LEY QUE NORMA EL USO, ADQUISICIÓN Y ADECUACIÓN DEL SOFTWARE EN LA ADMINISTRACIÓN PÚBLICA	LEY 28612
Congreso de la República Oficina de Tecnologías de Información Área de Infraestructura Tecnológica	

Informe Técnico Previo de Evaluación de Software Nº 003-2018/AIT-OTI/CR
EVALUACIÓN DE SOFTWARE DE SEGURIDAD

1. Nombre del Área

Área de Infraestructura Tecnológica

2. Responsable de la evaluación

Víctor Bedoya Prieto

3. Cargo

Jefe del Área de Infraestructura Tecnológica

4. Fecha

07 Agosto 2018

5. Requerimiento del Área Usuaria

La renovación de la suscripción de licencias para la solución de Software de Seguridad que incluye el soporte en línea que brinda el fabricante, el soporte técnico local y visita técnica trimestral.

6. Justificación

- **Necesidad:**

El Congreso de la República requiere renovar la suscripción de licencias, actualización de software, soporte en línea del fabricante, soporte técnico local y visitas técnicas trimestrales para la Solución de Software de Seguridad que permite proteger los servicios de correo electrónico, navegación web y servidores de la Institución, de ataques y/o amenazas externas e internas.

- **Antecedentes:**

En el año 2002 mediante el Contrato N° 068-2012-AJ/CR se adquirió el producto de seguridad InterScan Virus Wall, el que permitía proteger los servicios de correo electrónico y navegación en Internet contra las amenazas de virus. Este software ha sido actualizado por el fabricante durante el periodo de duración de los contratos de mantenimiento, adquiriendo durante los años posteriores un mayor número de licencias de uso para usuarios finales, dado que año tras año se ha incrementado el número de usuarios que tienen acceso a dichos servicios.

El fabricante ha evolucionado el producto inicial agregándole mayores funcionalidades que permiten proteger los sistemas de nuevos tipos de ataques con diferentes tecnología, brindando protección a una mayor cantidad de servicios que los atacantes intentan comprometer, por lo que los nombres y cantidad de productos se han modificado con el tiempo, tales como Enterprise Security for Gateways (Incluye InterScan Messaging Security, InterScan Web Security, entre otros), Enterprise Security for Endpoints (Incluye Office Scan, entre otros) todos de la marca Trend Micro.

Informe Técnico Previo de Evaluación de Software Nº 003-2018/AIT-OTI/CR
EVALUACIÓN DE SOFTWARE DE SEGURIDAD

Con fecha 07 de agosto de 2017 se suscribió el Contrato N° 030-2017-OAJ-CR correspondiente a la contratación del Servicio de Software de Seguridad por lo cual se obtuvo 2001 licencias de la suite "Trend Micro Smart Protection Complete" las cuales finalizaron su vigencia el 21 de julio de 2018.

Asimismo, el software de seguridad para correo electrónico, navegación web y servidores de la marca Trend Micro fue estandarizado con los siguientes documentos: Resolución N° 257-2010-DGA/CR, Resolución N° 108-2012-DGA/CR, Resolución N° 068-2014-DGA/CR y Resolución N° 111-2016-DGA/CR, la cual se encuentra vigente hasta el 31 de diciembre de 2018.

- **Funcionalidad requerida**

Las necesidades actuales de nuestros usuarios demandan funcionalidades de seguridad en sus comunicaciones contra ataques de tipo spam, phishing, malware y virus en el servicio de correo electrónico, protección contra virus, gusanos y malware en la descarga de archivos desde internet y acceso libre de ataques en la navegación por internet, protección contra páginas comprometidas e infectadas, así como, bloqueo de sitios no autorizados y con protección de medios sociales, también la seguridad end point para la continua operatividad de los servidores de la institución.

Se recomienda que la solución a ser implementada en el Congreso satisfaga las funcionalidades descritas en la siguiente tabla:

FUNCIONALIDAD	DESCRIPCIÓN
Desplegable como máquina virtual	La solución debe estar preparada para desplegarse como un virtual appliance
Protección en tiempo real	La ejecución de la seguridad debe brindarse de manera continua y permanente. Se deben ejecutar las tareas de protección como respuesta a las amenazas de virus o ataques de manera inmediata.
Facilidad de administración	La solución debe brindar facilidad para la gestión de supervisión, monitoreo y configuración.
Incluir plantillas de reportes y permitir personalizarlos	La solución debe generar reportes personalizados.
Contar con actualizaciones periódicas (parches de seguridad), liberadas frecuentemente.	La solución debe actualizarse en forma automática y manual.
Permitir la creación de roles para la administración	La solución debe permitir asignar funciones para la gestión de administración.
Archivos de registro (logs)	Se debe tener acceso a los archivos de registro del sistema para efectos de determinación de fallas y auditoría.

Informe Técnico Previo de Evaluación de Software N° 003-2018/AIT-OTI/CR EVALUACIÓN DE SOFTWARE DE SEGURIDAD

El Congreso de la República requiere de una plataforma de seguridad actualizada que cuente con el soporte técnico local y del fabricante así como mantener su efectividad mediante revisiones periódicas del producto con visitas técnicas programadas, para asegurar a los usuarios finales que los servicios y aplicaciones brindadas por la oficina de Tecnologías de Información cuenten con un estándar de seguridad que les permita trabajar y cumplir con sus objetivos de una manera confiable.

7. Alternativas

Las alternativas de solución para el Software de Seguridad que incluye: Antispam, Antivirus Web y Antivirus de servidores, por sus características similares de funcionamiento, disponibilidad y que son líderes en el mercado local son:

Trend Micro Smart Protection Complete
McAfee Endpoint Protection – Advance Suite
Symantec Protection Suite Enterprise Edition

CONGRESO DE LA REPÚBLICA V°B° V. GALVEZ Jefa de la Oficina de Tecnologías de la Información

8. Análisis Comparativo Técnico

El análisis comparativo técnico se hará sobre productos finales, es decir, productos ensamblados que vienen en formato de ejecutables. Para lo cual se debe:

- Comparar el producto con otros productos competitivos.
- Seleccionar un producto entre productos alternativos.
- Valorar tanto el aspecto positivo, como el negativo, cuando está en uso.
- Decidir cuándo mejorar o reemplazar un producto.

CONGRESO DE LA REPÚBLICA V°B° V. BEDOYA Jefe del Área de Infraestructura Tecnológica

Se utilizará la metodología establecida en la Guía Técnica sobre Evaluación de Software para la Administración Pública, aprobada por Resolución Ministerial N° 139-2004-PCM. En la cual se establece el modelo de calidad basada en los criterios de evaluación mostrados en el Anexo N°1.

En esta evaluación se considera la funcionalidad, fiabilidad, usabilidad y eficiencia como características del tipo de "Calidad Externa", es decir, aplicables a productos de software terminados (ejecutables), como los que consideramos en el numeral 7. Mientras que capacidad de mantenimiento y portabilidad se consideran del tipo de "Calidad Interna", aplicable a productos que se desarrollan a medida como son los sistemas propios de las instituciones, esto no significa necesariamente que los productos de software terminados no tengan métricas de calidad interna, igual se debe evaluar su capacidad en mantenimiento y su portabilidad pero con menos rigurosidad. Finalmente la "Calidad de Uso", definida por las características que se evaluarán y básicamente está relacionada con el grado de satisfacción y los esfuerzos que los usuarios experimentan al usar los productos.

Para el Congreso de la República es de vital importancia evaluar con mayor rigurosidad las métricas que se definen para la calidad externa, para este caso, la puntuación será mayor. Para las métricas que se definen para la calidad interna tendrán una menor puntuación. El detalle de la puntuación considerada para evaluar la "Solución de Software de Seguridad " se detalla en el anexo N ° 1, haciendo un total de 100 puntos.

Informe Técnico Previo de Evaluación de Software Nº 003-2018/AIT-OTI/CR
EVALUACIÓN DE SOFTWARE DE SEGURIDAD

Considerando las siguientes soluciones: Trend Micro Smart Protection Complete, McAfee Endpoint Protection – Advance Suite y Symantec Protection Suite Enterprise Edition se procedió a su evaluación, para ello se definieron las métricas con sus puntajes respectivos mostrados en el anexo N° 1.

Como se observa en el cuadro, la eficiencia del producto, productividad, satisfacción, funcionalidad y usabilidad son las principales características que la institución considera necesario evaluar de los productos y por tanto se les ha ponderado con un mayor puntaje.

En el mismo anexo, se muestran los resultados de la evaluación de los productos considerados para el requerimiento "Renovación de licencia de Software de Seguridad" del que se desprende que el software Trend Micro Smart Protección Complete es el que mejor se adecua a las necesidades de la institución

9. Análisis Comparativo Costo – Beneficio

- **Licenciamiento:**

Según los valores de mercado obtenidos se concluye que se requiere de la siguiente inversión para implementar el Software de Seguridad en el Congreso de la República.

A continuación se presentan los costos remitidos por las empresas de las soluciones indicadas en el numeral 7.

Precios en soles y con IGV.

Marca	Total S/.
Trend Micro Smart Protection Complete	137,385.25
McAfee Endpoint Protection – Advance Suite	368,572.41
Symantec Protection Suite Enterprise Edition	392,538.80

Los detalles de las cotizaciones se adjuntan al final del documento.

El Software de Seguridad de la marca Trend Micro Smart Protection Complete es la solución de software más económica.

- **Hardware necesario para su funcionamiento:**

El software a actualizar se integrará a la plataforma informática existente en el Congreso de la República, por lo tanto no será necesario adquirir hardware adicional para la implementación de cualquiera de los productos.

- **Soporte y mantenimiento externo:**

El servicio de soporte técnico para la resolución de incidentes, con asistencia telefónica y presencial, y el mantenimiento del producto, para las actualizaciones o upgrades a nuevas versiones, es parte de las especificaciones técnicas del requerimiento, por lo tanto, los valores de mercado obtenidos incluyen este costo.

- **Personal y mantenimiento interno:**

Un cambio del software implicaría un importante costo en horas-hombre y el potencial riesgo de perder información o funcionalidad incorporado en las actuales plataformas, sistemas y configuraciones.

- **Capacitación:**

Un cambio de software implicaría la capacitación del personal del Congreso para que conozcan las nuevas funcionalidades del software.

- **Beneficios de la solución propuesta por el Software de Seguridad de la marca Trend Micro:**

La actualización de la solución de Software de Seguridad, que dispone el Congreso de la República permite la continuidad natural y segura de las labores que realiza nuestra Institución.

La experiencia que tiene el personal técnico especializado en el uso de las funcionalidades del software y sus componentes, permitirá una mejor optimización de los tiempos del personal.

Se ha recorrido la curva de aprendizaje por lo cual se espera un menor tiempo para obtener resultados por medio del trabajo en equipo.

10. Conclusiones

Considerando los resultados del Análisis Comparativo Técnico y Análisis Comparativo Costo Beneficio, se concluye que:

- El software Trend Micro Smart Protection Complete ha obtenido el mayor puntaje en nuestra evaluación técnica (96 puntos).
- La solución Software de Seguridad Trend Micro Smart Protection Complete es el que mejor se adecua a las necesidades del Congreso de la República.

VÍCTOR M. BEDOYA PRIETO Jefe (e) del Área de Infraestructura Tenológica CONGRESO DE LA REPÚBLICA	Ing. VICTOR R. GÁLVEZ MEJÍA Jefe de la Oficina de Tecnologías de Información CONGRESO DE LA REPÚBLICA
EVALUADO POR: Víctor Bedoya Prieto **Jefe del Área de Infraestructura Tecnológica**	**APROBADO POR:** Víctor Gálvez Mejía **Jefe de la Oficina de Tecnologías de Información**

