INFORME TÉCNICO N° 00001-2014-1550-SUNAT/4E0100

A	:	**Sra. MARÍA DEL ROSARIO CARRANZA UGARTE** Gerente Administrativo
DE	:	**Sr. ISAAC ERNESTO BRINGAS MASGO** Jefe de la Oficina de Seguridad Informática (e)
ASUNTO	:	Solicita estandarización para la provisión de herramienta de monitoreo y auditoría en tiempo real de Base de Datos, de la marca IBM Guardium.
REF	:	a) Informe Técnico N° 005-2013-3358/4E0100 b) Acta de Reunión del 17-set-13
FECHA	:	Lima, 27 de febrero de 2014

1. MATERIA

La SUNAT dentro del objetivo estratégico de brindar servicio de calidad para facilitar y fomentar el cumplimiento voluntario, requiere contar con herramientas de seguridad que garanticen la calidad y seguridad de la información que SUNAT procesa.

En este contexto, con la finalidad de contar con una solución que permita el registro de la interacción que tenga el personal de SUNAT con las bases de datos institucionales, es necesario la provisión de la herramienta IBM Guardium que por sus especificaciones técnicas, permite realizar el monitoreo y auditoría en tiempo real de las Base de Datos INFORMIX y ORACLE que son con las que cuenta SUNAT.

2. BASE LEGAL

a. El Decreto Legislativo N° 1017–Ley de Contrataciones del Estado.
b. Decreto Supremo N° 184-2008-EF–Reglamento de la Ley de Contrataciones del Estado.
c. Directiva N° 010-2009-OSCE–CD-Lineamientos para la contratación en la que se hace referencia a determinada marca o tipo particular.

3. ANÁLISIS

De conformidad con la Directiva N° 10-2009-OSCE/CD, se procede a exponer el cumplimiento de los supuestos establecidos en la referida directiva, que sustentan la estandarización para la provisión de herramienta de monitoreo y auditoría en tiempo real de Base de Datos, de la marca IBM Guardium.

3.1. Descripción del Equipamiento preexistente.-

La SUNAT en la actualidad cuenta con catorce (14) servidores IBM AIX y dos (2) motores de Base de Datos comerciales: INFORMIX desde el año 1992 y ORACLE desde el año 1993; ambos motores utilizan el protocolo TCP/IP para permitir la conexión de clientes remotos. Adicionalmente, el motor de base de datos Informix permite la conexión a través de segmentos de memoria (shared memory) para clientes locales (aquellos que establecen la conexión desde el mismo servidor donde se encuentra alojada la BD).

Los catorce SERVIDORES tienen las características indicadas en el Anexo 1

Los motores de Bases de Datos tienen principalmente las características siguientes:

Base de Datos INFORMIX

a. - Replicación asíncrona o continua de la data.

b. - Potente y Escalable.
c. - Mínimo coste de Propiedad.
d. - Soporte de grandes bases de datos.

Base de Datos ORACLE

a. - Es la Base de Soluciones Integradas.
b. - Plataforma de desarrollo fácil y abierto.
c. - Procedimientos Almacenados en Java.
d. - Uno de los motores de Bases de datos más ampliamente difundido en la industria de TI.

3.2. Los bienes que se requiere contratar son accesorios o complementarios al equipamiento preexistente y son imprescindibles para garantizar su funcionalidad, operatividad o valor económico.

La herramienta consiste en una caja especializada para el monitoreo de la actividad de la base de datos, a instalarse en los servidores de SUNAT; es de precisar que por ser una "caja especializada", no es posible separar el bien del software para poder evaluarla independiente; en ese sentido no aplica la formulación del Informe Técnico Previo de Evaluación de Software al que se refiere la Ley N°28612.

Actualmente se carece de un proceso automático que permita la detección de vulnerabilidades en las bases de datos, así como el registro de las acciones que se realizan sobre las mismas, donde se almacena información de los contribuyentes y agentes de comercio exterior que administra SUNAT, sin afectar los motores de base de datos., que en el caso de SUNAT son dos Informix y Oracle

En consecuencia, la provisión de la herramienta de monitoreo y auditoría en tiempo real de Base de Datos, IBM Guardium, deviene en complementario e imprescindible a la infraestructura preexistente al brindar un alto grado de seguridad e integridad y confidencialidad a la información de las base de datos, debido a que a la fecha es la única con la capacidad de capturar y auditar el tráfico de base de datos con las características técnicas (conexión TCP/IP para accesos remotos y de segmentos de memoria –shared memory- para conexiones locales) con las que se cuenta en la institución para ambas BD Informix y Oracle.

3.3. Descripción del bien requerido

Ítem	Componentes para la solución DAM (Database Activity Monitoring)	Cantidad
01	**Prestación Principal** Solución de caja especializada IBM Guardium para el monitoreo de la actividad de la base de datos.	1
	Incluye: • Instalación, configuración e implementación • Capacitación	Incluida
	Prestación Accesoria Soporte de buen funcionamiento	Tres (03) años

a. Características principales

Las cajas especializadas para el monitoreo de la actividad de la base de datos IBM Guardium, cumplen con las funcionalidades que se detallan a continuación para los motores de bases de datos INFORMIX y ORACLE:

(1) Monitorear, capturar y auditar toda actividad sobre la base de datos en tiempo real, incluyendo las actividades de los administradores y las sentencias SELECT que no realizan cambios en la base de datos. Debe incluir toda actividad DML, DDL y DCL.

(2) Analizar, procesar y almacenar toda la actividad registrada de manera segura fuera de los motores de base de datos monitoreados. Se debe incluir el almacenamiento para el registro de la actividad.
(3) Agregar y consolidar las actividades capturadas desde múltiples y heterogéneos DBMSs y poder trabajar con múltiples motores de base de datos (DBMS).
(4) Generar alertas en tiempo real sobre violaciones a las políticas de seguridad o reglas definidas en la solución.
(5) La auditoría no debe realizarse sobre información almacenada en la base de datos a auditar, ni sobre los registros de auditoría que tienen los propios motores de base de datos.
(6) Funcionalidad para detectar vulnerabilidades sobre la base de datos, como por ejemplo: parches faltantes, contraseñas débiles, privilegios mal configurados, y cuentas por defecto en los DBMS.
(7) Funcionalidad, incluida en el producto, que permita auditar los cambios en los objetos de la base de datos, realizados a través de sentencias DDL.
(8) Permitir crear políticas de seguridad o reglas sobre eventos en los DBMS.
(9) Las políticas de seguridad como mínimo deben poder configurarse por usuario, IP y aplicación que originó la actividad SQL; e IP y nombre de la base de datos del servidor de DBMS monitoreado. Asimismo, deberá permitir definir grupos de cualquiera de estos parámetros para utilizarlos en la definición de las políticas.
(10) Las políticas de seguridad o reglas debe permitir el uso de expresiones regulares.
(11) Capacidad de detectar actividades anormales sobre los DBMSs. Es decir detectar patrones que están fuera de la actividad usual diaria del DBMS.
(12) Contar al menos con dos políticas predefinidas desde fábrica.
(13) Las alertas deben poder enviarse por correo, ejecutar algún evento, enviarse a una solución SIEM y enviarse utilizando protocolo Syslog o SNMP a otra solución o dispositivo.
(14) Permitir el monitoreo de usuarios a nivel de aplicación, con el objetivo de conocer qué usuario de aplicación realiza la transacción cuando se utiliza pool de conexiones contra la base de datos.
(15) Debe permitir el bloqueo de QUERIES a la base de datos.
(16) Capturar el nombre de la aplicación desde donde se realizó la conexión a la base de datos o se ejecutó la sentencia SQL, siempre que el driver original del fabricante del manejador de base de datos entregue dicha información.
(17) De utilizar algún agente, éste debe contar con soporte para el sistema operativo AIX en las versiones 5, 6 y 7.
(18) De utilizar algún agente instalado en el servidor de base de datos a monitorear, éste deberá poder ser actualizado sin necesidad de reiniciar el servidor, con el objetivo de minimizar el impacto en la disponibilidad de la base de datos.
(19) Permitir auditar los motores de base de datos INFORMIX y ORACLE instalados en las versiones del sistema operativo AIX indicados en el numeral anterior.
(20) Capturar y auditar el tráfico de base de datos que viaja a través del puerto de red configurado en el servidor UNIX al DBMS.
(21) Debe incluir, como mínimo, los roles de administrador de la solución, de usuario, de administrador de usuarios, y de auditor. Asimismo, se deberá poder crear nuevos roles.
(22) Los usuarios podrán ser asignados a uno o más de los roles existente.
(23) Permitir el monitoreo de cambios a archivos externos de la base de datos, por ejemplo, archivos planos y de configuración, registros en el Windows Registry o variables de ambiente
(24) Permitir buscar diferentes instancias de base de datos en diferentes segmentos IP, escanear las IP y puertos hasta que se encuentre bases de datos en la red para identificarlas.
(25) Permitir identificar, alertar, clasificar el tipo de objeto de las base de datos (Ejemplo: tablas, vistas, index, etc.), esta información se debe poder mostrar en reportes.
(26) Permitir la integración con LDAP para la autenticación y autorización de los usuarios, a su vez debe tener la capacidad de utilizar los grupos del LDAP para la extracción automatizada de usuarios.

FORTALECIMIENTO DE LA ARQUITECTURA INFORMÁTICA - DIRECTOR - JOSÉ SÁNCHEZ ZAMBRANO

(27) Contar con plantillas listas para el cumplimiento de estándares como SOX, PCI, DSS, HIPAA.
(28) Contar con reportes predefinidos con información de los privilegios de los usuarios sobre los objetos la base de datos.
(29) Si la solución utiliza agentes para el monitoreo, esta debe contar con un sistema de administración de agentes que permitan instalar, actualizar y desinstalar.
(30) Si la solución utiliza agentes debe permitir un despliegue masivo automático a través de la red.
(31) Capturar y auditar el tráfico de base de datos que se intercambia en la memoria compartida (Shared Memory) configurado en el servidor UNIX al DBMS INFORMIX y ORACLE.
(32) Para sistemas operativos UNIX, debe mostrar al usuario real que se conectó al sistema operativo y que mediante comando del sistema operativo (por ejemplo, "su") tomó otra identidad para conectarse al DBMS.

3.4. El uso o aplicación que se le dará al bien requerido.-
Detección en tiempo real de vulnerabilidades en las bases de datos Informix y Oracle y registro de las acciones que se realizan sobre las mismas.

3.5. La justificación de la estandarización.-
(1) La implementación de la herramienta IBM Guardium, permite monitorear y auditar las transacciones u operaciones de las bases de datos que se intercambian en la memoria compartida (shared memory) configurado en los servidores UNIX de la institución para las bases de datos Informix y Oracle.
(2) Preservar la información de las Bases de Datos de la SUNAT, a través de una herramienta que permita brindar seguridad, integridad y confidencialidad a la información.
(3) La herramienta IBM Guardium, permite monitorear y auditar ambas bases de datos, optimizando el tiempo para su gestión a través de una sola interface.
(4) Especializar al personal técnico de la Oficina de Seguridad Informática en la instalación, administración, operación y soporte de esta herramienta, para facilitar los periodos de estabilización de la solución informática.
(5) Reducción de potenciales violaciones a las políticas de seguridad, generando un efecto disuasivo para operaciones no autorizadas de la información.

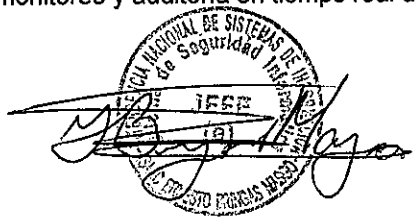
3.6. Nombre, cargo y firma del jefe del área usuaria responsable de la evaluación que sustenta la estandarización del bien o servicio

Nombre : **Isaac Ernesto Bringas Masgo**
Registro : 1550
Cargo : Jefe (e) Oficina de Seguridad Informática

FORTALECIMIENTO DE LA ARQUITECTURA INFORMÁTICA
DIRECTOR
JOSE SANCHEZ ZAMBRANO

4. VIGENCIA
Tres (3) años, sin embargo de variar las condiciones técnicas o tecnológicas que determinan esta estandarización, esta aprobación podría quedar sin efecto, debiéndose realizar un nuevo estudio.

5. RECOMENDACIÓN
En base a lo señalado y teniendo en cuenta la Directiva N° 010-2009-OSCE–CD-Lineamientos para la contratación en la que se hace referencia a determinada marca o tipo particular, se recomienda la estandarización para la provisión de la herramienta de monitoreo y auditoría en tiempo real de Base de Datos, de la marca IBM Guardium



Anexo 1

SERVIDORES

Servidor 1: P795 4GHz

Servidor lógico	Cores	# Instancias
Partición 1 (Informix)	7.8	1
Partición 7 (Informix)	2.6	3
Partición 8 (Informix)	5.2	1
Part 10 (Cont. Srv 2 P1)	5.2	1
Part 11 (Cont. Srv 2 P2)	1.9	1
Part 15 (Cont. Srv 2 P7)	5.2	1
Part 16 (Cont. Srv 2 P8)	5.2	1
Part 17 (Cont. Srv 2 P9)	1.3	1
[illegible]	[illegible]	5
[illegible]	[illegible]	4
[illegible]	[illegible]	1
[illegible]	[illegible]	6
[illegible]	[illegible]	4
[illegible]	[illegible]	2
[illegible]	[illegible]	1
[illegible]	[illegible]	4
[illegible]	[illegible]	4
[illegible]	[illegible]	

70.1

Servidor 2: P795 4GHz

Servidor lógico	Cores	# Instancias
Partición 1 (Informix)	5.2	1
Partición 2 (Informix)	1.9	1
Partición 7 (Informix)	5.2	1
Partición 8 (Informix)	5.2	1
Partición 9 (Informix)	1.3	1
Part 13 (Cont. Srv 1 P1)	7.8	1
Part 18 (Cont. Srv 1 P7)	2.6	3
Part 19 (Cont. Srv 1 P8)	5.2	1
Partición 3 (Informix)	1.9	2
Partición 4 (Informix)	3.9	2
Partición 5 (Informix)	3.9	0
Partición 6 (Informix)	3.9	1
Partición 10 (Informix)	3.9	4
Partición 11 (Informix)	3.9	6
Part 14 (Cont. Srv 1 P2)	3.9	4
Part 15 (Cont. Srv 1 P3)	3.9	3
Part 16 (Cont. Srv 1 P5)	3.9	1
Part 17 (Cont. Srv 1 P6)	3.9	1

71.4

Servidor 3: P740

Servidor lógico	Cores	# Instancias
Partición 1 (Oracle)	3.8	1
Part 2 (Cont. Srv 5 P1) y (Cont. Srv 6 P2)	3	3
Part 3 (Cont. Srv 6 P3)	3.2	19

10

Servidor 4: P740

Servidor lógico	Cores	# Instancias
Partición 1 (Oracle)	4	1
Partición 2 (Oracle) y (Cont. Srv 8 P1)	2.5	3
Partición 3 (Oracle)	3.2	19

9.7

Servidor 5: P740

Servidor lógico	Cores	# Instancias
Part 1 (Cont. Srv 7 P2)	3	5
Partición 2 (Oracle)	3.8	1

6.8

Servidor 6: P740

Servidor lógico	Cores	# Instancias
Part 1 (Cont. Srv 9 P2)	2.5	1
Partición 2 (Oracle)	4	5

6.5

Servidor 7: P740

Servidor lógico	Cores	# Instancias
Informix	2	2
Oracle		2

Servidor 8: P520 (EssaOnp1)

Servidor físico	Cores	# Instancias
Informix	4	3

Servidor 9: P520 (Sigadm01)

Servidor físico	Cores	# Instancias
Oracle	4	1

Servidor 10: P520 (Sigads01)

Servidor físico	Cores	# Instancias
1 Oracle-Enterprise 2 Oracle-Estandar	4	3

Servidor 11: P520 (ONP1)

Servidor físico	Cores	# Instancias
Informix	4	1

Servidor 12: P520 (ESSALUD1)

Servidor físico	Cores	# Instancias
Informix	4	1

Servidor 13: P740 (Insumos)

Servidor lógico	Cores	# Instancias
Partición 1 (Informix)	2	1

Servidor 14: P740 (Insumos)

Servidor lógico	Cores	# Instancias
Partición 1 (Informix)	2	1

FORTALECIMIENTO DE LA ARQUITECTURA INFORMÁTICA - DIRECTOR - JOSÉ SÁNCHEZ ZAMBRANO

SUNAT
INTENDENCIA NACIONAL DE ADMINISTRACIÓN
GERENCIA ADMINISTRATIVA
28 FEB. 2014
RECIBIDO
Reg. N° | Hora 10:07 | Firma

INFORME N° 015-2014-SUNAT/4G3400

A : **Sra. MARIA DEL ROSARIO CARRANZA UGARTE**
Gerente Administrativo

DE : **Sr. JUAN CARLOS CIELO FLORES**
Jefe de la División de Programación y Gestión (e)

ASUNTO : Estandarización para la provisión de herramienta de monitoreo y auditoría en tiempo real de Base de Datos, de la marca IBM Guardium.

REF. : Informe Técnico N°001-2014-1550-SUNAT/4E0100

FECHA : Lima, 27 de febrero de 2014

---

1. ANTECEDENTES

Informe Técnico N°001-2014-1550-SUNAT/4E0100 de la Oficina de Seguridad Informática.

2. OBJETIVO

Verificar si procede estandarizar la provisión de herramienta de monitoreo y auditoría en tiempo real de Base de Datos, de la marca IBM Guardium comprobando si el Informe señalado en los antecedentes, permite concluir que resulta inevitable contratar ésta provisión en la medida que garantiza la funcionalidad, operatividad o valor económico del equipamiento o infraestructura preexistente en la SUNAT.

3. BASE LEGAL

a. El Decreto Legislativo N° 1017–Ley de Contrataciones del Estado.
b. Decreto Supremo N° 184-2008-EF–Reglamento de la Ley de Contrataciones del Estado.
c. Directiva N° 010-2009-OSCE–CD-Lineamientos para la contratación en la que se hace referencia a determinada marca o tipo particular.

4. ANÁLISIS

De conformidad con la Directiva N° 10-2009-OSCE/CD, para comprobar la procedencia de estandarizar la provisión de herramienta de monitoreo y auditoría en tiempo real de Base de Datos, de la marca IBM Guardium, deben cumplirse los supuestos establecidos y estar expresados en el contenido del Informe.

GERENCIA ADMINISTRATIVA – División de Programación y Gestión – JEFE (e) – JUAN CARLOS CIELO FLORES

4.1 Supuestos que deben cumplirse para la estandarización

a. Informe Técnico Previo de Evaluación de Software

De conformidad con el art° 6 del Reglamento de Ley N° 28612 que Norma el uso, adquisición y adecuación de software en la administración pública: *"Toda adquisición y uso de licencias de software que pretenda ser llevada a cabo por una Entidad del Estado requerirá un Informe Técnico Previo de Evaluación de Software, que debe ser emitido por el área informática, o la que haga sus veces en la institución"*. . Asimismo, *"De ser el caso, el* ***Informe Técnico Previo de Evaluación de Software****, formará parte de los procesos de estandarización o exoneración…."*

Respecto a ello, el Informe sustenta que la herramienta consiste en una caja especializada para el monitoreo de la actividad de la base de datos, a instalarse en los servidores de SUNAT; precisando que al ser una "caja especializada", no es posible separar el bien del software para poder evaluarla independiente; en ese sentido, se concluye **que no aplica la formulación del Informe Técnico Previo de Evaluación de Software al que se refiere la Ley N°28612.**

b. Preexistencia de equipamiento o infraestructura.-
La SUNAT en la actualidad cuenta con catorce (14) servidores IBM AIX y dos (2) motores de Base de Datos comerciales: INFORMIX desde el año 1992 y ORACLE desde el año 1993; ambos motores utilizan el protocolo TCP/IP para permitir la conexión de clientes remotos.
Estos componentes conforman la infraestructura preexistente en la que se instalará la herramienta IBM Guardium.

c. Los bienes que se requieren contratar son accesorios o complementarios al equipamiento o infraestructura preexistente y son imprescindibles para garantizar su funcionalidad, operatividad o valor económico.-
Se carece de un proceso automático que permita la detección de vulnerabilidades en las bases de datos, así como el registro de las acciones que se realizan sobre las mismas, donde se almacena información de los contribuyentes y agentes de comercio exterior que administra SUNAT.

La herramienta IBM Guardium, deviene en complementaria e imprescindible a la infraestructura preexistente al brindar un alto grado de seguridad e integridad y confidencialidad a la información de las base de datos, debido a que a la fecha es la única con la capacidad de capturar y auditar el tráfico de base de datos con las características técnicas (conexión TCP/IP para accesos remotos y de segmentos de memoria –shared memory- para conexiones locales) con las que se cuenta en la institución para ambas BD Informix y Oracle.

4.2. Contenido del Informe

a. La descripción de la infraestructura preexistente.-
Los catorce **SERVIDORES** tienen las características siguientes:

GERENCIA ADMINISTRATIVA – División de Programación y Gestión – JEFE (e) – JUAN CARLOS CIELO FLORES

Servidor 1: P795 4GHz

Servidor lógico	Cores	# Instancias
Partición 1 (Informix)	7.8	1
Partición 7 (Informix)	2.6	3
Partición 8 (Informix)	5.2	1
Part 10 (Cont. Srv 2 P1)	5.2	1
Part 11 (Cont. Srv 2 P2)	1.9	1
Part 15 (Cont. Srv 2 P7)	5.2	1
Part 16 (Cont. Srv 2 P8)	5.2	1
Part 17 (Cont. Srv 2 P9)	1.3	1
Partición 2 (Informix)	3.9	5
Partición 3 (Informix)	3.9	4
Partición 4 (Informix)	2.6	1
Partición 5 (Informix)	3.9	6
Partición 6 (Informix)	3.9	4
Part 12 (Cont. Srv 2 P3)	1.9	2
Part 13 (Cont. Srv 2 P4)	3.9	1
Part 14 (Cont. Srv 2 P5)	3.9	4
Part 18 (Cont. Srv 2 P10)	3.9	4
Part 19 (Cont. Srv 2 P11)	3.9	

70.1

Servidor 2: P795 4GHz

Servidor lógico	Cores	# Instancias
Partición 1 (Informix)	5.2	1
Partición 2 (Informix)	1.9	1
Partición 7 (Informix)	5.2	1
Partición 8 (Informix)	5.2	1
Partición 9 (Informix)	1.3	1
Part 13 (Cont. Srv 1 P1)	7.8	1
Part 18 (Cont. Srv 1 P7)	2.6	3
Part 19 (Cont. Srv 1 P8)	5.2	1
Partición 3 (Informix)	1.9	2
Partición 4 (Informix)	3.9	2
Partición 5 (Informix)	3.9	0
Partición 6 (Informix)	3.9	1
Partición 10 (Informix)	3.9	4
Partición 11 (Informix)	3.9	6
Part 14 (Cont. Srv 1 P2)	3.9	4
Part 15 (Cont. Srv 1 P3)	3.9	3
Part 16 (Cont. Srv 1 P5)	3.9	1
Part 17 (Cont. Srv 1 P6)	3.9	1

71.4

Servidor 3: P740

Servidor lógico	Cores	# Instancias
Partición 1 (Oracle)	3.8	1
Part 2 (Cont. Srv 5 P1) y (Cont. Srv 6 P2)	3	3
Part 3 (Cont. Srv 6 P3)	3.2	19

10

Servidor 4: P740

Servidor lógico	Cores	# Instancias
Partición 1 (Oracle)	4	1
Partición 2 (Oracle) y (Cont. Srv 8 P1)	2.5	3
Partición 3 (Oracle)	3.2	19

9.7

Servidor 5: P740

Servidor lógico	Cores	# Instancias
Part 1 (Cont. Srv 7 P2)	3	5
Partición 2 (Oracle)	3.8	1

6.8

Servidor 6: P740

Servidor lógico	Cores	# Instancias
Part 1 (Cont. Srv 9 P2)	2.5	1
Partición 2 (Oracle)	4	5

6.5

Servidor 7: P740

Servidor lógico	Cores	# Instancias
Informix	2	2
Oracle		2

Servidor 8: P520 (EssaOnp1)

Servidor físico	Cores	# Instancias
Informix	4	3

Servidor 9: P520 (Sigadm01)

Servidor físico	Cores	# Instancias
Oracle	4	1

Servidor 10: P520 (Sigads01)

Servidor físico	Cores	# Instancias
1 Oracle-Enterprise 2 Oracle-Estander	4	3

Servidor 11: P520 (ONP1)

Servidor físico	Cores	# Instancias
Informix	4	1

Servidor 12: P520 (ESSALUD1)

Servidor físico	Cores	# Instancias
Informix	4	1

Servidor 13: P740 (Insumos)

Servidor lógico	Cores	# Instancias
Partición 1 (Informix)	2	1

Servidor 14: P740 (Insumos)

Servidor lógico	Cores	# Instancias
Partición 1 (Informix)	2	1

Los motores de Bases de Datos tienen principalmente las características siguientes:
Base de Datos INFORMIX: (1) Replicación asíncrona o continua de la data; (2)- Potente y Escalable; (3) Mínimo coste de Propiedad y (4) Soporte de grandes bases de datos.

Base de Datos ORACLE: (1) Es la Base de Soluciones Integradas, (2) Plataforma de desarrollo fácil y abierto; (3) Procedimientos Almacenados en Java y (4) Uno de los motores de Bases de datos más ampliamente difundido en la industria de TI.

b. El bien requerido, indicándose la marca o tipo de producto; así como términos de referencia.-

Ítem	Componentes para la solución DAM *(Database Activity Monitoring)*	Cantidad
01	**Prestación Principal** Caja especializada IBM Guardium para el monitoreo de la actividad de la base de datos.	1
	Incluye: • Instalación, configuración e implementación • Capacitación	Incluida
	Prestación Accesoria Soporte de buen funcionamiento	Tres (03) años

Características principales
Las cajas especializadas para el monitoreo de la actividad de la base de datos IBM Guardium, cumplen con las funcionalidades que se detallan a continuación para los motores de bases de datos INFORMIX y ORACLE:

(1) Monitorear, capturar y auditar toda actividad sobre la base de datos en tiempo real, incluyendo las actividades de los administradores y las sentencias SELECT que no realizan cambios en la base de datos. Debe incluir toda actividad DML, DDL y DCL.
(2) Analizar, procesar y almacenar toda la actividad registrada de manera segura fuera de los motores de base de datos monitoreados. Se debe incluir el almacenamiento para el registro de la actividad.
(3) Agregar y consolidar las actividades capturadas desde múltiples y heterogéneos DBMSs y poder trabajar con múltiples motores de base de datos (DBMS).
(4) Generar alertas en tiempo real sobre violaciones a las políticas de seguridad o reglas definidas en la solución.
(5) La auditoría no debe realizarse sobre información almacenada en la base de datos a auditar, ni sobre los registros de auditoría que tienen los propios motores de base de datos.
(6) Funcionalidad para detectar vulnerabilidades sobre la base de datos, como por ejemplo: parches faltantes, contraseñas débiles, privilegios mal configurados, y cuentas por defecto en los DBMS.
(7) Funcionalidad, incluida en el producto, que permita auditar los cambios en los objetos de la base de datos, realizados a través de sentencias DDL.

GERENCIA ADMINISTRATIVA
División de Programación y Gestión
JEFE (e)
JUAN CARLOS CIELO FLORES

(8) Permitir crear políticas de seguridad o reglas sobre eventos en los DBMS.
(9) Las políticas de seguridad como mínimo deben poder configurarse por usuario, IP y aplicación que originó la actividad SQL; e IP y nombre de la base de datos del servidor de DBMS monitoreado. Asimismo, deberá permitir definir grupos de cualquiera de estos parámetros para utilizarlos en la definición de las políticas.
(10) Las políticas de seguridad o reglas debe permitir el uso de expresiones regulares.
(11) Capacidad de detectar actividades anormales sobre los DBMSs. Es decir detectar patrones que están fuera de la actividad usual diaria del DBMS.
(12) Contar al menos con dos políticas predefinidas desde fábrica.
(13) Las alertas deben poder enviarse por correo, ejecutar algún evento, enviarse a una solución SIEM y enviarse utilizando protocolo Syslog o SNMP a otra solución o dispositivo.
(14) Permitir el monitoreo de usuarios a nivel de aplicación, con el objetivo de conocer qué usuario de aplicación realiza la transacción cuando se utiliza pool de conexiones contra la base de datos.
(15) Debe permitir el bloqueo de QUERIES a la base de datos.
(16) Capturar el nombre de la aplicación desde donde se realizó la conexión a la base de datos o se ejecutó la sentencia SQL, siempre que el driver original del fabricante del manejador de base de datos entregue dicha información.
(17) De utilizar algún agente, éste debe contar con soporte para el sistema operativo AIX en las versiones 5, 6 y 7.
(18) De utilizar algún agente instalado en el servidor de base de datos a monitorear, éste deberá poder ser actualizado sin necesidad de reiniciar el servidor, con el objetivo de minimizar el impacto en la disponibilidad de la base de datos.
(19) Permitir auditar los motores de base de datos INFORMIX y ORACLE instalados en las versiones del sistema operativo AIX indicados en el numeral anterior.
(20) Capturar y auditar el tráfico de base de datos que viaja a través del puerto de red configurado en el servidor UNIX al DBMS.
(21) Debe incluir, como mínimo, los roles de administrador de la solución, de usuario, de administrador de usuarios, y de auditor. Asimismo, se deberá poder crear nuevos roles.
(22) Los usuarios podrán ser asignados a uno o más de los roles existente.
(23) Permitir el monitoreo de cambios a archivos externos de la base de datos, por ejemplo, archivos planos y de configuración, registros en el Windows Registry o variables de ambiente
(24) Permitir buscar diferentes instancias de base de datos en diferentes segmentos IP, escanear las IP y puertos hasta que se encuentre bases de datos en la red para identificarlas.
(25) Permitir identificar, alertar, clasificar el tipo de objeto de las base de datos (Ejemplo: tablas, vistas, index, etc.), esta información se debe poder mostrar en reportes.
(26) Permitir la integración con LDAP para la autenticación y autorización de los usuarios, a su vez debe tener la capacidad de utilizar los grupos del LDAP para la extracción automatizada de usuarios.
(27) Contar con plantillas listas para el cumplimiento de estándares como SOX, PCI, DSS, HIPAA.
(28) Contar con reportes predefinidos con información de los privilegios de los usuarios sobre los objetos la base de datos.
(29) Si la solución utiliza agentes para el monitoreo, esta debe contar con un sistema de administración de agentes que permitan instalar, actualizar y desinstalar.
(30) Si la solución utiliza agentes debe permitir un despliegue masivo automático a través de la red.

GERENCIA ADMINISTRATIVA
División de Programación y Gestión
JEFE (e)
JUAN CARLOS CIELO FLORES

(31) Capturar y auditar el tráfico de base de datos que se intercambia en la memoria compartida (Shared Memory) configurado en el servidor UNIX al DBMS INFORMIX y ORACLE.
(32) Para sistemas operativos UNIX, debe mostrar al usuario real que se conectó al sistema operativo y que mediante comando del sistema operativo (por ejemplo, "su") tomó otra identidad para conectarse al DBMS.

b. El uso o aplicación que se le dará al bien requerido.-
Detección en tiempo real de vulnerabilidades en las bases de datos Informix y Oracle y registro de las acciones que se realizan sobre las mismas.

c. La justificación de la estandarización.-
(1) La implementación de la herramienta IBM Guardium, permite monitorear y auditar las transacciones u operaciones de las bases de datos que se intercambian en la memoria compartida (shared memory) configurado en los servidores UNIX de la institución para las bases de datos Informix y Oracle.
(2) Preservar la información de las Bases de Datos de la SUNAT, a través de una herramienta que permita brindar seguridad, integridad y confidencialidad a la información.
(3) La herramienta IBM Guardium, permite monitorear y auditar ambas bases de datos, optimizando el tiempo para su gestión a través de una sola interface.
(4) Especializar al personal técnico de la Oficina de Seguridad Informática en la instalación, administración, operación y soporte de esta herramienta, para facilitar los periodos de estabilización de la solución informática.
(5) Reducción de potenciales violaciones a las políticas de seguridad, generando un efecto disuasivo para operaciones no autorizadas de la información.

d. Nombre, cargo y firma de la persona responsable de la evaluación que sustenta la estandarización del bien o servicio y del jefe del área usuaria.

Nombre : **Isaac Ernesto Bringas Masgo**
Registro : 1550
Cargo : Jefe (e) Oficina de Seguridad Informática

c. La fecha de elaboración del informe técnico.
27 de febrero del 2014

5. VIGENCIA
Acorde con lo indicado en el Informe Técnico N°001-2014-1550-SUNAT/4E0100, tres (3) años.

6. CONCLUSIONES
El Informe Técnico N°001-2014-1550-SUNAT/4E0100, contiene y sustenta los supuestos previstos en la Directiva N° 010-2009-OSCE–CD, y en consecuencia procede estandarizar la provisión de herramienta de monitoreo y auditoría en tiempo real de Base de Datos, de la marca IBM Guardium.

7. RECOMENDACIÓN
Recomendar la emisión de la Resolución de Intendencia por la que el Titular de la Intendencia Nacional de Administración apruebe la estandarización para la provisión de herramienta de monitoreo y auditoría en tiempo real de Base de Datos, de la marca IBM Guardium.

Es todo cuanto tengo que informar

GERENCIA ADMINISTRATIVA – División de Programación y Gestión – JEFE (e) – JUAN CARLOS CIELOS FLORES

Juan Carlos Cielos Flores
Jefe División de Programación y Gestión (e)