GOBIERNO REGIONAL DEL CALLAO

INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE DE SEGURIDAD ANTIVIRUS PARA SERVIDORES Y ESTACIONES DE TRABAJO N° 001-2013-GRC/GGR/OTIC

1. GERENCIA
Gerencia General Regional

2. OFICINA
Oficina de Tecnologías de la Información y Comunicaciones

3. RESPONSABLE DE LA EVALUACION
ING. ELMER NEGREIROS MATTA

4. CARGO
Jefe de la Oficina de Tecnologías de la Información y Comunicaciones.

5. FECHA
28 de Febrero del 2013

6. JUSTIFICACION

Cumpliendo con la Norma Técnica Peruana "NTP-ISO/IEC 1779.9:2007 EDI". Tecnología de la Información código de buenas prácticas para la gestión de la seguridad de la información y con las Políticas de Seguridad en la función informática a nivel institucional y estado, según lo dispuesto en las Normas de Control Interno de la Contraloría General con Resolución N° 320-2006-CG.

El Gobierno Regional del Callao tiene como finalidad formular, aprobar, ejecutar, supervisar y evaluar; en armonía con la política general y los planes de gobierno, las políticas de alcance nacional, así como el aprovechamiento sostenible de los recursos. Para tal efecto, los funcionarios y profesionales hacen uso de Sistemas de Información y uso de herramientas de ofimática para la elaboración de una serie de documentación acorde a sus funciones.

OFICINA DE TECNOLOGIA DE LA INFORMACION Y COMUNICACIONES V°B° OTIC

El Gobierno Regional del Callao viene usando el antivirus Eset Nod32 con el cual se ha tenido problemas de infección en los equipos informáticos, con ánimos de salvaguardar el normal funcionamiento y la integridad de nuestra información evitando los ataques que se presenta en diferentes modalidades que van desde Denegación de Servicio, Desfacing, Hacking, hasta envío de correo electrónico con archivos adjuntos conteniendo software malicioso (malware) en la forma de Virus informático, troyanos, gusanos *y* otros modos de ataque.

Su puesta en servicio de un Antivirus potente debería permitir lo siguiente:

- Disminuir el riesgo de incidentes o eventos propiciados por virus informáticos que comprometan la seguridad.
- Mejorar la productividad de personal que labora en la Región Callao.
- Uso optimizado de ancho de banda y de los recursos de TI.
- Implementar políticas que definan distintas acciones a tomar al detectarse un virus, un ataque o un programa no deseado: limpiar el archivo infectado, moverlo a cuarentena, continuar la exploración, no tomar acción, eliminar el archivo, etc.
- Mantener un registro actualizado del nivel de protección contra virus de la plataforma informática del Gobierno Regional del Callao, pudiendo generar reportes personalizados por distintas variable, tales como: tipo de virus, acción tomada, nivel de actualización del motor de búsqueda, nivel de actualización de firmas de nuevos virus, etc.
- Detectar rápida y fácilmente riesgos de seguridad o problemas de productividad originados como resultado de la recepción de mensajes de correo electrónico infectados por virus informáticos y/0 por propagación de virus por motores SMTP propios.

Es necesario contar con esta solución para la seguridad de los Servidores y las Estaciones de la Red del Gobierno Regional del Callao, ya que permite disminuir los efectos producidos por virus informáticos y sus variantes. Por esta razón es de vital importancia evaluar software de antivirus, (de acuerdo a Ley); las mismas que deberán contar con mantenimiento por el periodo de al menos un (01) año, permitiendo mantener el producto actualizado con sus últimas versiones y los registros de firmas de los virus más recientes.

GERENCIA DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES
V°B°
OTIC

ALTERNATIVAS

Se ha tomado como referencia el Antivirus – Comparative - Summary Report 2012 http://www.av-comparatives.org/ (Antivirus – Comparative es una Organización austriaca con fines de lucro, que ofrece en forma libre e independiente prueba de software antivirus al público en general).

Se analizaron los siguientes productos:

- Eset Antivirus NOD32 (Smart Security)
- Kaspersky Endpoint Security (Bussines Space)
- Symantec (SEP 12)

GOBIERNO REGIONAL DEL CALLAO

8. ANÁLISIS COMPARATIVO TÉCNICO (Anexo 1)

Se aplicara el proceso de evaluación de software descrito en la Parte III de la Guía de Evaluación de Software aprobado por Resolución Ministerial N° 139-2004-PCM y la Ley N° 28612 que "Norma el uso, adquisición y adecuación del software de la administración pública".

