BANCO CENTRAL DE RESERVA DEL PERÚ

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE N° 0287-2017-GTI230-N

SOLUCIÓN DE PROTECCIÓN Y AUDITORÍA DE BASES DE DATOS

El presente informe sustenta la necesidad de la adquisición de una Solución de Protección y Auditoría de las Bases de Datos para el Centro Externo de Respaldo (CER) con la finalidad de garantizar los niveles de seguridad de las bases de datos aun cuando estas se encuentren operando en contingencia.

1. **NOMBRE DEL ÁREA:**
   Departamento de Redes Telecomunicaciones y Base de Datos

2. **RESPONSABLES DE LA EVALUACIÓN:**
   Ricardo Cisneros Pinto

3. **CARGOS:**
   Especialista en Redes Telecomunicaciones y Base de Datos

4. **FECHA:**
   18 de octubre del 2017

5. **JUSTIFICACIÓN:**

   El BCRP cuenta actualmente con un Firewall de Base de Datos DAM (Database Activity Monitoring) de la marca Imperva, este equipo permite monitorear, auditar las operaciones ejecutadas sobre las bases de datos corporativos Oracle, así mismo de ser necesario permite bloquear los accesos a las bases de datos. Este sistema de protección de base de datos permite visualizar, analizar y correlacionar rápidamente las actividades de las bases de datos, desde cualquier ángulo y a través de una sencilla interfaz de usuario, sin necesidad de crear scripts SQL. Los elementos interactivos de análisis de auditoría simplifican las investigaciones forenses y habilitan la identificación de tendencias y de patrones, que podrían señalar riesgos de seguridad. El DAM se encuentra instalado en la OP. La solución implementada funciona en forma independiente a la activación de la auditoría nativa de la base de datos.

   Sin embargo, cuando las bases de datos requieren ser movidas Centro Externo de Respaldo ya sea por una situación contingencia u otra que requiera dicho cambio, estas ya cuentan con la protección del DAM no siendo monitoreadas ni auditadas debido a que no se cuenta con un equipo de similares capacidades en dicho Data Center.

   Debido a lo antes mencionado se requiere una solución para la protección y auditoría de las bases de datos Oracle de producción para el Centro Externo de Respaldo (CER) considerando que estas almacenan información extremadamente valiosa y confidencial, para ello se requiere mecanismos de monitoreo continuo de todas las operaciones de las bases de datos, que incluyen el acceso de usuarios con privilegios, a fin de detectar y bloquear los ataques y las posibles fugas de información, la solución requerida debe permitir implementar en forma integral la

seguridad de las bases de datos de producción, ya sea que estas se encuentren operando en la Oficina Principal (OP) o en el Centro Externo de Respaldo (CER).
.

6. ALTERNATIVAS

Existen actualmente en el mercado distintas soluciones para la protección y auditoría de las bases de datos, dentro de estas soluciones hay algunas que están basadas en Hardware y otras que están basadas en Software.
Entre las alternativas de solución se encuentra Imperva que cuenta con ambas posibilidades tanto hardware como Software, así mismo el Guardium de la empresa IBM también cuenta con la posibilidad de brindar ambas alternativas, por otro lado la Empresa Oracle y McAfee cuentan con soluciones de Software.

7. ANÁLISIS COMPARATIVO TECNICO

En base a las características técnicas (funcionales y no funcionales) y tomando en cuenta las necesidades técnicas actuales del Banco Central de Reserva del Perú, a continuación se establecen las características del producto requerido:

Solución de Hardware:

- Existen diferentes proveedores que proporcionan soluciones de Hardware para la protección y auditoría de las bases de datos, dentro de estas tenemos a Imperva y Guardium.
- Las soluciones de hardware son equipos especializados y dedicados a la función de protección y auditoría de las bases de datos, para una protección completa también se debe instalar agentes en los servidores de base de datos.
- Permiten la actualización de su software (Firmware) y la aplicación de parches cuando lo requieren.
- La actualización del hardware para incrementar sus capacidades ya sea de procesamiento, memoria y storage (almacenamiento) requieren un gasto adicional y en algunos casos requieren del cambio de todo el equipo por limitaciones de crecimiento.
- El cambio de su ubicación física en los centros de cómputo del banco son complejos y requieren la participación del proveedor así como cambios en las configuraciones de los mismos.

Solución de Software:

- Existen diferentes proveedores que proporcionan soluciones de Hardware para la protección y auditoría de las bases de datos, dentro de estas tenemos a Imperva, McAfee, Oracle y Guardium.
- Las soluciones de software son productos especializados para la protección y auditoría de las bases de datos los cuales requieren ser instalados en servidores físicos o virtuales así como de agentes en los servidores de base de datos.
- Permiten la actualización del software y la aplicación de parches cuando lo requieren.

- Para el incremento de las capacidades de la solución no es necesario el cambio del software sino la asignación de mayores recursos en el caso de que sean servidores virtuales.
- Facilidad de cambio de ubicación física en los centros de cómputo del banco de ser necesario ya que si emplean servidores virtuales esto se realiza a través de la clonación de los mismos.
- Las interfaces de Gestión y Monitoreo son más "amigables" para los especialistas responsables ya que cuentan con mayores posibilidades de búsquedas y filtros para los bloqueos y auditorías.

8. ANÁLISIS COMPARATIVO DE COSTO – BENEFICIO

Beneficios:

- Las soluciones de software permite la actualización del mismo e incrementos de las capacidades de una forma más sencilla.
- Mayor facilidad para reubicar el servicio entre los centros de cómputo del banco de ser necesario.
- Las soluciones de software presentan interfaces de gestión más fácil de emplear y con mayores capacidades de filtros.
- Las soluciones de software son integrales lo que permitiría al Banco contar con un mecanismo de protección y auditoría de bases de datos sin importar donde se encuentren estas operando.

Costos:

Según las averiguaciones realizados con diferentes empresas dedicadas al rubro de seguridad de datos, los costos de soluciones de hardware tienen costos que van desde los S/ 507,950.04 (por equipo) monto que podría verse por lo menos duplicado a fin de brindar una solución integral tal como se requiere.
Las soluciones de software tiene un costo de alrededor de S/. 326,962.02 siendo esta solución integral y permitiendo proteger las bases de datos del Banco sin importar donde se encuentren operando.

Licenciamiento

Las soluciones de hardware incluyen dentro de sus costos el equipamiento y las licencias necesarias para su funcionamiento así como el soporte local y del fabricante por 3 años.
Las soluciones de software incluyen dentro de sus las licencias necesarias para su funcionamiento así como el soporte local y del fabricante por 3 años.

Hardware Necesario Para su Funcionamiento

Las soluciones de hardware incluyen los equipos por lo que no se requiere adquirir más hardware.
Las soluciones de software requieren al menos dos (02) equipos virtuales para su funcionamiento, el BCRP cuenta actualmente con los recursos necesarios para la implementación de los servidores virtuales por lo que no se requiere adquirir más hardware.

Soporte y Mantenimiento Externo

El soporte técnico y mantenimiento de los proveedores locales como los del fabricante están comprendidos dentro de las soluciones de hardware como en las soluciones software.

Personal y Mantenimiento Interno

El personal de especialistas de Banco responsable de la administración y gestión de la solución de protección y auditoría de las bases de datos cuentan con los conocimientos, la capacitación necesaria y experiencia para la cumplir dichas funciones.

Capacitación

Se está considerando dentro del proceso de adquisición de la solución de protección y auditoría de las bases de datos cursos de capacitación oficial del fabricante para dos (02) especialistas del Departamento de Redes, telecomunicaciones y Base de Datos, dicha capacitación es específica para el producto a implementar.

9. CONCLUSIONES

Por los motivos antes señalados, se concluye que en virtud a las ventajas y menores costos la solución de Software de protección y auditoría de bases de datos es la recomendada.

10. FIRMAS

Lima, 18 de octubre de 2017

cc. Departamento de Redes, Telecomunicaciones y Bases de Datos - Ricardo Cisneros Pinto
Departamento de Redes, Telecomunicaciones y Bases de Datos - Jorge Durán Grande

BANCO CENTRAL DE RESERVA DEL PERÚ

FIRMADO POR:

Leandro Manuel ALVAREZ FIGUEROA
Jefe de Departamento de Redes, Telecomunicaciones y Bases de Datos
Departamento de Redes, Telecomunicaciones y Bases de Datos

Miguel Angel TEJADA MALASPINA
Subgerente de Servicios de Tecnologías de Información
Subgerencia de Servicios de Tecnologías de Información

Felipe Ernesto ROEL MONTELLANOS
Gerente de Tecnologías de Información
Gerencia de Tecnologías de Información

Javier Ernesto OLIVERA VEGA
Gerente Central de Administración
Gerencia Central de Administración

Renzo Guillermo ROSSINI MIÑAN
Gerente General
Gerencia General

VISADO POR: