Firmado Electrónicamente por:
JOHNNY ANTONIO VALDEZ AREVALO
GERENTE
GERENCIA DE ARQUITECTURA
Fecha y hora: 30/05/2022 21:16

INFORME N.º 000002-2022-SUNAT/1U4000

ASUNTO : Informe Técnico de Estandarización de software de monitoreo integral de base de datos de la marca IBM Guardium o equivalente

LUGAR : Lima, 30 de mayo de 2022

SUNAT V° B° 1U4100 REG. 141A
NILTON CESAR MORI LEON
JEFE DE DIVISIÓN
30/05/2022 21:09:03

SUNAT V° B° 1U4100 REG. AL38
JORGE SILVANO GUTIERREZ MENDOZA
30/05/2022 21:07:37

1. MATERIA

Estandarización para la adquisición del software de monitoreo integral de base de datos de la marca IBM Guardium.

2. BASE LEGAL

- LCE – Ley de Contrataciones del Estado y Reglamento vigente.
- Directiva N° 004-2016-OSCE/CD, Lineamientos para la contratación en la que se hace referencia a determinada marca o tipo particular.

3. ANTECEDENTES

La Entidad dispone de una plataforma informática que almacena en sus bases de datos la información de todos sus administrados, lo cual es el soporte operativo para las actividades que la administración debe realizar. Por ello, es de vital importancia que se cuente con mecanismos que permitan mantener segura esta información, garantizando la confidencialidad e integridad de esta.

Actualmente se cuenta con una solución de monitoreo base de datos IBM Guardium, la cual permite la detección de vulnerabilidades en las bases de datos, así como el registro de las acciones que se realizan sobre las mismas, sin afectar los motores de base de datos en producción, que en el caso de SUNAT son tres Informix, Oracle y MongoDB

En consecuencia, la adquisición del software de monitoreo integral de base de datos, IBM Guardium, deviene en complementario e imprescindible para la operación de la infraestructura de servidores de bases de datos que la institución opera a fin de brindar un alto grado de seguridad e integridad y confidencialidad a la información de las base de datos.

Sin embargo, es necesario renovar esta herramienta dado que el contrato anterior ya culminó su prestación y teniendo en consideración lo señalado en el párrafo anterior es necesario extender el tiempo de estandarización de la herramienta por 36 meses más

4. ANÁLISIS

a) Descripción del equipamiento o infraestructura preexistente.

La SUNAT en la actualidad cuenta con treinta y cinco (35) servidores IBM AIX (Ver anexo 1), quince (15) Red Hat Linux (Ver anexo 2) y tres (3) motores de Base de Datos comerciales: INFORMIX desde el año 1992 , ORACLE desde el año 1993 y MongoDB desde el año 2019; ambos motores utilizan el protocolo TCP/IP para permitir la conexión de clientes remotos. Los servidores se encuentran ubicados en los centros de cómputo de la institución (San Isidro y Surco). La relación de servidores puede verse en el Anexo 1.

SUNAT
V° B°
1U4100
REG. 141A
NILTON CESAR MORI LEON
JEFE DE DIVISIÓN
30/05/2022 21:09:03

b) Descripción del bien requerido.

SUNAT
V° B°
1U4100
REG. AL38
JORGE SILVANO GUTIERREZ MENDOZA
30/05/2022 21:07:37

La SUNAT a fin de garantizar la operatividad servicios informáticos e incrementar los recursos para mejorar la velocidad de procesamiento y obtener oportunamente la información solicitada de las áreas usuarias, así como reducir las quejas de los accesos para los usuarios, requiere contar con lo siguiente:

Adquisición de software de monitoreo integral de base de datos de la marca IBM Gardium para los servidores de base de datos por 36 meses (incluye servicio de Soporte y buen funcionamiento)

Para ello deberá cumplir con las características que se detallan a continuación para los motores de bases de datos Informix, Oracle y MongoDB:

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 la actividad de DML, DDL y DCL de las bases de datos incluidas en el alcance definido por la entidad.
2) Debe 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 (mínimo 1 TB).
3) Debe agregar y consolidar las actividades capturadas desde múltiples DBMS.
4) Debe poder trabajar con múltiples motores de base de datos (DBMS).
5) Debe generar alertas en tiempo real sobre violaciones a las políticas de seguridad o reglas definidas en el software.

6) 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.
7) Debe contar con la 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) Debe permitir crear políticas de seguridad o reglas sobre eventos en los DBMS.
9) Las políticas y reglas deberían poder realizarse sobre:
    a. Querys específicos.
    b. Cantidad de filas retornadas al ejecutar sentencias DML.
    c. Funciones administrativas (Creación de usuarios, cambios de privilegios, cambios en Stored Procedures y otros cambios en la configuración).
    d. Detección de incidentes de SQL Injection.
    e. Actualizaciones u otros tipos de transacciones por usuarios sobre el total o grupos de tablas.
    f. Basado en contenido del resultado de la evolución de sentencias DML.