ANEXO N° 1 - HOJA DE EVALUACIÓN DE CALIDAD DEL PRODUCTO

Evaluación de Software de Seguridad

TIPO CALIDAD	CARACTERISTICAS	SUB CARACTERISTICA	PUNTAJE MAXIMO	CRITERIOS DE CALIFICACION	PUNTAJE	McAfee Endpoint Protection Advance Suite	Symantec Protection Suite Enterprise Edition	Trend Micro Smart Protection Complete
CALIDAD INTERNA Y EXTERNA	FUNCIONALIDAD	Adecuación	3	SI NO	3 0	3	3	3
		Exactitud	3	ALTA MEDIA BAJA	3 2 1	3	3	3
		Interoperatividad	3	SI NO	3 0	3	3	3
		Seguridad (Vulnerabilidad)	3	ALTA MEDIA BAJA	3 2 1	3	3	3
		Conformidad de Funcionalidad	2	SI NO	2 0	2	2	2
	FIABILIDAD	Madurez	3	ALTA MEDIA BAJA	3 2 1	3	3	3
		Tolerancia a fallas	2	SI NO	2 0	2	2	2
		Recuperabilidad	3	ALTA MEDIA BAJA	3 2 1	3	3	3
		Conformidad de fiabilidad	2	SI NO	2 0	2	2	2
	USABILIDAD	Entendimiento	3	ALTA MEDIA BAJA	3 2 1	2	2	2
		Aprendizaje	3	ALTA MEDIA BAJA	3 2 1	3	2	3
		Operabilidad	3	ALTA MEDIA BAJA	3 2 1	3	3	3
		Atracción (amigable)	3	SI NO	3 0	3	3	3
		Conformidad de uso	2	SI NO	2 0	2	2	2
	EFICIENCIA	Comportamiento de tiempos (performance)	4	ALTA MEDIA BAJA	4 2 1	4	2	4
		Utilización de recursos	4	SI NO	4 2	2	2	2
		Conformidad de eficiencia	4	SI NO	4 1	4	4	4
	CAPACIDAD DE MANTENIMIENTO	Facilidad de mantenimiento	2	SI NO	2 0	2	2	2
	PORTABILIDAD	Adaptabilidad	2	SI NO	2 0	2	2	2
		Facilidad de Instalación	3	ALTA MEDIA BAJA	3 2 1	2	2	3
		Coexistencia	3	ALTA MEDIA BAJA	3 2 1	2	3	2
		Reemplazabilidad (upgrade)	1	SI NO	1 0	1	1	1
		Conformidad de portabilidad	1	SI NO	1 0	1	1	1
CALIDAD DE USO	EFICIENCIA	Alcanzar las metas con exactitud e integridad	12	ALTA MEDIA BAJA	12 6 1	12	12	12
	PRODUCTIVIDAD	Alcanzar los objetivos a menores costos	12	SI NO	12 6	6	6	12
	SEGURIDAD	Riesgo de propiedad	2	SI NO	2 0	2	2	2
	SATISFACCION	Usuarios satisfechos	12	ALTA MEDIA BAJA	12 6 1	12	12	12
		TOTAL OBTENIDO	**100**			**89**	**87**	**96**

CONGRESO DE LA REPÚBLICA * Oficina de Tecnologías de la Información * V°B° V. GALVEZ

CONGRESO DE LA REPÚBLICA * Secretaría de Infraestructura Tecnológica * V°B° V. BEDOYA

siscotec

Código: COM-VT-PL-01-03

Rev.: 2
Fecha:
15/01/2015

PROFORMA

Empresa:	CONGRESO DE LA REPUBLICA	Nº Cotización:	121-06-TM-CONGRESO-PE-LM
Contacto:	Ernesto Becerra	Fecha:	28/06/2018
eMail:	ebecerra@congreso.gob.pe	Vendedor:	Javier Ruiz
Teléfono:	311-7777	Teléfono:/Fax:	989615863
Ciudad:	Lima	Moneda:	Soles

ASUNTO: Licenciamiento de Software de Seguridad

Nº PARTE	DESCRIPCION DE PRODUCTOS	CANT.	PRECIO UNITARIO	PRECIO SUBTOTAL
TM	**Licenciamiento de Software de Seguridad** *** Licencias de Smart Protection Complete (SPC) - 12 meses** **Incluye: Instalación y Configuración**	2001	S/ 55.10	S/ 110,255.10
ISO	**Servicios SISCOTEC** *** Soporte Técnico Siscotec 8x5 para las 2001 Licencias SPC - (12 Meses)**	1	S/ 6,173.08	S/ 6,173.08

NOTA:			
Los Precios estan Expresados en Soles.		SubTotal:	S/ 116,428.18
	IGV	18%	S/ 20,957.07
		Total:	S/ 137,385.25

Plazo de Entrega:	15 Días una vez recibida la Orden de Servicio	Nombre del Vendedor	
Validez de la Oferta:	30 días	Javier Ruiz	
Entregables:	Licencias Electrónicas	Cargo	
Lugar de Entrega:	Mail del Cliente y con la Factura electrónica	Gerente Comercial	
Forma de Pago:	Factura 30 días	eMail	
Tiempo de Servicio:	12 Meses	javier.ruiz@siscotec.com	
Soporte:	Servicio de Soporte Avanzado - 8x5		

Para confirmar su Orden de Compra, por favor firme esta proforma en la linea de abajo y envíela vía eMail.

Firma y Sello Autorizada	Nombre	Cargo	Fecha

Trend Micro™

SMART PROTECTION COMPLETE

Máxima seguridad para el endpoint con Trend Micro™ XGen™ proporcionada por su partner de seguridad de confianza

Las soluciones de seguridad tradicionales no pueden seguir el ritmo de las amenazas actuales. Volver a la fórmula de varios productos para hacer frente a la gran cantidad de desafíos sólo aumenta la complejidad, ralentiza a los usuarios y puede dejar huecos en su seguridad. Para complicar aún más las cosas, usted está migrando a la nube y necesita opciones de despliegue de seguridad flexibles que sean capaces de adaptarse a medida que cambien sus necesidades. Es necesario contar con una seguridad multidimensional que consolide su visión a través de todas las capas de protección y todos los modelos de despliegue.

Trend Micro™ Smart Protection Complete es una suite interconectada con capacidades de seguridad que ofrece protección a los usuarios sin importar dónde van o lo que hacen. Esta moderna seguridad ofrece la mejor protección en múltiples capas: endpoint, aplicación y red, trabajando de forma conjunta para detener las amenazas en toda la organización. El núcleo de la suite reside en XGen™ endpoint security, que aplica high-fidelity machine learning en un conjunto de técnicas de protección contra amenazas para eliminar las brechas de seguridad en cualquier actividad del usuario y en el endpoint. Además, puede mejorar la protección de su negocio a medida que este evoluciona gracias a la flexibilidad de los modelos de implementación in situ, en la nube e híbrido, que se adaptan a su entorno tecnológico actual y futuro. La carga administrativa está minimizada con la gestión centralizada a través de múltiples vectores de amenaza desde un único "panel de control", que proporciona visibilidad completa de la seguridad de su entorno.

Múltiples capas de protección frente a amenazas conectadas

Esta completa suite integra la seguridad a través de las capas de protección con un despliegue cloud flexible, concesión de licencias simplificada y gestión centralizada para la visibilidad de la red y el control de amenazas y datos. Esta suite incluye las siguientes capas de seguridad:

- **SEGURIDAD ENDPOINT.** XGen™ endpoint security sintetiza y aglutina el machine learning con otras técnicas para ofrecer máxima protección. Asegura la actividad del usuario en desktop físicos y virtuales, laptops o dispositivos móviles con protección de datos y frente a amenazas, control de aplicaciones, protección de vulnerabilidades y cifrado.
- **SEGURIDAD MÓVIL.** Protege, rastrea, supervisa y gestiona los dispositivos móviles de los empleados y los datos corporativos con seguridad, equilibrando el fenómeno de la consumerización con el control TI.
- **SEGURIDAD PARA EL CORREO ELECTRÓNICO Y COLABORACIÓN.** Ofrece protección superior contra spam, phishing, malware y ataques dirigidos al servidor, al gateway o a las aplicaciones en la nube como Office 365.
- **SEGURIDAD WEB.** Protege la actividad web de los usuarios en cualquier dispositivo y lugar. Ellos ganan un acceso seguro a las últimas aplicaciones web y medios sociales, y usted obtiene visibilidad completa y control del uso que hace su empleado de la web en modo SaaS basado en cloud, o con una solución para el gateway de Internet segura desplegada in situ.
- **GESTIÓN CENTRALIZADA DE LA SEGURIDAD.** Gestiona múltiples capas conectadas de protección de datos y amenazas para una visibilidad integral y centrada en el usuario a través de todo el ciclo de vida de la amenaza

Puntos de Protección

- Endpoints
- Smartphones y tablets
- USB y unidades extraíbles
- Servidores de correo
- Servidores de archivos
- Gateway de mensajería
- Gateway web
- Portales de colaboración
- Servidores IM
- Intercambio de archivos e email en la nube

Protección de Amenazas y Datos

- Ransomware
- Malware desconocido
- Ataques dirigidos
- Firewall endpoint and prevención de intrusiones en el host
- Protección de vulnerabilidades
- Control de aplicaciones
- Contenido inapropiado
- Ataques de phishing
- Spam y bots
- Spyware y rootkits
- Virus y troyanos
- Amenazas web

Protección de Datos y Cumplimiento

- Riesgos de incumplimiento
- Pérdida de dispositivos
- Pérdida de datos accidental
- Robo de datos

Principales beneficios

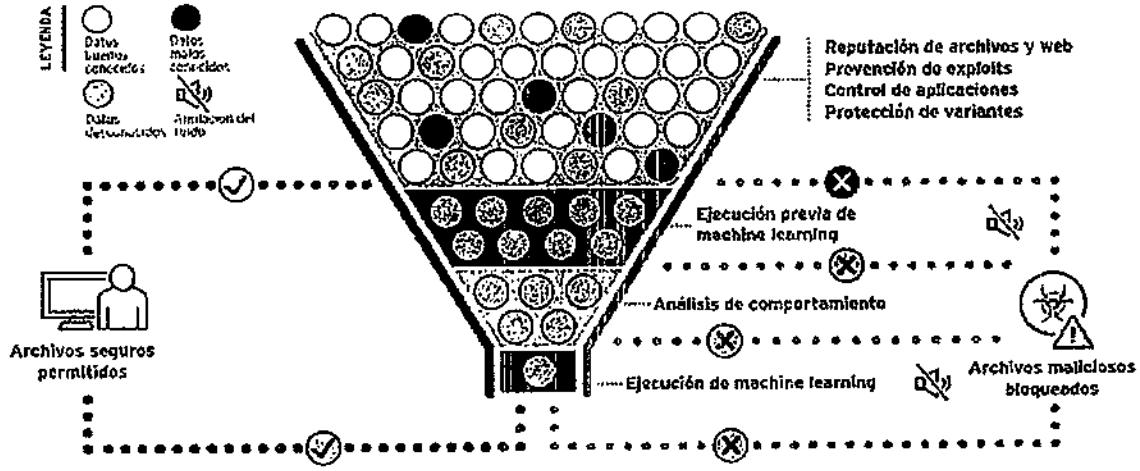
- Recupera el control del entorno TI del usuario final mediante la centralización de la protección de datos y amenazas a través de las capas de seguridad
- Detiene al ransomware de cifrar sus endpoints
- Bloquea el malware zero-day con técnicas sin firma
- Permite a los usuarios trabajar con seguridad desde las plataformas que les son más productivas
- Protege los datos sin incrementar el impacto en la gestión o en el cliente
- Minimiza los riesgos con cualquier combinación de seguridad cloud en tiempo real y de forma proactiva
- Reduce la complejidad de gestión y los costes totales

VENTAJAS

Máxima protección

XGen™ endpoint security

Aplica high-fidelity machine learning con otras técnicas de detección para ampliar la protección contra el ransomware y los ataques avanzados.



- Filtra las amenazas progresivamente utilizando las técnicas más eficaces para maximizar la detección sin falsos positivos.
- Mezcla técnicas sin firma, incluyendo high-fidelity machine learning, análisis de comportamiento, protección de variantes, verificación de census, control de aplicaciones, prevención de exploits y verificación de archivos válidos con otras técnicas tales como la reputación de archivos, reputación Web y bloqueo de comunicaciones de comando y control (C&C).
- Gracias al high-fidelity machine learning es posible realizar análisis tanto antes como durante la ejecución, a diferencia de otros proveedores de machine learning que sólo utilizan una de las dos técnicas.
- Despliega técnicas de anulación de ruido como comprobación de census y de listas blancas en cada capa para reducir los falsos positivos.
- Aprovecha los 11 años de experiencia de Trend Micro en el uso de machine learning, filtrado de spam y análisis web.

