

BANCO CENTRAL DE RESERVA DEL PERÚ

INFORME N° 0094-2018-GTI230-N

ASUNTO : Informe técnico previo de evaluación de software - servicio de renovación de suscripciones del equipamiento de seguridad informática para el acceso a Internet (McAfee Web Gateway).

1. NOMBRE DEL ÁREA:

Dpto. de Redes, Telecomunicaciones y Bases de Datos

2. RESPONSABLE DE LA EVALUACIÓN:

Jackes Matos Manguinuri

3. CARGO:

Especialista en Redes, Telecomunicaciones y Bases de Datos

4. JUSTIFICACIÓN:

Internet se ha convertido en una herramienta valiosa y necesaria para las empresas y organizaciones alrededor del mundo. Con su expansión y crecientes facilidades, Internet también ha llegado a ser un medio para completar transacciones financieras en forma rápida y eficiente. Adicionalmente Internet es un invaluable recurso para obtener información e investigar sobre cualquier tópico.

Sin embargo, como sucede con otros recursos, el acceso Internet puede ser objeto de uso inadecuado. Este mal uso se puede dar de muchas formas, las que incluyen acceso a web sites de contenido pornográfico, web sites de juegos, descarga de archivos de procedencia no fiable, etc. Asimismo debe considerarse que cada empresa tiene sus propios fines institucionales lo que conlleva a que ciertos web sites que son de acceso requerido en una organización no lo sean en otra. Por ejemplo el acceso a diarios online puede ser considerado necesario en una empresa de difusión de noticias, pero otra institución puede considerar que ello debe ser limitado porque afecta la productividad de sus empleados. Cada empresa tiene por tanto que establecer sus propios límites.

En muchos casos el uso para propósitos personales puede ser beneficioso para la empresa, por ejemplo un empleado puede realizar un trámite bancario por Internet, reduciendo considerablemente el tiempo que le tomaría si tuviese que efectuar el mismo trámite en forma presencial, en este caso el beneficio para la empresa es el ahorro en tiempo laboral. También existe el lado contrario, por ejemplo empleados utilizando el acceso a Internet para actualizar fotos y videos en páginas web personales, desperdiçando en ello tiempo laboral, por el que la empresa le paga, así como recursos de ancho de banda, que también tienen costo para la institución y que podrían ser utilizados en fines laborales. Por ello generalmente las empresas desean evitar que el tiempo destinado por los empleados en el uso de Internet para propósitos personales, tenga efectos negativos en su productividad laboral.

Otro aspecto importante es que existe la posibilidad de que ciertos actos de mal uso por parte de los empleados, ocasionen que la organización se vea comprometida en procesos legales, al haberse utilizado sus recursos e instalaciones, para cometer dichas

BANCO CENTRAL DE RESERVA DEL PERÚ

acciones ilícitas. Por ejemplo usar software P2P para transferir ilegalmente audio/video que está protegido por copyright. En este rubro también debemos considerar el robo de información confidencial de la institución, por ejemplo un empleado puede transmitir información financiera confidencial en forma encriptada mediante Dropbox para uso en beneficio de terceros.

Efectos colaterales del mal uso son el incremento la probabilidad de exposición a infecciones de malware diverso (worms, trojan horses, spyware, etc.), que pueden poner en riesgo la seguridad de la red informática institucional, así como el uso de recursos de ancho de banda en propósitos ajenos a los requerimientos laborales.

Ante esta situación las organizaciones requieren de formas de controlar el acceso y uso de Internet, que cumplan los siguientes requerimientos:

- Evitar la exposición a ataques
Internet es uno de los principales medios de difusión de malware. Algunos sitios web como web sites de contenido pornográfico, piratería de software, entretenimiento, juegos en línea, descarga de archivos MP3, videos (Youtube), redes sociales (por ejemplo Facebook) son usualmente utilizados por hackers para incrustar código malware. Otro vector de infecciones son sitios web que han sido comprometidos. Una vez que un computador es infectado es usual que los atacantes utilicen técnicas de phone-homing para transmitir información hacia sitios web que están bajo su control.
- Asegurar un adecuado performance de acceso
Cada vez es mayor el número de sistemas de información y aplicaciones de negocio que son accedidos a través de Internet, por dicho motivo es importante contar con herramientas de control que permitan priorizar la asignación de los recursos disponibles, a las aplicaciones y usos de carácter institucional.
- Garantizar el cumplimiento de las políticas internas de uso aceptable del servicio
Las organizaciones requieren garantizar que el acceso a Internet que proporcionan a sus empleados les sirva para fines laborales, a la vez que se reducen los riesgos asociados al acceso de sitios web de contenido poco fiable, el desperdicio de recursos de ancho de banda y la pérdida de tiempo laboral. Asimismo se necesita evitar que la organización asuma responsabilidades legales derivadas de malos usos de los empleados. Definir que es aceptable y que no lo es, generalmente requiere el uso de dos criterios simples, el primero es el determinar el nivel de acceso necesario para fines laborales. El segundo criterio se refiere a establecer que acciones o usos son considerados no aceptables. Los sistemas de control de acceso no son perfectos y por ello establecer estos criterios (políticas) es requisito para salvaguardar la responsabilidad de la institución frente a posibles malos usos no detectados oportunamente.

Resumen del historial de contratación

A fines del año 2013, a través del proceso ADP 0008-2013-BCRPLIM, el BCRP adquirió una solución de seguridad informática para el acceso a Internet, conformada por dos equipos Intel McAfee Web Gateway 5500B (en cluster) y el software de reportes Intel McAfee Web Reporter.

Situación actual

Nº Sistema: INF-2018-002402

Firmado con certificados digitales emitidos por RENIEC. Los nombres de los firmantes figuran en la última página.

BANCO CENTRAL DE RESERVA DEL PERÚ

A continuación se presenta un resumen de los servicios proporcionados por la solución:

- Autenticación y autorización de usuarios
- Filtro de acceso a URLs basado en categorías
- Filtro de reputación Web
- Inspección de tráfico SSL
- Control de aplicaciones que usan tunneling
- Antimalware en gateway para el acceso web

5. ALTERNATIVAS:

El BCRP cuenta con equipamiento de seguridad informática para el acceso a Internet McAfee Web Gateway, para la protección de 1100 nodos, adquirido el año 2013. Esta solución se encarga de brindar control y protección a la navegación web en Internet.

6. ANÁLISIS COMPARATIVO TÉCNICO:

Equipamiento de seguridad informática para el acceso a Internet, McAfee Web Gateway adquirido el año 2013.

7. ANÁLISIS COMPARATIVO DE COSTO – BENEFICIO:

Beneficios:

- Activar funcionalidades de control (autenticación y autorización de usuarios, inspección de tráfico SSL)
- Protección actualizado dinámicamente por el fabricante (filtrado URL basado en categorías y reputación, antimalware en el gateway de acceso a Internet).
- Consola de web para gestión de la solución con capacidad de generación de reportes estadísticos.
- Configuración en alta disponibilidad, que permite mantener la continuidad del servicio aún ante el evento de caída del site principal.

Costos:

- Suscripción a los servicios del fabricante McAfee.
- Mantenimiento de software (incluyendo el suministro de nuevas versiones y patches), soporte técnico del fabricante (escalamiento), por el periodo de un (01) año.
- Servicios del partner (proveedor local).
- Mesa de ayuda y soporte presencial, en el esquema 24x7x2 y mantenimiento técnico preventivo anual y optimización de configuraciones.
- En lo que respecta a los costos asociados, se ha recibido una cotización referencial por S/ 74 200,27 incluido IGV.

BANCO CENTRAL DE RESERVA DEL PERÚ

8. CONCLUSIONES:

Por lo expuesto anteriormente, se considera conveniente la contratación de la renovación de suscripciones del equipamiento de seguridad informática para el acceso a Internet (McAfee Web Gateway).

Lima, 19 de junio de 2018

cc.

BANCO CENTRAL DE RESERVA DEL PERÚ

FIRMADO POR:

VISADO POR: