

BANCO CENTRAL DE RESERVA DEL PERÚ

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE No.0005-2014-GTI000

SERVICIO DE RENOVACIÓN DE SUSCRIPCIONES DEL SOFTWARE PARA EVALUACIÓN DE LA SEGURIDAD DE LA RED Y GESTIÓN DE ACTUALIZACIONES (GFI LANGUARD)


Renzo Rossini Milán
Gerente General

1. NOMBRE DEL ÁREA:

Dpto. de Redes, Telecomunicaciones y Bases de Datos

2. RESPONSABLE DE LA EVALUACIÓN:

Alexander Gamboa Inga

3. CARGO:

Especialista en Redes, Telecomunicaciones y Bases de datos

4. FECHA:

25 de febrero de 2014.

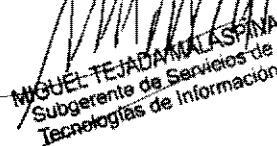
5. JUSTIFICACIÓN:

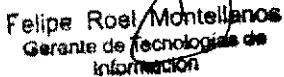
La aplicación proactiva de actualizaciones de seguridad o parches es esencial para mantener la disponibilidad operacional y la integridad de los sistemas de TI de las organizaciones, pues reduce la probabilidad de explotación de vulnerabilidades.

La gestión de actualizaciones es un proceso que debe hacerse de manera rutinaria y deben ser lo más amplio posible para que sea más eficaz. En una red de cientos de sistemas, todo lo que necesita es que un equipo llegue a ser comprometido para que múltiples equipos sean comprometidos también. Esto no quiere decir que todos los sistemas deben ser tratados por igual, cada empresa debe asignar prioridades a sus activos y proteger a los más críticos en primer lugar. Lo que es importante es asegurarse de que la aplicación de parches se realice en todos los equipos y no sólo en los más críticos.

La gestión de actualizaciones juega un rol importante en la postura de seguridad de la empresa, pero no debe ser entendida como la solución para todas las vulnerabilidades de seguridad. Contar con múltiples controles de seguridad, de los cuales la gestión de actualizaciones es parte, es el medio más eficaz de protegerse contra las amenazas potenciales.


Leandro Marcer Figueroa
Jefe, Dpto. de Redes, Telecomunicaciones
y Bases de Datos


Miguel TEJADA ALASPINA
Subgerente de Servicios de
Tecnologías de Información


Felipe Roel Montellanos
Gerente de Tecnologías de
Información


JAVIER OLIVERA VEGA
Gerente Central de Administración


Alexander Gamboa Inga
Reg. 2002



BANCO CENTRAL DE RESERVA DEL PERÚ

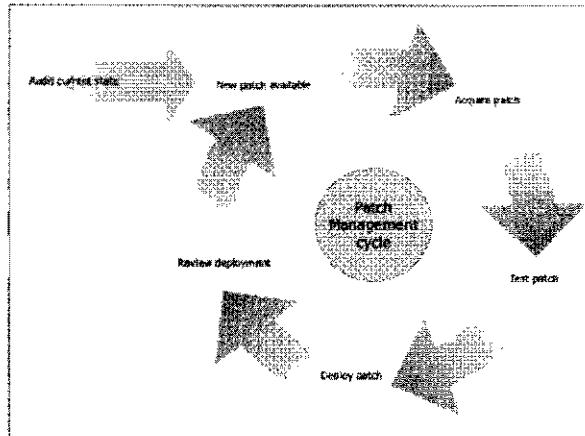


Figura N° 1: Patch Management Cycle

Fuente: *Patch Management (SANS Institute InfoSec Reading Room)*

La gestión de vulnerabilidades es algo más que aplicar parches. Para construir un sistema verdaderamente robusto se necesita incorporar la gestión de inventarios, gestión de configuración y gestión de cambios en el ciclo de vida de aplicación de actualizaciones. Además, para un control más eficaz se necesita ejecutar evaluaciones de seguridad periódicas.

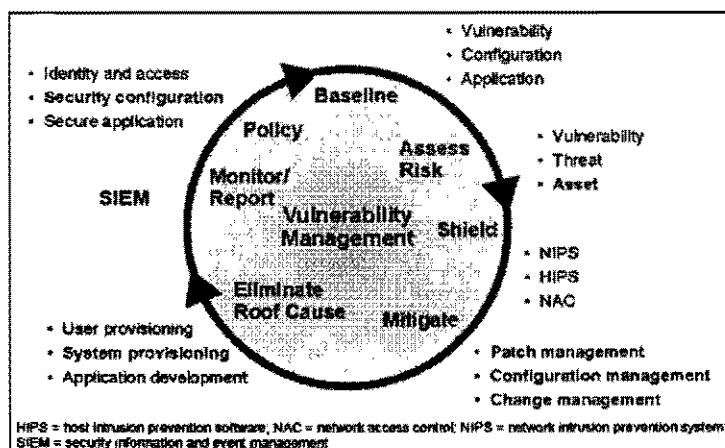


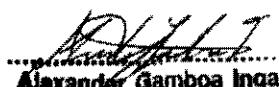
Figura N° 2: Vulnerability Management Life Cycle

Fuente: *Understanding Vulnerability Management Life Cycle Functions (Gartner)*

La Norma Técnica Peruana NTP-ISO/IEC 17799 2007 establece que "una vez identificadas las vulnerabilidades técnicas potenciales, la organización debe identificar los riesgos asociados y las acciones a ser tomadas en cuenta. Estas acciones pueden implicar el parchado de los sistemas vulnerables y/o la aplicación de otros controles".

Alexandro Alvarez
Dpto de Redes, Telecomunicaciones y Bases de Datos
2174 / 0808004665




Alexander Gamboa Inga
Reg. 2092

BANCO CENTRAL DE RESERVA DEL PERÚ

6. ALTERNATIVAS:

En el mercado local se han encontrado productos de los siguientes fabricantes: GFI, BeyondTrust y ManageEngine.

En el año 2012 el BCRP adquirió el software GFI LANguard, licenciado para 1300 nodos, a través del proceso AMC-0071-2012-BCRPLIM – “Adquisición de licencias de software para evaluación de la seguridad de la red y gestión de actualizaciones”

El software GFI LANguard proporciona las siguientes funcionalidades:

- ✓ Es capaz de gestionar actualizaciones para software no Microsoft, tales como Adobe Reader, Adobe Flash Player y Oracle Java Runtime, de uso común en las estaciones. Las actualizaciones proporcionadas son probadas previamente por el fabricante GFI.
- ✓ Puede operar con o sin un agente de gestión en las estaciones.
- ✓ Opera en modo push, realizando actualizaciones directas desde la consola hacia las estaciones.
- ✓ Proporciona la funcionalidad de evaluación de seguridad (análisis de vulnerabilidad y auditorías de seguridad de la red).
- ✓ Permite generar reportes de las evaluaciones realizadas y del estado de distribución de actualizaciones.

7. ANÁLISIS COMPARATIVO TÉCNICO:

Debido a que es un sistema con el cual ya cuenta el BCRP y el cual ha sido solicitado sea estandarizado, lo que se desea es la contratación del servicio de renovación de suscripciones, por lo que no cabe un análisis comparativo técnico.

8. ANÁLISIS COMPARATIVO DE COSTO – BENEFICIO:

Beneficios:

El servicio de suscripción a las actualizaciones del fabricante GFI permite lo siguiente:

- ✓ Acceder tanto a actualizaciones a la base de datos de vulnerabilidades sobre las cuales el software GFI LANguard realiza sus evaluaciones.
El acceso a la base de datos de vulnerabilidades del fabricante es necesario, por cuanto se amplía el catálogo de aplicaciones evaluadas, así como que nuevas vulnerabilidades son descubiertas.
- ✓ Descargar actualizaciones de software que se aplicarán en las estaciones.
Dichas actualizaciones han recibido verificación previa por el fabricante GFI (reduciendo con la probabilidad de presentarse efectos adversos por la aplicación de una actualización de software) y permitirán corregir las vulnerabilidades detectadas.

Mantenimiento de software

Acceso a actualizaciones de versiones y/o motores de escaneo al propio software GFI LANguard, permitiendo optimizar las capacidades de detección y operación.

2174 / 0808004665



* INFORME TECNICO 0005 - 2014 - GTI 000 *

Página 3 de 4

Alexander Gamboa Inga
Reg. 2092

BANCO CENTRAL DE RESERVA DEL PERÚ

- ✓ Soporte técnico del fabricante

Costos:

- Suscripciones

Servicio de renovación de suscripciones para el software GFI LANguard, incluyendo el mantenimiento de software (actualizaciones) y el soporte técnico por el periodo de un (01) año.

Se obtuvieron cotizaciones referenciales por montos de S/. 21 450 ,00 y S/. 25 331 incluido IGV.

- Plazo de implementación del servicio, con las condiciones exigidas por el BCRP

El plazo de implementación del servicio no será mayor de 10 días calendario, contabilizados a partir del día siguiente de la suscripción de la orden de compra o contrato.

9. CONCLUSIONES:

Por lo expuesto anteriormente, se recomienda la contratación del servicio de renovación de suscripciones del Software para evaluación de la seguridad de la red y gestión de actualizaciones (GFI LANguard).

10. FIRMAS:


Leandro Alfonso Flores
Jefe, Unidad de Redes, TI, ... Actualizaciones
y Bases de Datos


Alexander Gamboa Inga
Reg. 2092