Protección de datos

- Protege los datos con cifrado de carpetas, archivos y de disco completo para mantener la privacidad de los mismos
- Control de dispositivos para evitar que la información se traspase a lugares donde no debe estar, como memorias USB o almacenamiento cloud.
- Seguridad móvil que protege los dispositivos móviles de sus empleados y los datos de la compañía con gestión de dispositivos móviles (MDM) y protección de datos.
- Prevención de pérdida de datos (DLP) integrada y basada en plantillas para proteger los datos sensibles a través del endpoint, web, email y apps SaaS.

Protección de Email y Web

- Altas valoraciones de forma sistemática en seguridad para el correo electrónico a la hora de detener y evitar que ataques de email dirigidos, spam, phishing ransomware y malware desconocido impacten y afecten a su negocio.
- Detiene las amenazas antes de que lleguen a los usuarios con técnicas de detección avanzadas incluyendo detección de exploits en documentos y análisis de malware en sandbox.
- Seguridad para el servidor de correo electrónico, el gateway, portales de colaboración, mensajería instantánea y aplicaciones cloud tales como Office 365.
- La seguridad del gateway web protege a los usuarios contra las amenazas procedentes de la web y ofrece control granular y visibilidad de uso de la web.

Defensa de Amenazas Conectada

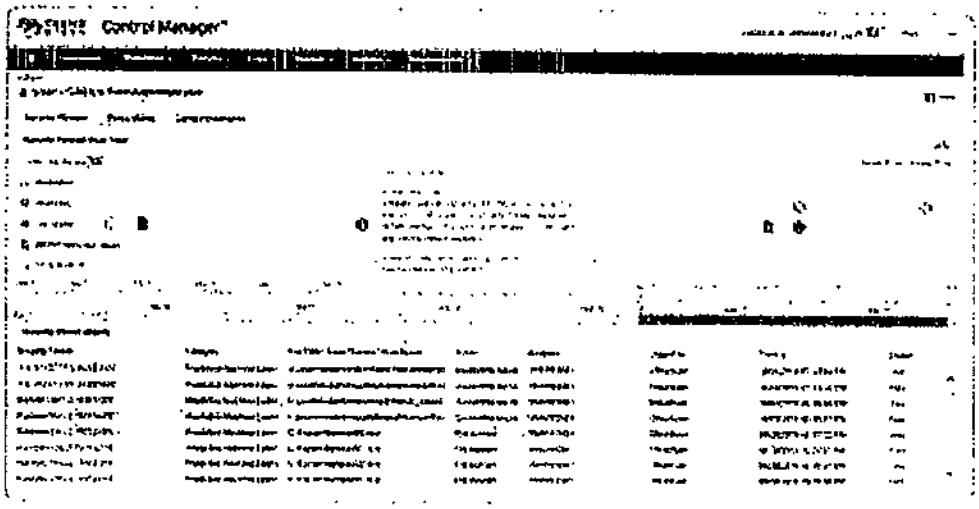
- Comparte información de forma instantánea de la actividad sospechosa en la red con archivos y otras capas de seguridad para detener ataques posteriores
- Reduce el tiempo de protección contra ataques emergentes y dirigidos.

Impacto mínimo

Protección de datos

Alto rendimiento y detección precisa:

- Seguridad ligera y optimizada que utiliza la técnica de detección correcta en el momento adecuado para asegurar un impacto mínimo en dispositivos y redes.
- Emplea múltiples métodos y controles contra los falsos positivos reduciendo así la necesidad de contactar con el soporte de TI.



Visibilidad y gestión centralizada

- Visión centralizada e integral de la seguridad del usuario que permite analizar datos y amenazas en toda la solución de forma rápida y eficaz
- Visibilidad centrada en el usuario a través de entornos cloud y on-premise que permite comprender de forma fácil cómo afectan las amenazas a un usuario particular a través de múltiples sistemas.
- Intercambio automático de inteligencia de amenazas a través de las capas de seguridad permitiendo la protección contra amenazas emergentes en toda la organización
- Consolas personalizables adaptadas a cada nivel de responsabilidad administrativa.

Gestión y permisos de licencias flexible:

- Flexibilidad para desplegar la seguridad endpoint de la forma que mejor soporte los cambiantes modelos de negocio, ya sea en entornos on-premise o en la nube.

  Combina y une productos cloud u on-premise sin cambios en el acuerdo comercial.

Soporte extraordinario

- Soporte 24x7, lo que significa que ante un problema Trend Micro estará ahí para resolverlo rápidamente

Partner de seguridad perfecto

Trend Micro cuenta con una historia de innovación constante para ofrecer las tecnologías de seguridad más eficaces y eficientes. Siempre estamos mirando hacia el futuro para desarrollar los avances necesarios en la lucha contra las amenazas en constante cambio.

- Más de 25 años innovando en seguridad.
- Más de 155 millones de endpoints protegidos.
- Con la confianza de 45 de las 50 principales multinacionales de todo el mundo.
- Líder desde 2002 en el Magic Quadrant de Gartner para Plataformas de Protección Endpoint y posicionada en la parte más a la derecha del cuadrante de «Integridad de Visión» de 2016

TREND MICRO SMART PROTECTION COMPLETE

Construye una base sólida de seguridad en la red para la protección completa del usuario final con una amplia plataforma que proporciona seguridad para entornos heterogéneos y protección para la configuración de red única.