A. PROPOSITO DE LA EVALUACION

Determinar los atributos o características mínimas para el Producto final del Software requerido.

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES V°B° OTIC

ANALISIS COMPARATIVO TECNICO

ANALISIS COMPARATIVO TECNICO	Kaspersky Lab	ESET	Symantec
	Kaspersky Endpoint Security 8 for Windows	Smart Secuirty 4 + Remote Administration Console	SEP 12
Control Aplicaciones			
Salida Predeterminada	✓	×	✓
Denegada por defecto	✓	×	✓
Soporte de excepciones	✓	×	×
Categoria Golden - Confianza de aplicaciones conocidas para realizar las actualizaciones por producto	✓	×	✓
Posibilidad de aplicar en determinados grupos de usuarios/ordenadores	✓	×	✓
Posibilidad de restringir determinadas acciones para aplicaciones específicas o grupos (acceso al dispositivo, acceso al registro, la copia, procesos propios, etc.)	✓	×	×
Actualizaciones de Confianza	✓	×	✓
Inventario de Software	✓	×	✓
Inventario de Aplicaciones en toda la Red	✓	×	×
Categorizar las Aplicaciones en toda la Empresa	✓	×	×
Test de prueba	✓	×	✓
Reputación de Objetos (basada en cloud)	✓	×	✓
Aplicación confianza (usuario es capaz de enviar la solicitud a través de la interfaz como administrador)	✓	×	×

GOBIERNO REGIONAL DEL CALLAO

Posibilidad de restringir aplicaciones vulnerables	✓	×	×
Control de App - Categorización/lista blanca			
Categorización	✓	×	×
Alrededor de 100 KL-categorías definidas están disponibles	✓	×	×
250 Millones de archivos buenos conocidos	✓	×	×
integración en cloud (KSN)	✓	×	×
Creación flexible de grupos	✓	×	×
Integración con AD/LDAP	✓	×	×
Control de App - Lista Negra			
Lista Negra de Aplicaciones	✓	×	✓
Lista Negra de Grupos	✓	×	✓
Lista Negra por categorías	✓	×	×
Lista negra de calificaciones de seguridad	✓	×	×
Colaboración/Servicios de Reputación	.	.	.
Aplicación Monitor de actividad: Reputación	✓	×	×
Supervisar las aplicaciones en ejecución (incluso de confianza)	✓	×	×
Agrupar las aplicaciones basadas en la confianza (evaluación de fuentes)	✓	×	×
Base de Firmas	✓	×	×
Analiza módulos de protección	✓	×	×
reputación cloud (KSN puntaje)	✓	×	×
programas de confianza	✓	×	×
web sites de confianza	✓	×	×
programas sospechosos	✓	×	×
web sites sospechosos	✓	×	×
Sistema de Detección Urgente (UDS)	✓	×	✓
Control de dispositivos			

GOBIERNO REGIONAL DEL CALLAO

Control de dispositivos en el nivel de bus	✓	×	✓
Denegación por defecto para dispositivos	✓	×	✓
Lista blanca basado en números de serie	✓	×	×
Permiso de lectura/escritura granularidad	✓	×	✓
Integración con AD	✓	×	✓
Control Web			
Filtro URL	✓	×	×
Categorización de Web Site	✓	×	×
Las restricciones de acceso basado en categoría web (red social, juegos, porno etc.)	✓	×	×
Reglas flexibles & programación	✓	×	×
Integración con AD	✓	×	×
Informes sobre navegación web actividad por PC	✓	×	×

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES
V°B°
OTIC

Protección anti-malware (forma clásica)			
Firma basada tecnología	✓	✓	✓
Frecuencia de actualización (estimación)	1 hora	8 horas	4-6 horas
Según la demanda y en acceso tareas de escaneo	✓	✓	✓
Cloud disponibilidad de la actualización (KSN)	✓	✓	✓
Archivo Reputación/comentarios de malware en la nube	✓	×	✓
Nivel bajo de escaneo (QScan)	✓	✓	×
File Antivirus	✓	✓	✓
Anti-Spyware	✓	✓	✓
Web Antivirus	✓	✓	✓
Mail Antivirus	✓	✓	✓
IM Antivirus	✓	×	×
P2P Antivirus	×	×	×
Escaneado inteligente (exclusión de archivos ya escaneados)	✓	×	✓
Protección Avanzada			
Protección proactiva	✓	✓	✓

