Firmado Digitalmente por:
HERMES FERNANDO AGUILAR CACERES
JEFE DE DIVISIÓN
DIVISIÓN DE PROGRAMACIÓN Y GESTIÓN
Fecha y hora: 31/05/2022 16:09

INFORME N.º 000043-2022-SUNAT/8B7100

A : **ORDOÑEZ ENRIQUEZ MAGALY**
GERENCIA DE GESTIÓN DE CONTRATACIONES

DE : **AGUILAR CACERES HERMES FERNANDO**
DIVISIÓN DE PROGRAMACIÓN Y GESTIÓN

ASUNTO : Estandarización para sustentar la adquisición del software de monitoreo integral de base de datos de la marca IBM Guardium

LUGAR : Lima, 31 de mayo de 2022

SUNAT
V° B°
8B7101
REG. 2259
ROBERTO CARLOS ARREDONDO GALLEGOS
SUPERVISOR ENCARGADO
31/05/2022 16:07:55

---

1. Antecedentes

Mediante el Informe N.º 000002-2022-SUNAT/1U4000, la Gerencia de Arquitectura, sustenta la estandarización para la adquisición del software de monitoreo integral de base de datos de la marca IBM Guardium.

2. Objetivo

Verificar si el Informe, señalado en los antecedentes, permite concluir que resulta imprescindible contratar dicho bien haciendo referencia a una marca, con el objetivo de que la Intendencia Nacional de Administración apruebe el proceso de estandarización.

3. Base Legal

a. Texto Único Ordenado de la Ley N° 30225, Ley de Contrataciones del Estado.
b. Decreto Supremo N° 344-2018-EF, Reglamento de la Ley de Contrataciones del Estado y modificatorias.
c. Directiva N° 004-2016-OSCE–CD - Lineamientos para la contratación en la que se hace referencia a determinada marca o tipo particular.

4. Análisis

4.1 Sobre el proceso de estandarización para la adquisición del software de monitoreo integral de base de datos de la marca IBM Guardium.

En el Informe N.º 000002-2022-SUNAT/1U4000, la Gerencia de Arquitectura, sustenta el cumplimiento de los siguientes presupuestos:

4.1.1 **La Entidad posee determinado equipamiento o infraestructura preexistente.**

El Anexo 1 del Reglamento de la Ley de Contrataciones del Estado, define **Estandarización** como el “Proceso de racionalización consistente en ajustar a un determinado tipo o modelo los bienes o servicios a contratar, en atención a los equipamientos preexistentes”.

Conforme se indica en el literal a) del numeral 4., del Informe N.º 000002-2022-SUNAT/1U4000:

“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)"

4.1.2 **Descripción de los bienes requeridos**

En el literal b), del numeral 4, del Informe N° 000002-2022-SUNAT/1U4000, se señala:

“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.

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. 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."

4.1.3 **Uso o aplicación que se le dará al bien requerido.**

En el literal c), del numeral 4, del Informe N° 000002-2022-SUNAT/1U4000 se indica lo siguiente:

"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".

4.2 **<u>Justificación de la Estandarización</u>**

Conforme se precisa en el literal d), del numeral 4, del Informe N° 000002 - 2022-SUNAT/1U4000:

(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°
8B7101
REG. 2259
ROBERTO CARLOS ARREDONDO GALLEGOS
SUPERVISOR ENCARGADO
31/05/2022 16:07:55

(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".

(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".

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.

5.1.	**RESPONSABLE DE LA ELABORACIÓN DEL INFORME**	
	APELLIDOS Y NOMBRES	Jorge Silvano Gutierrez Mendoza
	REGISTRO SUNAT	AL38
	CARGO	Arquitecto TI Senior
	UNIDAD ORGANIZACIONAL	1U4100 División de Arquitectura de Información y Aplicaciones

5.2.	**RESPONSABLE DE LA EVALUACIÓN DEL INFORME**	
	APELLIDOS Y NOMBRES	Nilton César Mori León
	REGISTRO SUNAT	141A
	CARGO	Jefe de la División de Arquitectura de la Información y Aplicaciones
	UNIDAD ORGANIZACIONAL	1U4100 – División de Arquitectura de Información y Aplicaciones

Fecha de Elaboración del Informe
Lima, 30 de mayo de 2022

5. Conclusiones

El informe Técnico presentado por la unidad orgánica sustenta con criterio técnico y objetivo que la estandarización para la adquisición del software de monitoreo integral de base de datos de la marca IBM Guardium resultan complementarios e imprescindibles para garantizar la funcionalidad, operatividad o valor económico de la infraestructura preexistente.

El Informe N° 000002-2022-SUNAT/1U4000, referido a la estandarización para la adquisición del software de monitoreo integral de base de datos de la marca IBM Guardium fue elaborado por el señor Jorge Silvano Gutierrez Mendoza, Arquitecto TI Senior de la División de Arquitectura de la Información y Aplicaciones y evaluado por el señor Nilton César Mori León, jefe de la División de Arquitectura de la Información y Aplicaciones.

Finalmente, cabe precisar que, según lo indicado en el Informe de la referencia, se confirma que esta estandarización 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°
8B7101
REG. 2259
ROBERTO CARLOS ARREDONDO GALLEGOS
SUPERVISOR ENCARGADO
31/05/2022 16:07:55

6. Recomendación

Considerando lo señalado en los antecedentes, objetivo, análisis de los aspectos técnicos y formales, así como lo dispuesto en la Directiva N° 04-2016-OSCE–CD - Lineamientos para la contratación en la que se hace referencia a determinada marca o tipo particular, se recomienda la estandarización para la adquisición del software de monitoreo integral de base de datos de la marca IBM Guardium por un periodo de treinta y seis (36) meses; sin embargo, de variar las condiciones que determinan esta estandarización, su aprobación quedará sin efecto.

Es todo cuanto tengo que informar.

Hermes Fernando Aguilar Cáceres
Jefe de la División de Programación y Gestión