SUNAT
V° B°
1U4100
REG. 141A
NILTON CESAR MORI LEON
JEFE DE DIVISIÓN
30/05/2022 21:09:03

10) 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.
11) Las políticas de seguridad o reglas deben permitir el uso de expresiones regulares.
12) Debe tener la capacidad de detectar actividades anormales sobre los DBMS. Es decir, detectar patrones que están fuera de la actividad usual diaria del DBMS.
13) Debe contar al menos con un par de políticas predefinidas desde fábrica.
14) 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.
15) Debe permitir el bloqueo de queries a la base de datos.
16) Debe capturar el nombre de la aplicación desde donde se realizó la conexión a la base de datos o se ejecutó la sentencia SOL, 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 la versión 7.1 como mínimo.
18) De utilizar algún agente en los servidores de bases de datos, estos no deben sobrepasar el consumo de 10% de CPU.
19) Debe permitir monitorear los motores de base de datos INFORMIX y ORACLE instalados en las versiones del sistema operativo AIX 7.1 como mínimo. Los motores de bases de datos utilizados son: Informix 11.x como mínimo. Oracle 12.x como mínimo.
20) Así también debe permitir monitorear el motor de base de datos no relacional MONGODB versión 4.0.x como mínimo e instalado en la versión del sistema operativo RedHat Linux Enterprise 7
21) Debe poder capturar y auditar el tráfico de base de datos que viaja a través del puerto de red configurado en el servidor UNIX al DBMS.
22) Debe incluir, como mínimo, los roles de administrador de la herramienta, de usuario, de administrador de usuarios, y de auditor.

SUNAT
V° B°
1U4100
REG. AL38
JORGE SILVANO GUTIERREZ MENDOZA
30/05/2022 21:07:37

Asimismo, se deberá poder crear nuevos roles. Los usuarios podrán ser asignados a uno o más de los roles existente.

23) Debe 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.
24) Debe 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.
25) Debe contar con plantillas listas para el cumplimiento de estándares como SOX, PCI, DSS, HIPAA.
26) Si la herramienta utiliza agentes para el monitoreo, esta debe contar con un sistema de administración de agentes que permitan instalar, actualizar y desinstalar.
27) Si la herramienta utiliza agentes debe permitir un despliegue masivo automático a través de la red.
28) Debe poder 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.
29) 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.
30) Todos los componentes de la herramienta deben contar con un 99.5% de disponibilidad.
31) La solución debe permitir exportar toda la información de un día especifico colectada en formato texto y/o csv y/o pdf

SUNAT V° B° 1U4100 REG. 141A
NILTON CESAR MORI LEON
JEFE DE DIVISIÓN
30/05/2022 21:09:03

c) Uso o aplicación que se le dará al bien requerido.

El software a adquirir será utilizado para realizar las acciones que permitan garantizar la seguridad de la información, proporcionando capacidades de monitoreo y auditoría en tiempo real.

SUNAT V° B° 1U4100 REG. AL38
JORGE SILVANO GUTIERREZ MENDOZA
30/05/2022 21:07:37

d) Justificación de la estandarización.

(1) La Entidad posee determinado equipamiento o infraestructura.

De acuerdo con lo indicado en el literal a) Descripción del equipamiento o infraestructura preexistente”.

(2) Los bienes que se requieren contratar son accesorios o complementarios al equipamiento preexistente.

La adquisición del software de monitoreo integral de base de datos de la marca IBM Guardium es una herramienta complementaria a la infraestructura preexistente, en razón que dicha provisión le da sostenibilidad al uso de la misma y éstos únicamente pueden ser brindados por el fabricante, distribuidores o partner autorizados del fabricante de los productos en razón que, como propietarios y desarrolladores del hardware y software, son los únicos en proveer las actualizaciones, así como respaldar con el escalamiento las atenciones del servicio de soporte

(3) Los bienes que se requieren contratar son imprescindibles

Si no se cuenta con el software de monitoreo integral de base de datos de la marca IBM Guardium no se podrá garantizar la confidencialidad e integridad de la información que se encuentra en las bases de datos de la Entidad que se encuentran detallados en el literal a) Descripción del equipamiento o infraestructura preexistente". lo que ocasionaría que los sistemas informáticos de la SUNAT sean más vulnerables y que ante un evento de alteración o fuga de información no se podría determinar la causa raíz.

El software de monitoreo integral de base de datos IBM Guardium, fue elegida por la institución dado que es la única herramienta existente en el mercado que es compatible con la base de datos Informix 11.7 mínimo, base de datos que solicita la institución como requisito obligatorio de interoperabilidad, considerando que en esta versión se encuentran las bases de datos de negocio tributario que dan soporte a las dependencias de SNATI.

En consecuencia, resulta imprescindible la contratación de esta herramienta únicamente a través de los canales, representantes o partner o directamente del fabricante.

SUNAT
V° B°
1U4100
REG. 141A
NILTON CESAR MORI LEON
JEFE DE DIVISIÓN
30/05/2022 21:09:03

(4) Consecuencias de no contar con el software de monitoreo integral de base de datos de la marca IBM Guardium

El software de monitoreo integral de base de datos de la marca IBM Guardium, brinda un alto grado de seguridad e integridad y confidencialidad a la información de las base de datos de la SUNAT, son el fabricante o distribuidores o partners autorizados de la marca IBM Guardium, no se contaría con actualizaciones en hardware y software, así como el respaldo en el escalamiento de atenciones del servicio de soporte y lo cual implicaría que se tengan que desarrollar mecanismos manuales de monitoreo los cuales pueden afectar la disponibilidad de los servicios por el consumo de recursos informáticos que demandarían

SUNAT
V° B°
1U4100
REG. AL38
JORGE SILVANO GUTIERREZ MENDOZA
30/05/2022 21:07:37

(5) Incidencia Económica de la Contratación

Prescindir del software de monitoreo integral de base de datos de la marca IBM Guardium, afectaría a los servicios que brinda la SUNAT lo que se traduciría en pérdidas para el país en la recaudación de tributos y facilitación de las actividades de comercio exterior.

5. VIGENCIA

Treinta y seis (36) meses, sin embargo, de variar las condiciones técnicas o tecnológicas que determinan esta estandarización, esta aprobación puede quedar sin efecto.

6. RESPONSABLE DE LA ELABORACIÓN Y EVALUACIÓN

El funcionario *mínimo de tercer nivel* es quien evalúa y suscribe el Informe de Estandarización.

6.1.	**RESPONSABLE DE LA ELABORACIÓN DEL INFORME**	
	APELLIDOS Y NOMBRES	**GUTIERREZ MENDOZA JORGE SILVANO**
	REGISTRO SUNAT	**AL38**
	CARGO	**ARQUITECTO TI SENIOR**
	UNIDAD ORGÁNICA	**1U4100**

6.2.	**RESPONSABLE DE LA EVALUACIÓN DEL INFORME**	
	APELLIDOS Y NOMBRES	**MORI LEON NILTON CESAR**
	REGISTRO SUNAT	**141A**
	CARGO	**JEFE DE DIVISIÓN**
	UNIDAD ORGÁNICA	**1U4100**

7. CONCLUSIÓN

Del análisis realizado se demuestra que la SUNAT tiene la necesidad de contratar el software de monitoreo integral de base de datos de la marca IBM Guardium, para poder contar con mecanismos que permitan brindar seguridad a la información de los contribuyentes y operadores de comercio exterior

La estandarización propuesta no constituye un mecanismo de restricción a la libre competencia, en razón que en el mercado se cuenta con más de un canal o partner autorizados por el fabricante.

SUNAT
V° B°
1U4100
REG. 141A
NILTON CESAR MORI LEON
JEFE DE DIVISIÓN
30/05/2022 21:09:03

8. RECOMENDACIÓN

En base a lo señalado y teniendo en cuenta la Directiva N° 004-2016-OSCE/CD, Lineamientos para la contratación en la que se hace referencia a determinada marca o tipo particular; se recomienda dar inicio al proceso de estandarización.

SUNAT
V° B°
1U4100
REG. AL38
JORGE SILVANO GUTIERREZ MENDOZA
30/05/2022 21:07:37

ANEXO Nº 1

N°	Informix	N°	Oracle
1	INFP03S1	25	ORAP01S2
2	INFP05S1	26	ORAP06S1
3	INFP06S1	27	ORAP01S4
4	INFP10S1	28	ORAP01S5
5	INFP14S1	29	ORAP02S4
6	INFP18S1	30	ORPP02S5
7	INFP22S1	31	ORAP03S4
8	INFP25S1	32	ORAP03S5
9	INFP01S2	33	ORAP04S4
10	INFP02S2	34	ORAP04S5
11	INFP03S2	35	ORAP05S5
12	INFP04S2		
13	INFP07S2		
14	INFP08S2		
15	INFP11S2		
16	INFP13S2		
17	INFP14S2		
18	INFP1552		
19	INFP16S2		
20	INFP18S2		
21	INFP20S2		
22	INFP21S2		
23	INFP26S2		
24	INFP29S2		

SUNAT
V° B°
1U4100
REG. 141A
NILTON CESAR MORI LEON
JEFE DE DIVISIÓN
30/05/2022 21:09:03

SUNAT
V° B°
1U4100
REG. AL38
JORGE SILVANO GUTIERREZ MENDOZA
30/05/2022 21:07:37

ANEXO Nº 2

N°	MongoDB
1	S00PLXBMDB014
2	S00PLXBMDB015
3	S00PLXBMDB016
4	S00PLXBMDB016
5	S01PLXBMDB017
6	S00PLXBMDB017
7	S00PLXBMDB018
8	S00PLXBMDB019
9	S01PLXBMDB018
10	S01PLXBMDB019
11	S00PLXBMDB020
12	S00PLXBMDB021
13	S00PLXBMDB022
14	S01PLXBMDB020
15	S01PLXBMDB021

SUNAT
V° B°
1U4100
REG. 141A
NILTON CESAR MORI LEON
JEFE DE DIVISIÓN
30/05/2022 21:09:03

SUNAT
V° B°
1U4100
REG. AL38
JORGE SILVANO GUTIERREZ MENDOZA
30/05/2022 21:07:37