COMPONENTES DE LA SUITE

PROTECCIÓN MULTICAPA	PLATAFORMA COMPATIBLE	VENTAJA
Gestión Centralizada		
Control Manager	Software: Windows	Gestión de seguridad centralizada
Seguridad Endpoint		
OfficeScan	Software: Windows, Apple Macintosh	Detección proactiva de amenazas aplicando machine learning para clientes Windows físicos y virtuales. Arquitectura plug-in extensible que se implementa y administra desde una única consola.
Vulnerability Protection	Software: Windows	Protege contra las vulnerabilidades en sistemas operativos y aplicaciones cliente con un Sistema de Prevención de Intrusiones Host (HIPS) a nivel de red.
Endpoint Application Control	Software: Windows	Protección de datos y equipos contra accesos sin autorización, errores de usuario, bloquea los endpoints para evitar que se ejecuten aplicaciones no deseadas o desconocidas.
Endpoint Encryption	PCs, portátiles, CDs, DVDs, y USB	Asegura los datos almacenados en PC, portátiles, CD, DVD y unidades USB con cifrado completo del disco, carpetas, archivos y medios extraíbles con gestión de claves y políticas multi-OS.
Worry-Free Services	SaaS basado en Cloud	Protección de amenazas proactiva gestionada en modo SaaS para clientes Windows, Mac y Android.
Server Protect	Windows/Netware, Linux	Mantiene el malware fuera del servidor de ficheros.
Seguridad Móvil		
Mobile Security	iOS, Android, Blackberry, Symbian y Windows Mobile	Gestión de dispositivos móviles (MDM), seguridad de datos, seguridad móvil antimalware y web, y gestión de aplicaciones.
Seguridad para Colaboración y Correo Electrónico		
Hosted Email Security	SaaS basado en Cloud: protege el tráfico de email hacia sistemas de correo electrónico cloud o on-premise	Protección continuamente actualizada para detener spam y virus antes de que lleguen a la red.
Cloud App Security	SaaS basado en Cloud: email Office 365, SharePoint Online, Box for Business, Dropbox for Business, Google Drive	Refuerza la seguridad de Office 365 con análisis de malware en sandbox y prevención de pérdida de datos. Protege el intercambio de archivos del malware y de los riesgos de cumplimiento.
InterScan Messaging Security	• Software de Appliance Virtual: VMware, Hyper-V, Software Appliance • Software: Windows, Linux	Protege el gateway de correo electrónico del spam y otras amenazas de correo electrónico.
ScanMail Suite for Microsoft Exchange	Software: Windows	Bloquea spam, malware y otras amenazas de correo electrónico en el servidor de correo.
ScanMail Suite for Lotus Domino	• Software: Windows, Linux para x86, IBM AIX, IBM IS OS, Sun • Solaris™, Linux en IBM® zSeries, IBM z/OS	Bloquea spam, malware y otras amenazas de correo electrónico en el servidor de correo.
PortalProtect for Microsoft SharePoint	Software: Windows en SharePoint server	Asegura sus colaboraciones en SharePoint protegiéndolas del malware, las amenazas web y los riesgos de cumplimiento.
IM Security for Microsoft Lync	Software: Windows en Lync server	Protege las comunicaciones IM del malware, las amenazas web y los riesgos de cumplimiento.
Seguridad para el Gateway Web		
InterScan Web Security	• Software de Appliance Virtual: VMware, Hyper-V, Software Appliance • SaaS basado en Cloud	Protege a la actividad web de los usuarios. Funciones antimalware y de reputación web en tiempo real de primer nivel. Proporciona visibilidad completa y control con un control de aplicaciones granular, filtrado URL flexible y generación de informes completa.
Protección de Datos Integrada		
Data Loss Prevention	Integrada a través de endpoints, email y colaboración, y el gateway de seguridad web	Refuerza políticas DLP en toda la empresa utilizando plantillas sencillas y personalizables.

TREND MICRO

Securing Your Journey to the Cloud

electrodata

16/07/2018

GRUPO ELECTRODATA SAC
20516530686
Av. Principal 456 - Surquillo - Lima

Raul Moscol
995007866
(511) 4760808 – Ext. 213
rmoscol@electrodata.com.pe

Empresa: CONGRESO DE LA REPUBLICA

Referencia : Licenciamiento de Software de Seguridad

Ejecutivo Comercial Raul Moscol - rmoscol@electrodata.com.pe - 995007866

"Licenciamiento de Software de Seguridad"

#	P/N	Descripcion	Cant.	Precio de Costo Unitario S/	Precio de Costo Total S/
1	Lic_Symantec	Licenciamiento de Software de Seguridad Marca: SYMANTEC Productos: * Symantec™ Protection Suite Enterprise Edition 12 meses Incluye: Instalación y Configuración	2001	S/ 160.00	S/ 320,160.00
2	ST8x5	Soporte Técnico para las 2001 Licencias - (12 Meses)	1	S/ 12,500.00	S/ 12,500.00
		Precio de Venta Subtotal S/			S/ 332,660.00
		Precio de IGV S/			S/ 59,878.80
		Precio de Venta Total S/			S/ 392,538.80

Details / Detalles

Moneda	Soles
Forma de Pago	Factura 30 días
Plazo del servicio	12 meses
Validez de la oferta	La cotización tiene validez de 25 días útiles desde su presentación.

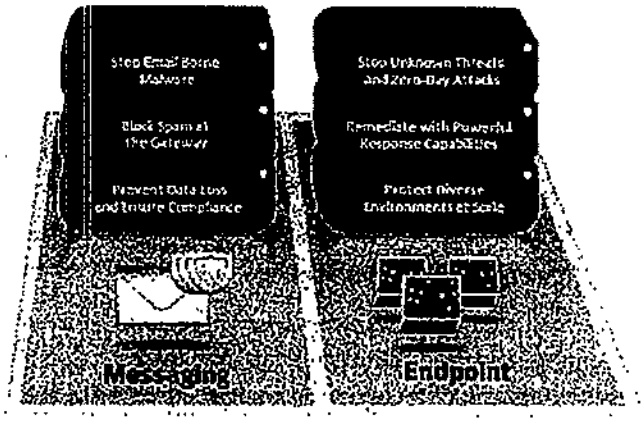
Symantec™ Protection Suite Enterprise Edition

Comprehensive, powerful endpoint and messaging protection for less money

Data Sheet: Endpoint Security

Multilayered Protection from Endpoint to Gateway

Securing your business is challenging, but made easier with Symantec™ Protection Suite Enterprise Edition. Protect against more threats and secure your environment against data loss, malware, and spam by accurately identifying and addressing risks consistently across different platforms. Multiple layers of protection fuse next generation and essential technologies to ensure you are accurately identifying and addressing risks while delivering consistent protection in both physical and virtual environments. Symantec combines the broad spectrum of necessary security protections across your endpoint with industry-leading messaging infrastructure to keep you safe.



Fastest, most effective security - Powered by next generation and essential technologies, you can confidently protect your infrastructure with industry-leading endpoint and messaging security, with data protection solutions built to secure your physical and virtual environments.

Layered security and intelligence - efficiently manage your endpoint and mail system's security with real time actionable intelligence across protection technologies.

More protection, for less - Increase the security posture across your IT infrastructure, while reducing upfront and on-going IT costs and force out unnecessary complexity.

Fastest, Most Effective Security

Endpoint security

Protection Suite delivers advanced threat prevention that protects your endpoints—laptops, desktops, and servers—from targeted attacks and attacks not seen before. Proactive technologies automatically analyze application behaviors and network communications to detect and block suspicious activities, including administrative control features that allow you to deny specific devices and applications.

- **Symantec next generation protection** - Advanced Machine Learning stops unknown threats before they can execute, Memory Exploit Mitigation blocks zero-day exploits of vulnerabilities in common applications, and more.
- **Patented technology** - Insight separates files at risk from those that are safe, for faster and more accurate malware detection on Windows and Mac laptops, desktops, servers, and messaging gateways.
- **Proactive threat protection** - Real Time SONAR behavioral analysis examines programs as they run, identifying and stopping malicious behavior even for new and previously unknown threats.

1. AV-Test. Product Review. Corporate Solutions for Windows 7. April 2015

- **Protection for virtual environments**—Integration with VMware vShield protects your virtual infrastructure with virtual image exception, resource leveling, shared Insight cache, virtual client tagging to optimize your virtual environment's security posture.
- **Antivirus and antispyware for Windows®, Linux®, and Macintosh®**— Provides unmatched malware protection, market leading antivirus, new emulator capabilities, reduced footprint and improved network performance.
- **Advanced content filtering** - Identify and control the flow of sensitive data in email and IM to catch more than 99% of spam and prevent data loss.
- **Deeper security insights** - The world's largest civilian threat intelligence network provides deeper understanding into local and global threat landscape.

Layered Security and Intelligence

Effective email security with layered messaging and spam protection

Identify emerging threats and accelerate time to protection based on relevant, actionable intelligence. Protection Suite delivers inbound and outbound messaging security, with accurate real-time antispam and antivirus protection, advanced content filtering, and data loss prevention. Protection Suite messaging security components can be deployed on your messaging server and at the gateway (physical or virtual appliance-based).

- **Context-aware security management** - Correlate data from endpoint, messaging and third-party security products with early warning alerts from the world's largest civilian threat intelligence network.
- **VMware® vShield integration** - The Shared Insight Cache functionality integrates with vShield Endpoint
- **Spam and Malware Protection for email** - Symantec™ Messaging Gateway and Symantec™ Mail Security for Exchange blocks email born threats and more than 99 percent of spam with less than 1 in a million false positives.
- **Content filtering of inbound and outbound traffic** – comply with industry and government regulations.
- **Safeguard sensitive information** - identify and control the flow of sensitive information via email with advanced content filtering and data loss prevention.

More Protection for Less

Maximize protection, minimize complexity, and stay under budget

Protection suite is a cost efficient way to deploy security technologies across your IT infrastructure. Reduce upfront and ongoing IT costs by forcing out complexity—Symantec technologies are centrally managed and work seamlessly together.

- **Cost efficient** - Solve crucial security challenges across multiple threat vectors, while saving up to 70 percent over the purchase of individual point products.
- **Eliminate environment complexity** - Deploy a unified solution including endpoint and messaging security.
- **Streamline processes** - Eliminate additional steps and costs with one decision, one purchase, and one vendor for comprehensive protection.

Component Products of Protection Suite

The products included within the Symantec Protection Suite Enterprise Edition (including system requirements) are:

- Symantec Endpoint Protection (Windows, Linux, and Macintosh)
- Symantec Mail Security for Microsoft Exchange
- Symantec Messaging Gateway

More Information

To speak with a Product Specialist in the U.S.
Contact your Symantec Security Specialist or call Symantec Partner Hotline (888)780-7962.

To speak with a Product Specialist outside the U.S.
For specific country offices and contact numbers, please visit our Symantec Partner Website:
www.symantec.com/partners

Americatel
una empresa del grupo entel

Lima, 24 de julio de 2018

Empresa:	CONGRESO DE LA REPUBLICA
Referencia :	Licenciamiento de Software de Seguridad

"Licenciamiento de Software de Seguridad"

#	P/N	Descripcion	Cant.	Precio de Costo Unitario S/	Precio de Costo Total S/
1	CETP	Licenciamiento de Software de Seguridad Marca: Mcafee Producto: * McAfee Endpoint Protection—Advanced Suite 12 meses Incluye: Instalación y Configuración	2001	S/ 149.50	S/ 299,149.50
2	ST - 8x5	Soporte Técnico para las 2001 Licencias - (12 Meses)	1	S/ 13,200.00	S/ 13,200.00
		Precio de Venta Subtotal S/			S/ 312,349.50
		Precio de IGV S/			S/ 56,222.91
		Precio de Venta Total S/			S/ 368,572.41

Razón social	Americatel Perú S.A.
N° RUC	20428698569
Correo Electrónico	framos@americatel.com.pe
Teléfono fijo	710-1426
Persona de contacto	Fernando Ramos
Condiciones comerciales	-
Plazo de servicio	12 meses
Validez Oferta	60 días calendario
Forma de pago	Factura a 30 días

Victor Valle Meléndez
Gerente Comercial TIC
Victor José Roberto Valle Meléndez
Representante legal
Americatel Perú S.A.

McAfee
Together is power.

McAfee Endpoint Protection—Advanced Suite

Protection against zero-day attacks and help with regulatory compliance

A mobile workforce plus increased regulation could equal a security nightmare. With integrated, proactive security to combat sophisticated malware and zero-day threats, McAfee® Endpoint Protection—Advanced Suite, part of the McAfee product offering, protects endpoints when they leave your network and helps protect your network when they return. Its integrated intrusion prevention secures desktops and laptops from advanced threats. Centralized policy-based management, multiplatform support, and auditing keep all of your endpoint assets safe and compliant.

Key Advantages

- Guard Microsoft Windows, Mac, and Linux devices against system, data, email, and web threats, and the risk of noncompliance.
- Consolidate endpoint and data security efforts with an integrated solution from one vendor—securing stronger protection at a lower cost.
- Enable increased protection immediately, with the simplicity and efficiency of centralized management and an extensible endpoint security framework.

The increasing sophistication of attackers is challenging security practitioners to have the visibility and tools they need to detect and defend against advanced threats. Although every endpoint is at risk from the subtle technologies criminals use today, portable systems face extra threats. Laptops venture to hotels, coffee shops, and home offices without traditional protective layers, such as web and email gateways, network firewalls, and network intrusion prevention systems. On a Wi-Fi network, anyone might listen and pick up more than the news.

PCs can miss patches and other updates, becoming even more vulnerable to zero-day threats by simply being disconnected from the corporate network. And those patches and other updates are increasingly required for regulatory compliance. Beyond more stringent industry regulations, your governance controls may expect you to manage distribution of sensitive data as well as appropriate web use—on-site or on the road.

McAfee® Endpoint Protection—Advanced Suite puts you in charge with broad protections, compliance controls, and unified management. Whether you want to keep viruses, hackers, spammers, data thieves, or auditors at bay, this seamless solution has the perfect combination of capabilities and cost savings.

Intelligent, Collaborative Defenses

Organizations need a strategy for threat protection, detection, and correction, as well as a security framework that empowers security components to collaborate against targeted attacks for rapid detection and action. That's why McAfee Endpoint Security 10 (included with the suite), communicates with multiple

endpoint defense technologies in real time to analyze and collaborate against new and advanced threats—blocking and quickly halting them before they impact your systems or users. Its framework helps remove duplicate technologies and connect other McAfee solutions to enable simpler management and stronger defenses. Additionally, McAfee Global Threat Intelligence (McAfee GTI) provides insights from the largest volume of observations and analysis available in the market.

Advanced Email Virus and Spam Protection

Our solution scans your inbound and outbound emails to intercept spam, inappropriate content, and harmful viruses. We can quarantine suspicious emails to prevent evolving email threats from affecting your network and users. And, a layer of antivirus on your email server prevents malware from reaching user inboxes.

Zero-Day and Vulnerability Shielding

Say goodbye to emergency patching. Exploit and intrusion prevention technologies patrol your desktops and laptops against malware, block malicious code from hijacking an application and trying to run with higher privileges, and provide automatically updated signatures that shield laptops and desktops from attack. It's safe to implement and test patches on your schedule. Combined with our patented behavioral protection, which prevents buffer overflow attacks, you get the most advanced system vulnerability coverage on the market.

Integrated Firewall

Bar unsolicited inbound traffic and control outbound traffic with our integrated firewall, which uses McAfee GTI to protect desktops and laptops from botnets, distributed denial-of-service (DDoS) attacks, advanced persistent threats, and risky web connections. Systems are also protected by allowing only outbound traffic during startup until the complete firewall policy has been enforced.

Efficient Policy Auditing and Compliance

Agent-based policy auditing scans your endpoints and documents to ensure that all policies are up to date. Organizations can measure compliance to best practice policies—ISO 27001 and CoBIT—as well as to key industry regulations.

Comprehensive Device Control

Prevent critical data from leaving your company through USB drives, Apple iPods, Bluetooth devices, recordable CDs, and DVDs. Tools help you monitor and control data transfers from all desktops and laptops—regardless of where users and confidential data go, even when users are not connected to the corporate network.

Why Choose McAfee?

- We offer a true centralized experience for administrators.
- Our integrated endpoint and security frameworks help you remove redundancies, connect other solutions, and provide an extensible architecture to build on.
- McAfee Global Threat Intelligence offers the strongest volume of threat intelligence on the market. We see and protect more than anyone else.

Proactive Web Security

Help ensure compliance and reduce risk from web surfing by warning users about malicious websites before they visit. Host-based web filtering ensures that you can authorize and block website access, protecting users and ensuring their policy compliance whenever and wherever they are web surfing. Lastly, private URLs can also be blocked, and the latest versions of multiple web browsers are supported.

Management that Lowers Operational Costs

For efficiency and comprehensive visibility across your security and compliance status, McAfee® ePolicy Orchestrator® (McAfee ePO™) software provides a single, centralized, platform that manages security, enforces protection, and lowers the cost of security operations.

Correlate threats, attacks, and events from endpoint, network, and data security, as well as compliance audits, to improve the relevance and efficiency of security efforts and compliance reports. No other vendor can claim a single integrated management platform across all these security domains. McAfee ePO software simplifies security management.

Deploy Quickly and Easily

Enable increased protection without delay. The EASI installer gets your strong protection running in as few as four clicks. Integration with McAfee ePO software lets you deploy and manage security using a single environment.

Migration Made Easy

Environments with current versions of McAfee ePO software, McAfee VirusScan® Enterprise, and the McAfee agent can leverage our automatic migration tool to migrate your existing policies to McAfee Endpoint Security 10 in about 20 minutes or less.

Feature	Why You Need It
Single integrated management	Instant visibility into security status and events and direct access to management for unified control of all your security and compliance tool with McAfee ePO software
Multiplatform	Protects the full range of endpoints required by mobile and knowledge workers, including Mac, Linux, and Microsoft Windows
Device control	Lets you monitor and restrict data copied to removable storage devices and media to keep it from leaving company control
Intrusion prevention system (IPS) and integrated firewall for desktops and laptops	Provides zero-day protection against new vulnerabilities, which reduces the urgency to patch, and controls desktop applications that can access the network to stop network-borne attacks
Anti-malware	Blocks viruses, Trojans, worms, adware, spyware, and other potentially unwanted programs that steal confidential data and sabotage user productivity
Anti-spam	Helps eliminate spam, which can lead unsuspecting users to sites that distribute malware and phish
Web control with URL filtering and safe search	Helps ensure compliance, warns users before they visit malicious websites, and protects them whether they are on or off the corporate network
Email server security	Protects your email server and intercepts malware before it reaches the user inbox
Policy auditing	Provides tightly integrated compliance reporting for HIPAA, PCI, and more

Learn More

For more information, visit www.mcafee.com/endpoint, or call us at 1 888 847 8766, 24 hours a day, seven days a week.

* The migration time is dependent on your existing policies and environment.

McAfee
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

417_0816
AUGUST 2016