BANCO CENTRAL DE RESERVA DEL PERÚ

INFORME Nº0063-2017-GTI220-N

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE

ADQUISICIÓN E IMPLEMENTACIÓN DE SOLUCIÓN DE AUDITORÍA EN TIEMPO REAL PARA EL SERVICIO DE MICROSOFT EXCHANGE

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. 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.

El servicio de correo institucional del BCRP es administrado con Microsoft Exchange, el cual se encuentra integrado al servicio de Directorio Activo. El servicio de correo es crítico para asegurar la continuidad de las actividades que realizan los usuarios del BCRP debido a que soporta todas comunicaciones electrónicas dentro de la organización.

Actualmente, no se cuenta con una solución de seguimiento de eventos, que permita realizar una auditoría en tiempo real de todos los accesos y cambios realizados por los usuarios en la plataforma de Microsoft Exchange. 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.

5. 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 for Exchange	ManageEngine Exchange Reporter Plus	Netwrix Auditor for Exchange

6. 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 “5. ALTERNATIVAS”.

Se definió la siguiente calificación:

No cumple	0
Cumple regularmente	3
Cumple Satisfactoriamente	5

.

Requerimiento	Quest ChangeAuditor for Exchange	ManageEngine ExchangeReporter Plus	Netwrix Auditor for Exchange
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	3	3
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	3	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	3	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	3	3
Centralizar la administración del software en una única consola.	5	5	5

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	3	3
Debe proveer el seguimiento a los cambios en los parámetros de configuración del servidor Exchange, en las políticas (tamaño del mensaje, tamaño de la casilla), en las carpetas públicas del Exchange incluyendo creaciones, eliminaciones, renombres y en los permisos.	5	5	5
Registrar y proveer el seguimiento de cambios hechos a buzones (mailbox) que han sido accedidas por alguien que no es el propietario, incluyendo quién accesó, eliminó, copió, movió o creó e-mails.	5	5	5
Debe poder impedir que cualquier persona, excepto el propietario del buzón de correo, acceda a los buzones de correos críticos o confidenciales.	3	3	3
Debe proporcionar reportes, incluyendo una colección completa de informes de cumplimiento (compliance), así como la capacidad de crear rápidamente reportes personalizados.	5	5	5
Los reportes deben ser exportables en varios formatos, tales como PDF, XLS, CSV y HTML.	5	5	5
Debe proveer de una instalación simplificada que permita implementar la solución en poco tiempo.	5	5	5
	68	58	58

.

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

7. 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/. 89 007,83**, que incluye el IGV.

Beneficio:

- La implementación de esta herramienta de seguimiento y auditoria 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 Microsoft Exchange, y se podrán tomar acciones correctivas en el menor tiempo posible.

8. CONCLUSIONES:

- Se determinaron los atributos o características técnicas mínimas de la solución de rastreo y auditoría sobre plataforma de Microsoft Exchange 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 Microsoft Exchange.

Lima, 29 de marzo de 2017

cc.

BANCO CENTRAL DE RESERVA DEL PERÚ

FIRMADO POR:

Luis Enrique DIAZ VARGAS
Jefe de Departamento de Operaciones y Plataforma
Departamento de Operaciones y Plataforma

Eduardo Alfonso NAVARRO VASCONES
Especialista en Operaciones y Plataforma
Departamento de Operaciones y Plataforma

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: