

BANCO CENTRAL DE RESERVA DEL PERÚ

INFORME N° 0440-2025-GTI220-N

Informe Técnico Previo de Evaluación de Software adquisición de servicio de suscripción y soporte por 3 años de software de gestión automatizada de parches y remediación de vulnerabilidades para los sistemas operativos de 400 servidores del BCRP

1. NOMBRE DEL ÁREA:

Subgerencia de Servicios de Tecnologías de Información

2. RESPONSABLE DE LA EVALUACIÓN:

Miguel Tejada Malaspina
Subgerente, Subgerencia de Servicios de Tecnologías de Información

Luis Díaz Vargas
Jefe, Departamento de Infraestructura de Tecnologías de Información

Gerson Manuel Chumbimuni Segura
Especialista en Software Base y Middleware

3. FECHA:

19 de agosto del 2025

4. JUSTIFICACIÓN:

El aumento y sofisticación de amenazas cibernéticas y el aumento de la superficie de ataque debido a las diferentes plataformas tecnológicas en el BCRP, exigen adoptar mecanismos avanzados que aseguren la continuidad operativa y la protección de los activos de información de nuestra institución. En este sentido, la gestión manual o parcial de parches y la remediación de vulnerabilidades resulta insuficiente frente al volumen y la criticidad de los 400 servidores en producción del BCRP.

La incorporación de un software de gestión automatizada de parches y remediación de vulnerabilidades, respaldado con suscripción y soporte especializado por un periodo de tres (3) años, permitirá:

- Reducir riesgos de seguridad asociados a vulnerabilidades conocidas y ataques, mediante la aplicación oportuna y centralizada de actualizaciones.
- Cumplir con normativas y estándares de seguridad que exigen la implementación de controles para el endurecimiento de la infraestructura tecnológica.
- Optimizar recursos operativos del área de TI, evitando procesos manuales que consumen tiempo y son propensos a errores.

BANCO CENTRAL DE RESERVA DEL PERÚ

- Incrementar la disponibilidad y estabilidad de los servicios críticos del BCRP, al minimizar el impacto de incidentes relacionados con fallas de seguridad o sistemas desactualizados.
- Garantizar la escalabilidad y cobertura en un entorno heterogéneo de sistemas operativos (Windows Server, Oracle Linux, CentOS Linux, Red Hat Linux, Solaris y AIX), asegurando la uniformidad en la administración.

En consecuencia, la adquisición de esta solución no solo responde a una necesidad técnica, sino también estratégica, al fortalecer la protección de ciberseguridad del BCRP, garantizar la continuidad de los servicios en producción, y asegurar el cumplimiento de las normativas y estándares de la institución.

5. ALTERNATIVAS:

Las alternativas de mercado más relevantes son:

Soluciones empresariales de gestión de parches multiplataforma

Estas son diseñadas para entornos con gran cantidad de servidores heterogéneos:

- **IBM BigFix**
 - Cobertura muy amplia (Windows, Linux, AIX, Solaris, macOS).
 - Gran capacidad de automatización y remediación.
 - Integración con escáneres de vulnerabilidades.
 - Uso extendido en banca y sector público por su robustez y cumplimiento normativo.
- **Microsoft Endpoint Configuration Manager (SCCM) + Microsoft Intune**
 - Excelente gestión en **Windows Server**.
 - Requiere integraciones adicionales para cubrir entornos Linux/Unix.
 - Puede complementarse con herramientas de terceros para plataformas no-Microsoft.
- **ManageEngine Patch Manager Plus**
 - Soporte para Windows, Linux y macOS (no cubre Solaris/AIX de manera nativa).
 - Buena relación costo/beneficio.
 - Menos robusta que BigFix para infraestructuras críticas.

