REPUBLICA DEL PERU

SUNAT

RESOLUCIÓN DE INTENDENCIA

No. 52 -2019/SUNAT/8B0000

CARMEN SALARIO BRAMONT
Intendente Nacional
INTENDENTE NACIONAL DE ADMINISTRACIÓN

APRUEBA ESTANDARIZACIÓN PARA LA CONTRATACIÓN DE LA PROVISIÓN DE LA HERRAMIENTA DE MONITOREO Y AUDITORIA EN TIEMPO REAL DE LA BASE DE DATOS DE LA MARCA IBM GUARDIUM

Lima, 04 JUN. 2019

VISTOS:

El Informe Técnico de Estandarización N°04-2019-SUNAT/1U0100 de la Oficina de Seguridad Informática, el Informe N°31-2019-SUNAT/8B1100 de la División de Programación y Gestión, y el Memorándum N°191-2019-SUNAT/8B1000 de la Gerencia Administrativa, y;

CONSIDERANDO:

Que, de acuerdo con el numeral 6.2 del artículo 6 del Texto Único Ordenado de la Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 006-2017-JUS, el acto administrativo puede motivarse mediante la declaración de conformidad con los fundamentos y conclusiones de anteriores dictámenes, decisiones o informes obrantes en el expediente, a condición de que se les identifique de modo certero, y que por esta situación constituyan parte integrante del respectivo acto;

INTENDENCIA NACIONAL DE ADMINISTRACIÓN Gerencia Administrativa GERENTE FELIPE OSWALDO PANTA CAMPOS

De conformidad con los fundamentos y conclusiones contenidos en el Informe Técnico de Estandarización N°04-2019-SUNAT/1U0100 y el Informe N°31-2019-SUNAT/8B1100, que se adjuntan y forman parte de la presente resolución, y;

En aplicación de lo dispuesto en el artículo 29°, numeral 29.4, del Reglamento de la Ley de Contrataciones del Estado, aprobado mediante Decreto Supremo N°344-2018-EF y de conformidad con los lineamientos establecidos en la Directiva N°004-2016-OSCE/CD; y, en uso de las facultades conferidas mediante Resolución de Superintendencia N°110-2019/SUNAT;

SE RESUELVE:

ARTÍCULO PRIMERO.- APROBAR la estandarización para la contratación de la provisión de la herramienta de monitoreo y auditoria en tiempo real de la base de datos de la marca IBM Guardium, por un periodo de treinta y seis (36) meses; dicha vigencia se mantendrá siempre que no varíen las condiciones que determinaron la presente estandarización.

ARTÍCULO SEGUNDO.- DISPONER que la División de Programación y Gestión, publique la presente resolución junto con los informes que forman parte de la misma, en la página web Institucional, al día siguiente de producida su aprobación.

Regístrese y comuníquese.

CARMEN SALARDI BRAMONT
Intendente Nacional
INTENDENTE NACIONAL DE ADMINISTRACIÓN

INTENDENCIA NACIONAL DE ADMINISTRACIÓN
Gerencia Administrativa
GERENTE
FELIPE OSWALDO PANTA CAMPOS

MEMORANDUM N° 191-2019-SUNAT/8B1000

A : **CARMEN SALARDI BRAMONT**
Intendente Nacional de Administración

DE : **FELIPE OSWALDO PANTA CAMPOS**
Gerente Administrativo

ASUNTO : Estandarización para la contratación de la provisión de la herramienta de monitoreo y auditoria en tiempo real de la base de datos de la marca IBM Guardium

REFERENCIA : a) Informe Técnico de Estandarización N° 04 - 2019-SUNAT/1U0100
b) Memorándum N° 010-2019-SUNAT/1U0100
c) Informe N° 31-2019-SUNAT/8B1100

FECHA : Lima, 03 JUN. 2019

Me dirijo a usted, a fin de hacer de su conocimiento que mediante Informe Técnico de estandarización de la referencia a), elevado mediante documento de la referencia b), la Oficina de Seguridad Informática, sustentó la necesidad de realizar el proceso de estandarización para la provisión de la herramienta de monitoreo y auditoria en tiempo real de la base de datos de la marca IBM Guardium.

En virtud a lo señalado en el informe de la referencia c), la División de Programación y Gestión, recomendó la aprobación de la estandarización solicitada, mediante documento de la referencia a), el mismo que cuenta con opinión favorable de esta Gerencia, habiéndose justificado la estandarización acorde con lo dispuesto en la Directiva N° 004-2016-OSCE/CD – *"Lineamientos para la contratación en la que se hace referencia a determinada marca o tipo particular"*.