GOBIERNO REGIONAL DEL CALLAO

Análisis de actividad de aplicaciones	✓	×	✓
Roll-back de actividad maliciosa	✓	×	×
Análisis de las amenazas de emulación de aplicación	✓	×	×
Protección Web			
Anti-phishing y lista negra de sitios de malware	✓	×	×
Anti-Spam	×	✓	✓
Protección en Red			
Firewall	✓	✓	✓
Sistema de detección de intrusos (IDS) - red de seguimiento actividad típica de los ataques a la red	✓	✓	✓
Soporte para VM			
Reconocer y administrar los productos instalados en la máquina virtual	✓	✓	✓
Escanear Offline imágenes VM	×	×	✓
Caché compartida en la lectura	✓	×	✓
Agente de Comunicación			
Agente independiente	✓	✓	×
Perfil de conexión	✓	✓	✓
Instalación			
Desinstalar productos de la competencia al realizar la instalación	✓	×	✓
Tarea para la desinstalación de la competencia	✓	×	×
Inventario de Software de la competencia	✓	×	×
Desinstalación actualizando los scripts	✓	×	×
Scripts personalizables	✓	×	×
Administración remota de la aplicación			
Administración de la consola	✓	✓	✓
Posibilidad de instalar los clientes de forma remota	✓	✓	✓
Capacidad para gestionar los clientes de forma remota	✓	✓	✓

OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES
V°B°
OTIC

GOBIERNO REGIONAL DEL CALLAO

Consola Web	✓	×	✓
Despliegue basado en aplicación de terceros	✓	×	×
Gestión centralizada para el Control de la aplicación	✓	×	✓
Gestión centralizada de Control de dispositivo	✓	×	✓
Gestión centralizada de control Web	✓	✓	✓
Gestión centralizada de vulnerabilidades	✓	×	×
Cuarentena centralizada	✓	✓	×
Copia de seguridad centralizada de eliminar archivos maliciosos	✓	✓	×
Pre-definir agrupación de equipos basada en estado	✓	×	×
Gestión remota / Soporte Multi Plataforma			
Windows endpoints	✓	✓	✓
Mac endpoints	✓	×	✓
Linux endpoints	✓	×	×
Mobile devices	✓	×	×

OFICINA DE TECNOLOGIA DE LA INFORMACION Y COMUNICACIONES
V°B°
OTIC

Soporte de Base de Datos			
MS SQL Server Express	✓	✓	×
MS SQL Server Enterprise	✓	✓	✓
MySQL	✓	×	×
Oracle	×	×	×
Firebird	×	×	×
Ultra portátil y alta disponibilidad			
Conmutación automática	✓	×	×
Recuperación de Desastres (Copia de seguridad, ...)	✓	✓	×
Registros & Reportes			
Control de actividades de aplicación	✓	×	✓
Integración con AD	✓	×	✓
Personalización de reportes	✓	✓	×
Personalización dashboard	✓	×	×

GOBIERNO REGIONAL DEL CALLAO

Exportación de reportes	✓	✓	✓
Monitorización de vulnerabilidad de aplicaciones	✓	x	✓

ANTIVIRUS PARA SERVIDORES Y ESTACIONES DE TRABAJO

ITEM	ATRIBUTOS	DESCRIPCION
ATRIBUTOS INTERNOS		
1	Sistemas Operativos Estaciones de Trabajo	Windows XP/Vista/Windows 7; 32/64 bits
2	Sistemas Operativos de Servidores de Red	Windows Server 2003/2008/2012; 32/64 bits
3	Actualización de firmas	Debe ser manuales y automáticas (programadas) del fichero de firma de virus y del motor de búsqueda en los servidores y en las estaciones de trabajo desde internet; Debe brindar la creación de repositorios distribuidos y programados.
4	Protección Proactiva	La solución debe contar con una tecnología de detección proactiva de amenazas conocidas y desconocidas que detecte malware antes de su ejecución (pre-execution) y en ejecución (on-execution).
5	Protección contra la perdida de información	La solución debe contar con un sistema del mismo fabricante que permita controlar o bloquear el uso de dispositivos, grabadores CD/DVD y lectores externos, dispositivos wireless como WIFI y Bluetooth; mediante la creación y administración de políticas de uso de dispositivos las cuales permitan cumplir con los requerimientos de seguridad de información.
6	Control y Productividad en la Red	El sistema de control de aplicaciones debe ser mantenida por el fabricante y deberá actualizar las categorías en forma automática, no se aceptaran soluciones que necesiten la intervención del administrador para mantener al día dichas categorías y/o listas de aplicaciones a controlar.
7	Compatibilidad	Con los sistemas operativos de Microsoft y Linux
8	Instalación	La instalación del software a las computadoras de los usuarios deberá ser mediante: - Sincronización de Directorio Activo. - La instalación debe ser a través de la consola de administración. - Adicionalmente debe permitir instalar por medio de CD o USB.
ATRIBUTOS EXTERNOS		
1	Consola de Administración	La herramienta debe contar con una consola de Administración desde donde se pueda administrar y controlar la solución antivirus en forma centralizada.

OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES – V°B° OTIC

2	Protección y defensa frente a malware en estaciones y servidores	La solución de seguridad para estaciones y servidores; debe ser de tipo integrada; es decir debe incluir un único agente que brinde protección frente a virus, spyware, adware, rootkits, comportamientos sospechosos, detección web de ataques, scripts maliciosos, pomdial/dialers, keylogers, hackers (firewall personal) y aplicaciones potencialmente peligrosos en todos los protocolos de red.
3	Escaneo	Permitir configurar la detección sobre todo los archivos o tipos de archivos comprimidos (cualquier formato de compresión rar, zip, cab, arj, arz) ocultos y archivos en ejecución. En tiempo real, bajo demanda, programado y remoto a través de la consola de administración.
4	Productividad	No deberá consumir muchos recursos de memoria y procesador en los equipos de los usuarios.
5	Protección en el Servidor de correo	Se requiere una solución que brinde seguridad y control de la información entrante y saliente de la red vía correo.
		ATRIBUTOS DE USO
1	Alertas y Reportes	La consola de administración deberá de ser capaz de notificar los eventos de virus a través de diferentes medios (correo electrónico, alertas de registros, etc.) Generar reportes gráficos imprimibles y exportables de la cobertura de versiones, actualizaciones e infecciones
2	Facilidad de uso	Toda solución deberá incluir capacitación a usuarios para el uso más fácil y rápido.
3	Seguridad de Protocolo	El producto debe contar con medidas de seguridad para el usuario de la estación de trabajo no deje sin efecto políticas corporativas a la vez que esté integrado con el agente NAC.
4	Proveedor	Debe contar con soporte técnico 24/7 escalable hacia la casa matriz incluido en la licencia y en español. El postor deberá presentar un documento del fabricante donde certifique que cuenta con este tipo de soporte.
5	Seguridad de Protocolo	Debe ser capaz de permitir al área de TI de la entidad lograr las metas especificas con exactitud e integridad, de acuerdo a las especificaciones técnicas y requerimientos de la organización.

OFICINA DE TECNOLOGIA DE LA INFORMACION Y COMUNICACIONES – V°B° OTIC

Legenda	
✘	No soporta
✓	Soporta

B. IDENTIFICAR EL TIPO DE PRODUCTO:
Software de seguridad antivirus para Servidores y Estaciones de trabajo.

C. ESPECIFICACION DEL MODELO DE CALIDAD:
Se aplicara el Modelo de Calidad de Software descrito en la Parte I de la Guía de Evaluación de Software aprobado por Resolución Ministerial N° 139-2004-PCM y la Ley N° 28612 que "Norma el uso, adquisición y adecuación del software en la administración pública".

D. SELECCIÓN DE METRICAS
Las métricas fueron seleccionadas en base al análisis de las características técnicas de los productos antivirus señalados en el párrafo A. PROPOSITO DE LA EVALUACION.

9. CONCLUSIONES

Del presente informe se concluye:

- Luego del análisis realizado, concluimos que las principales características evaluadas como son: frecuentes actualizaciones, control de aplicaciones, control web, protección avanzada, la instalación, la administración remota, el soporte multiplataforma, así también el registro y reportes, se determina finalmente el resultado de la evaluación a favor del software de seguridad antivirus para servidores y estaciones de trabajo **KASPERSKY ENDPOINT SECURITY (Bussines Space).**

10. FIRMA