4	Satisfacción	Permite la generación de reportes fiables de vulnerabilidades técnicas asociando valores de riesgo que permitan gestionarlos de acuerdo a su criticidad.	5	3	Total	5	5	5	5
					Parcialmente	3			
Sub total			20	12			20	20	20
Total			100	52			100	98	98

ANEXO 02

COSTOS REFERENCIALES DE LICENCIAS DE SOFTWARE DE MONITOREO Y AUDITORIA DE BASE DE DATOS.

Cantidad	Software	Costo por Licencia (*)
1	McAfee Database Security	42,010.01
1	SecureSphere Database Activity Monitoring	216,269.63
1	Security Guardium Data Activity Monitor	133,014.65

* Precio expresado en Nuevos Soles (S/.)

Tipo de cambio dólar: S/. 3.33

Fecha: 28/06/2018

ANÁLISIS COSTO - BENEFICIO

Cantidad	Software	Costos S/.	Beneficio	Costo / Beneficio
1	McAfee Database Security	42,010.01	100	100.00%
1	SecureSphere Database Activity Monitoring	216,269.63	98	74.43%
1	Security Guardium Data Activity Monitor	133,014.65	98	78.07%

ANEXO 03

COSTOS REFERENCIALES DE LICENCIAS DE SOFTWARE

a) McAfee Database Security

NEXSYS — McAfee

PROPUESTA ECONOMICA

CLIENTE: MINISTERIO DE EDUCACION
CONTACTO: JORGE ABAD
FECHA: 31/05/2018
FORMA DE PAGO: *según créditos*

PAIS: PERU
VIGENCIA: 7 días
FABRICANTE: MCAFEE
FACTURACION / ENTREGA: HARDWARE 45 DIAS / SOFTWARE (LICENCIAS) 4 DIAS

DESCRIPCION DE SOLUCION: Propuesta de solución de licenciamiento paquete soporte Business

#	SKU	DESCRIPCION	CANTIDAD	PRECIO DE VENTA	
				PRECIO UNITARIO	TOTAL
1	DCDCKE-AA-AA	MFE Datacenter Sec Suite DbaseP:1BZ [P+]	1	$10,691.20	$ 10,691.20

Subtotal		$ 10,691.20
IGV	18%	$ 1,924.42
Total		$ 12,615.62

https://www.mcafee.com/es/products/database-security/index.aspx

b) SecureSphere Database Activity Monitoring

CONFIDENCIAL

Hoja de Cotización Secure One

S1 Secure One — Aseguramos tu información

Preparada Por:
Carmen Agurto - Ejecutiva de Cuentas
Celular: 979-377-510
Telefono:
Fax: 51(1) 7112900
Email: magurto@secureone.com.pe

País: Perú
Cliente: MINISTERIO DE EDUCACIÓN
Contacto: Jorge Abad
Telefono: 6155800
Fax:

Fecha: 16/02/2018

Cotización N° 0048 - 2018

Item	Part Number	Marca	Descripcion	Cant.	Monto en Soles S/.
1	SS-DBF-V25-V1	IMPERVA	V2500 Database Firewall Virtual Appliance	1	S/. 96,525.00
2	SS-DBF-V25-SL1		V2500 Database Firewall Virtual Appliance, 12 Months Enhanced Support	1	S/. 22,522.50
3	A-WAF-V25		Add-on: V2500 Web Application Firewall	1	S/. 32,175.00
	A-WAF-V25-SL1		Add-on: V2500 Web Application Firewall, 12 Months Enhanced Support	1	S/. 7,507.50
	U-DBURM-25		Upgrade: User Rights Management License for 25DBis	1	S/. 8,043.75
	U-DBURM-25-SL1		Upgrade: User Rights Management License for 25DBis, 12 Months Enhanced Support	1	S/. 1,876.88
	U-DBURM-25		VM150 Management Server Virtual Appliance	1	S/. 38,610.00
	U-DBURM-25-SL1		VM150 Management Server Virtual Appliance , 12 Months Enhanced Support	1	S/. 9,009.00
			SUBTOTAL PRODUCTOS (S/.)		S/. 216,269.63

https://www.imperva.com/products/data-security/database-audit-protection/

c) Security Guardium Data Activity Monitor

P/N	Descripción	Cantidad	Precio S/	IGV	Total S/
Licenciamiento de software IBM Security Guardium					
D1NE3LL	IBM Security Guardium Data Protection for Databases Resource Value Unit (MVS) License + SW Subscription & Support 12 Months	1	93,685.27	16,863.35	110,548.61
D0THSLL	IBM Security Guardium Collector Software Appliance Install License + SW Subscription & Support 12 Months	2	8,693.66	1,564.86	10,258.52
D1E0JLL	IBM Security Guardium Vulnerability Assessment for Databases Resource Value Unit (MVS) License + SW Subscription & Support 12 Months	1	10,345.35	1,862.16	12,207.51
		Total software en S/			**133,014.65**

https://www-03.ibm.com/software/products/es/ibm-security-guardium-data-activity-monitor