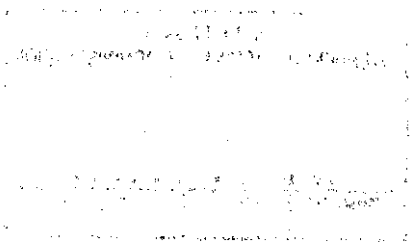
En este sentido, se remite el proyecto de Resolución de Intendencia y los documentos que sustentan la misma, para la aprobación correspondiente.

Atentamente,

FELIPE OSWALDO PANTA CAMPOS
Gerente Administrativo
INTENDENCIA NACIONAL DE ADMINISTRACIÓN

SUNAT
INTENDENCIA NACIONAL DE ADMINISTRACIÓN
04 JUN. 2019
RECIBIDO
Reg. N° | Hora | Firma

FPC/FAC/RAG/dcf.
c.c.: División de Programación y Gestión



INFORME N° 31-2019-SUNAT/8B1100

A	:	**FELIPE OSWALDO PANTA CAMPOS** Gerente Administrativo
DE	:	**HERMES FERNANDO AGUILAR CACERES** Jefe de la División de Programación y Gestión
ASUNTO	:	Estandarización para la contratación de la provisión de la herramienta de monitoreo y auditoria en tiempo real de la base de datos de la marca IBM Guardium
REFERENCIA	:	a) Informe Técnico de Estandarización N° 04-2019-SUNAT/1U0100 b) Memorándum N° 010-2019-SUNAT/1U0100
FECHA	:	30 MAYO 2019

1. **Antecedentes**

Mediante el Informe Técnico de Estandarización de la referencia a), la Oficina de Seguridad de Informática, sustenta la estandarización para la contratación de la provisión de la herramienta de monitoreo y auditoria en tiempo real de la base de datos de la marca IBM Guardium.

2. **Objetivo**

Verificar si el Informe, señalado en los antecedentes, permite concluir que resulta inevitable adquirir 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.
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 provisión de la herramienta de monitoreo y auditoria en tiempo real de la base de datos de la marca IBM Guardium.

En el Informe Técnico de Estandarización de la referencia a) la Oficina de Seguridad Informática, 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, entre otros, 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".*

En el numeral 4. literal a, del Informe Técnico de Estandarización, la Oficina de Seguridad Informática, precisa que, la SUNAT cuenta con treinta y cinco (35) servidores IBM AIX y dos motores de base de datos comerciales: uno Informix y otro Oracle.

4.1.2 **Descripción del bien requerido**
Conforme lo indicado en el numeral 4. literal b, del Informe Técnico de Estandarización es para la adquisición de la herramienta de monitoreo y auditoria en tiempo real de base de datos de la marca IBM Guardium para los 35 servidores de base de datos por 36 meses (incluye servicio de soporte y buen funcionamiento).

4.1.3 **Uso o aplicación que se le dará al bien o servicio requerido**
En el numeral 4. literal c, del mencionado Informe Técnico de Estandarización se indica los usos y aplicaciones que se le dará a la herramienta de monitoreo y auditoria en tiempo real de base de datos de la marca IBM Guardium

4.2 **Justificación de la Estandarización**
Los bienes que se requieren contratar son accesorios o complementarios al equipamiento preexistente.

Conforme lo indicado en el Numeral 2 de la Justificación de la estandarización del Informe Técnico de Estandarización de la referencia se argumenta la necesidad de estandarizar, indicando que la herramienta es complementaria a la Infraestructura preexistente, pues da sostenibilidad al uso de la misma y esta únicamente puede ser brindada por el fabricante, distribuidores o partner autorizados por el fabricante, pues son estos los únicos en proveer las actualizaciones, así como respaldar con el escalamiento las atenciones del servicio de soporte.

Los bienes que se requieren contratar son imprescindibles.
Conforme lo indicado en el Numeral 4 de la Justificación de la estandarización del Informe Técnico de Estandarización de la referencia, si no se cuenta con la herramienta indicada no se podrá garantizar la confidencialidad e integridad de la información que se encuentra en la base de datos de la entidad, 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 podrá determinar las causas.
La herramienta de monitoreo y auditoría en tiempo real de Base de datos IBM Guardium, fue elegida por la institución dado que es la única herramienta existente en el mercado capaz de soportar, en el monitoreo que realiza conexiones TCP/IP para accesos remotos y de segmento de memoria shared memory con las que cuenta la institución para las labores realizadas en las bases de datos Informix y Oracle.

GERENCIA ADMINISTRATIVA – División de Programación y Gestión – VºBº – HERMES FERNANDO AGUILAR CARRASCO

SUPERVISOR (e)

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

Incidencia Económica de la prestación
Conforme lo indicado en el Numeral 3 de la Justificación de la estandarización del Informe Técnico de Estandarización de la referencia "El no contratar con la provisión y soporte de la herramienta de monitoreo y auditoria en tiempo real de la base de datos de la marca IBM Guardium, para brindar un alto grado de seguridad e integridad y confidencialidad a la información de las base de datos de la SUNAT, con 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 y que 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. **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 : Omar Gonzales Elías
Registro : 1559
Cargo : Jefe de la Oficina de Seguridad Informática

Nombre : Omar Gonzales Elías
Registro : 1559
Cargo : Jefe de la Oficina de Seguridad Informática

Fecha de Elaboración del Informe
23 de Mayo de 2019

6. **Conclusiones**
El Informe Técnico de Estandarización presentado por la unidad orgánica sustenta con criterio técnico y objetivo que la contratación de la provisión de la herramienta de monitoreo y auditoria en tiempo real de la base de datos de la marca IBM Guardium resulta complementario e imprescindible a la infraestructura preexistente.

El Informe Técnico de Estandarización N° 04-2019-SUNAT/1U0100, referido a la estandarización para la provisión de la herramienta de monitoreo y auditoria en tiempo real de la base de datos de la marca IBM Guardium fue evaluado y aprobado por el señor Omar Gonzáles Elías, jefe de la Oficina de Seguridad Informática.

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.

GERENCIA ADMINISTRATIVA - División de Programación y Gestión - JEFE - HERMES FERNANDO AGUILAR CÁCERES

GERENCIA ADMINISTRATIVA - División de Programación y Gestión - SUPERVISOR (e) - ROBERTO CARLOS ARREDONDO GALLEGOS

7. **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 provisión de la herramienta de monitoreo y auditoria en tiempo real de la base de datos de la marca IBM Guardium, por el periodo de vigencia de treinta y seis meses (36) meses; sin embargo, de variar las condiciones técnicas o tecnológicas que determinan esta estandarización, esta aprobación quedará sin efecto.

Es todo cuanto tengo que informar.

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

SUPERVISOR (e)

1U1200 SUNAT FOLIO 03

INFORME TÉCNICO DE ESTANDARIZACIÓN
N° 04 -2019-SUNAT/1U0100

1. MATERIA

Estandarización para la contratación de la provisión de la herramienta de monitoreo y auditoria en tiempo real de la 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 la misma.

Actualmente se cuenta con la herramienta de monitoreo y auditoría en tiempo real de 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, 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 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, debido a que a la fecha es la única con la capacidad de capturar y auditar el tráfico del tipo shared memory.

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.

INTENDENCIA NACIONAL DE SISTEMAS DE INFORMACIÓN Oficina de Seguridad Informática JEFE (e) JOMAR GONZALES ELIAS

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) 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 seguimientos de memoria (shared memory) para clientes locales (aquellos que establecen la conexión desde el mismo servidor donde se encuentra alojada la BD). Los servidores se encuentran ubicados en los centros de

cómputo de la institución (sede San Isidro y sede Miraflores). La relación de servidores puede verse en el Anexo 1.

b) Descripción del bien o servicio requerido.

Adquisición de herramienta de Monitoreo y Auditoria en Tiempo Real de Base de Datos de la Marca IBM Guardium para los 37 servidores de base de datos por 36 meses (incluye servicio de Soporte y buen funcionamiento)

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

La herramienta a adquirir será utilizada para realizar las acciones que permitan garantizar la seguridad de la información, proporcionando capacidades de monitoreo y auditoría en tiempo real.
Para ello deberá cumplir con las características 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 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 DBMSs.

(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 la herramienta.

(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) Queries 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 ejecución de sentencias DML.

(10) Las políticas de seguridad como mínimo deben poder configurarse por usuario, IP

(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 DBMSs. 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 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 7 y superior.

(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 auditar los motores de base de datos INFORMIX y ORACLE instalados en las versiones del sistema operativo AIX indicados en el numeral anterior.

(20) 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.

(21) Debe incluir, como mínimo, los roles de administrador de laherramienta, 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.

(22) 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.

(23) 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.

(24) Debe contar con plantillas listas para el cumplimiento de estándares como SOX, PCI, DSS, HIPAA.

(25) Si la herramienta utiliza agentes para el monitoreo, esta debe contar con un sistema de administración de agentes que permitan instalar, actualizar y desinstalar.

(26) Si la herramienta utiliza agentes debe permitir un despliegue masivo automático a través de la red.

(27) 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.

(28) 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.
(29) Todos los componentes de la herramienta deben contar con un 99.5% de disponibilidad.
(30) La herramienta debe permitir exportar toda la información colectada en formato texto de manera diaria

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 contratación de la provisión y soporte de la herramienta de monitoreo y auditoria en tiempo real de la 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. **Incidencia económica de la contratación.**

   El no contratar con la provisión y soporte de la herramienta de monitoreo y auditoria en tiempo real de la base de datos de la marca IBM Guardium, para brindar un alto grado de seguridad e integridad y confidencialidad a la información de las base de datos de la SUNAT, con el fabricante o distribuidores o partners autorizados de la marca IBM Guardium, no se contaría con actualizaciones en hardware y software, asi 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 y que 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.

4. **Los servicios que se requieren contratar son imprescindibles.**

   Si no se cuenta con la herramienta de Monitoreo y Auditoria en Tiempo Real 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 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 podrá determinar las causas.

   La herramienta de monitoreo y auditoría en tiempo real de Base de Datos IBM Guardium, fue elegida por la institución dado que es la única herramienta existente en el mercado capaz de soportar, en el monitoreo

que realiza, conexiones TCP/IP para accesos remotos y de segmento de memoria – shared memory con las que cuenta la institución para las labores realizadas en las bases de datos Informix y Oracle.

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

5. VIGENCIA

El periodo de vigencia de la presente estandarización es de treinta y seis (36) meses.

6. RESPONSABLE DE LA ELABORACIÓN Y EVALUACIÓN

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

6.1.	**EVALUADO POR**	
	APELLIDOS Y NOMBRES	**GONZALES ELIAS , OMAR**
	REGISTRO SUNAT	**1559**
	CARGO	**JEFE DE OFICINA**
	UNIDAD ORGANIZACIONAL	**OFICINA DE SEGURIDAD INFORMÁTICA**

6.2.	**JEFE DEL ÁREA RESPONSABLE DE LA EVALUACIÓN DEL INFORME**	
	APELLIDOS Y NOMBRES	**GONZALES ELIAS , OMAR**
	REGISTRO SUNAT	**1559**
	CARGO	**JEFE DE OFICINA**
	UNIDAD ORGANIZACIONAL	**OFICINA DE SEGURIDAD INFORMÁTICA**

7. CONCLUSIÓN

Del análisis realizado se demuestra que la SUNAT tiene la necesidad de contratar la herramienta de Monitoreo y Auditoria en Tiempo Real 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.

8. RECOMENDACIÓN

Se recomienda dar inicio al proceso de estandarización para la contratación de la herramienta de Monitoreo y Auditoria en Tiempo Real de Base de Datos de la marca IBM Guardium , tomando como base la Directivas o procedimientos emitidos por el OSCE y las normas y procedimientos aprobados por la SUNAT.

RESPONSABLE DEL INFORME OMAR GONZALES ELIAS Jefe de la Oficina de Seguridad Informática (e) INTENDENCIA NACIONAL DE SISTEMAS DE INFORMACIÓN	JEFE DEL AREA RESPONSABLE DE LA EVALUACIÓN OMAR GONZALES ELIAS Jefe de la Oficina de Seguridad Informática (e) INTENDENCIA NACIONAL DE SISTEMAS DE INFORMACIÓN

Anexo 1: Relación de servidores a monitorear y auditar

Nro.	Informix	Nro.	Oracle
1	INFP03S1	25	ORAP01S2
2	INFP05S1	26	ORAP06S1
3	INFP06S1	27	ORAP01S4
4	INFP10S1	28	ORAP01S5
5	INFP14S1	29	ORAP02S4
6	INFP18S1	30	ORAP02S5
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	INFP15S2		
19	INFP16S2		
20	INFP18S2		
21	INFP20S2		
22	INFP21S2		
23	INFP26S2		
24	INFP29S2		