Soluciones integradas con seguridad y vulnerabilidades

Estas combinan parcheo y remediación con gestión de vulnerabilidades:

- **Qualys Patch Management (parte de Qualys Cloud Platform)**
 - Gestiona parches y vulnerabilidades en entornos híbridos.
 - Cobertura sólida para Windows y Linux.
 - Solaris y AIX tienen soporte limitado o requieren configuración adicional.
- **Tenable Nessus + Tenable.ot + Tenable Patch Management (con integración BigFix o SCCM)**

BANCO CENTRAL DE RESERVA DEL PERÚ

- Muy fuerte en **detección de vulnerabilidades**.
- El parcheo se gestiona en integración con BigFix o SCCM.
- Adecuado para instituciones financieras por el enfoque en cumplimiento.
- **Rapid7 InsightVM con remediación automatizada**
 - Enfocado en vulnerabilidades y workflows de parcheo.
 - Integración con Ansible, BigFix, SCCM para aplicar correcciones.

6. ANÁLISIS COMPARATIVO TÉCNICO:

IBM BigFix: Cobertura completa (incluye Solaris y AIX), escalabilidad comprobada en banca y gobierno, costo medio-alto, fácil integración con cumplimiento normativo.

Qualys Patch Management: Excelente en Windows/Linux, pero sin soporte para Solaris/AIX.

Tenable + BigFix: Máxima cobertura y capacidades de seguridad avanzadas, pero costo y complejidad mayores.

Microsoft SCCM/Intune: Muy sólido en Windows, limitado en Linux y sin soporte Solaris/AIX.

Ansible Automation: Flexible y económico, pero requiere alto nivel técnico interno y carece de madurez para entornos regulados.

7. ANÁLISIS COMPARATIVO DE COSTO - BENEFICIO:

Costos:

Suscripción y soporte

El precio referencial de solo la suscripción y soporte del fabricante es de US\$ 95,875.00 por cada año.

Beneficios:

- **Automatización de parches:** reduce la intervención manual y asegura que los servidores se mantengan actualizados frente a vulnerabilidades críticas.
- **Reducción del riesgo de ciberataques:** al cerrar oportunamente brechas de seguridad se mitigan riesgos de explotación por malware, ransomware o intrusiones.
- **Homogeneidad en el cumplimiento:** garantiza que todos los servidores tengan un nivel uniforme de seguridad y configuración, evitando “puntos débiles” en la infraestructura.
- **Visibilidad centralizada:** permite un control unificado del estado de parches y vulnerabilidades de los 400 servidores.

BANCO CENTRAL DE RESERVA DEL PERÚ

- **Optimización de recursos TI:** libera tiempo del personal técnico para tareas estratégicas en lugar de gestión manual de parches.
- **Escalabilidad:** la solución soporta el crecimiento en número de servidores sin que se incremente exponencialmente la carga operativa.
- **Trazabilidad y evidencia:** mantiene registros detallados de actualizaciones y acciones correctivas aplicadas.
- **Reducción de costos por incidentes:** mitiga el riesgo de pérdidas económicas derivadas de brechas de seguridad o indisponibilidad de servicios críticos.
- **Soporte especializado del fabricante:** acceso a soporte técnico avanzado y actualizaciones garantizadas durante los 3 años.
- **Continuidad del negocio:** asegura la disponibilidad de los sistemas críticos del BCRP minimizando ventanas de vulnerabilidad.

9. CONCLUSIONES

Por los motivos antes señalados, se concluye que se requiere la adquisición de servicio de suscripción y soporte por 3 años de software de gestión automatizada de parches y remediación de vulnerabilidades para los sistemas operativos de 400 servidores del BCRP a fin de garantizar a fin de garantizar la seguridad, continuidad operativa, cumplimiento normativo, eficiencia en la gestión y soporte especializado.

Lima, 19 de agosto de 2025

cc.

BANCO CENTRAL DE RESERVA DEL PERÚ

FIRMADO POR:

Gerson Manuel CHUMBIMUNI SEGURA
Especialista en Software Base y Middleware
Departamento de Infraestructura de Tecnologías de
Información

Luis Enrique DIAZ VARGAS
Jefe de Departamento de Infraestructura de
Tecnologías de Información
Departamento de Infraestructura de Tecnologías de
Información

VISADO POR:

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

Miguel Angel TEJADA MALASPINA
Gerente de Tecnologías de Información Interino
Gerencia de Tecnologías de Información
Firma como encargado.

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