

BANCO CENTRAL DE RESERVA DEL PERÚ

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE No.0028-2013-GTI000

ADQUISICIÓN E IMPLEMENTACIÓN DE SOLUCIÓN DE REGISTRO Y SEGUIMIENTO DE EVENTO AUDITORÍA EN TIEMPO REAL PARA EL SERVICIO DE DIRECTORIO ACTIVO

1. **NOMBRE DEL ÁREA:**
Subgerencia de Servicios de Tecnologías de Información
2. **RESPONSABLE DE LA EVALUACIÓN:**
Miguel Tejada Malaspina
Luis Díaz Vargas
Eduardo Navarro Váscones
3. **CARGOS:**
Subgerente de Servicios De Tecnologías de Información
Jefe del Departamento de Operaciones y Plataforma
Especialista en Operaciones y Plataforma
4. **FECHA:**
2013-12-13
5. **JUSTIFICACIÓN:**

Dentro de las principales tareas del Gerencia de Tecnologías de Información, se encuentra el de velar y asegurar el correcto uso y funcionamiento de los servicios que soportan la plataforma de soluciones informáticas.

La BCRP utiliza el servicio de Directorio Activo para la administración, autenticación y delegación de permisos y funciones para los usuarios de su red de datos. El servicio de Directorio Activo es primordial e indispensable para el funcionamiento de la plataforma informática de la BCRP.

Actualmente, no se cuenta con una solución de seguimiento de eventos, que permita realizar una auditoría en tiempo real de todos los cambios realizados en el servicio de Directorio Activo, tales como altas, bajas y modificación de usuarios, permisos de seguridad sobre recursos de red, delegación de funciones sobre grupos y usuarios, entre otras. Así mismo, esta solución permitirá identificar las posibles anomalías en lo que se refiere a cambios no autorizados y, de esta manera, tomar las acciones correctivas correspondientes.

6. ALTERNATIVAS:

En la siguiente tabla se presentan el software alternativo que se evaluará técnicamente en el siguiente capítulo.

Software Alternativo

Alternativa 1	Alternativa 2	Alternativa 3
Quest ChangeAuditor	NetIQ Change Guardian	Prism EventTracker



BANCO CENTRAL DE RESERVA DEL PERÚ

7. ANÁLISIS COMPARATIVO TÉCNICO:

Para realizar el análisis comparativo de las alternativas de software, se han definido métricas que fueron seleccionadas en base al análisis de los requerimientos y a la información técnica de los productos señalados en el punto "6. ALTERNATIVAS".

Se definió la siguiente calificación:

No cumple	0
Cumple regularmente	3
Cumple Satisfactoriamente	5

El puntaje aprobatorio mínimo definido es de 60 puntos.

Requerimiento	Alternativa 1	Alternativa 2	Alternativa 3
Debe ser capaz de capturar y registrar los cambios de información sin la necesidad de los registros de auditoría nativos del sistema operativo, es decir, no debe depender del registro de eventos del sistema operativo.	5	5	5
Rastrear la actividad de los usuarios y administradores con información detallada que incluya el qué, quién, cuándo, dónde y por qué de los eventos registrados. Deberá registrar desde que computador se registró el cambio.	5	5	5
Los eventos registrados deben contener valores originales (antes del cambio) y los valores actuales (después del cambio).	5	0	5
Enviar inmediatamente una alerta cuando ítems críticos son cambiados o cuando los patrones de cambio ocurren. Debe tener la capacidad de modificar la criticidad de un ítem.	5	5	3
Ofrecer la posibilidad de habilitar o deshabilitar eventos generados, en caso de que se requiera excluir cuentas seguras o de alto tráfico de ser auditadas.	5	5	5
Centralizar la administración del software en una única consola.	5	5	5

Luis Enrique Díaz Vargas
Jefe Dpto. de Operaciones y Plataformas



[Handwritten signature]

BANCO CENTRAL DE RESERVA DEL PERÚ

Los eventos deben seguir un flujo en tiempo real, permitiendo ser mostrados inmediatamente por la consola y almacenados en la base de datos que el producto use como repositorio.	5	5	3
Debe permitir controlar quién puede iniciar y detener los agentes del producto.	5	5	5
Registro y seguimiento de los eventos sobre grupos incluidos dentro de otros grupos (grupos anidados).	5	3	3
Auditar eventos de cambio como creación, eliminación, movimiento y renombramiento de objetos seleccionados de ADAM (Active Directory Application Mode) y AD LDS (Active Directory Lightweight Directory Services).	3	3	3
Registro y seguimiento de cambios en los principales componentes del Directorio Activo, tales como Schema, Sites, Domain Naming e inclusive el servicio DNS.	5	3	5
Debe proporcionar reportes, incluyendo una colección completa de informes de cumplimiento (compliance), así como la capacidad de crear rápidamente reportes personalizados.	5	5	3
Los reportes deben ser exportables en varios formatos, tales como PDF, XLS, CSV y HTML.	5	5	3
Debe proveer de una instalación simplificada que permita implementar la solución en poco tiempo.	5	5	5
	68	69	58

En esta evaluación, el software que cumple con los requisitos mínimos (factores técnicos de evaluación) es la alternativa 1, pudiendo en el proceso de adquisición presentarse otros softwares.

8. ANÁLISIS COMPARATIVO DE COSTO – BENEFICIO:

Costo:

➤ Licenciamiento

En base al análisis realizado en el punto 7, la alternativa 1, tiene un precio referencial de **S/. 74 332,30**, que incluye el IGV.

Enrique Díaz Vargas
Jefe Dpto. de Operaciones y Plataforma

2174 / 1152026378



* I N F O R M E T E C N I C O 0 0 2 8 - 2 0 1 3 - G T 1 0 0 0 *

Página 3 de 4

[Signature]

BANCO CENTRAL DE RESERVA DEL PERÚ

Beneficio:

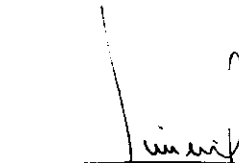
- La implementación de esta herramienta de seguimiento y auditoría permitirá tener un mejor control sobre las políticas aplicadas a los usuarios y administradores de la organización. Además llevará un registro detallado de los cambios realizados y su respectiva notificación en tiempo real.
- Así mismo, permitirá cumplir con la normatividad vigente, en lo que a las buenas prácticas de seguridad se refiere. Adicionalmente, se reducirán considerablemente las horas hombre en el monitoreo de los cambios en el Directorio Activo, y se podrán tomar acciones correctivas en el menor tiempo posible.

9. CONCLUSIONES:

- Se determinaron los atributos o características técnicas mínimas de la solución de rastreo y auditoría sobre plataforma de Directorio Activo requerida por la BCRP.
- Con la adquisición de la herramienta, se podrán auditar eventos de cambios de configuraciones y permisos de manera detallada.

Por las razones anteriormente expuestas, se recomienda la adquisición de una herramienta para el registro y seguimiento de eventos de auditoría para Directorio Activo.

10. FIRMAS:



Luis Enrique Díaz Vargas
Jefe Dpto. de Operaciones y Plataforma

