BANCO CENTRAL DE RESERVA DEL PERÚ

INFORME Nº 0126-2023-GTI230-N

Informe técnico previo de evaluación de software - Contratación de suscripciones de seguridad en el acceso a Internet

1. NOMBRE DEL ÁREA:

Dpto. de Ciberseguridad y Redes

2. RESPONSABLE DE LA EVALUACIÓN:

Luis Alberto Peña Palacios

3. CARGO:

Especialista en Ciberseguridad y Redes

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 webs 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, desperdiciando 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 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, 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.

Las soluciones de seguridad informática para el acceso a Internet permiten cumplir con los requerimientos mencionados anteriormente, a través del uso de los siguientes módulos de control:

- ✓ 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:

En el mercado nacional hemos identificado las siguientes soluciones de seguridad, las mismas que están también consideradas en las evaluaciones de empresas consultoras de prestigio (Gartner, Forrester, Radicatti)

- Skyhigh Security Web Gateway
- Broadcom Symantec Web Protection

6. ANÁLISIS COMPARATIVO TÉCNICO:

El análisis técnico ha sido realizado de conformidad con la metodología establecida en el documento "Guía Técnica sobre evaluación de software en la administración pública" (Resolución Ministerial N° 139-2004-PCM), tal como se exige en el reglamento de la Ley N° 28612.

Propósito de evaluación
Comparar alternativas de productos existentes en el mercado.

Identificar el tipo de producto
Seguridad en el acceso a internet.

Identificación del modelo de calidad
Se aplicará el Modelo de Calidad de Software descrito en la Parte I de la Guía de evaluación de software aprobado por RM N° 139-2004-PCM.

Selección de métricas.
Las métricas fueron seleccionadas en base a las características técnicas descritas en el Anexo N° 1.

7. ANÁLISIS COMPARATIVO DE COSTO – BENEFICIO:

Beneficios:

- Activar funcionalidades de control (autenticación y autorización de usuarios, inspección de tráfico SSL)
- Protección actualizada 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:

Las prestaciones requeridas corresponden al periodo de tres (03) año de servicio:

- Prestación principal: Servicios del fabricante
  Suscripción a una solución de seguridad informática para el acceso a internet, incluyendo actualizaciones de software (incluyendo el suministro de nuevas versiones y patches) y soporte técnico del fabricante (escalamiento).

- Prestación accesoria: Servicios del partner (proveedor local)
  Mesa de ayuda y soporte presencial, en el esquema 24x7, mantenimiento técnico preventivo anual y capacitación.

En base a las cotizaciones referenciales obtenidas se estima que el costo del servicio se encuentra dentro del margen presupuestado en PAC 2023.

8. CONCLUSIONES:

Por lo expuesto anteriormente, se considera conveniente la Contratación de suscripciones de seguridad en el acceso a Internet, por el periodo de tres (03) años.

BANCO CENTRAL DE RESERVA DEL PERÚ

Anexo 1

Atributos	Puntaje Maximo	Skyhigh Web Gateway	Broadcom Symantec Web Protection
Autenticación y autorización de usuarios	20	20	20
Filtro de acceso a URLs basado en categorías	20	19	18
Filtro de reputación Web	20	19	19
Inspección de tráfico SSL	10	9	8
Control de aplicaciones que usan tunneling	15	15	15
Antimalware en gateway para el acceso web	15	13	13
Total	100	95	93

Lima, 11 de julio de 2023

cc.

BANCO CENTRAL DE RESERVA DEL PERÚ

FIRMADO POR:

Luis Alberto PEÑA PALACIOS
Especialista en Ciberseguridad y Redes
Departamento de Ciberseguridad y Redes

Alexander John Anthony GAMBOA INGA
Jefe de Departamento de Ciberseguridad y Redes
Interino
Departamento de Ciberseguridad y Redes
Firma como encargado.

VISADO POR:

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

Marco Antonio GRANADINO CACERES
Subgerente de Riesgos de Tecnologías de Información
Subgerencia de Riesgos de Tecnologías de Información

Silvia Elizabeth MEDINA MORENO
Gerente de Tecnologías de Información
Gerencia de Tecnologías de Información

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