INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE PARA ANTIVIRUS CORPORATIVO

Informe Técnico Previo de Evaluación de Software para Antivirus Corporativo

1. NOMBRE DEL ÁREA

Área de Tecnologías de la Información

2. RESPONSABLES DE LA EVALUACIÓN

Alberto Sánchez Espinoza
Asistente en Soporte Técnico

Rubén Valdez Guillen
Asistente en Soporte Técnico

3. FECHA

22 de Septiembre de 2015

4. JUSTIFICACIÓN

En cumplimiento a la Ley Nº 28612 (Ley que norma el uso, adquisición y adecuación del software en la Administración Pública) y su reglamento, se ha elaborado el presente informe, para determinar el software que cumpla con las necesidades de la entidad, bajo los principios de neutralidad, vigencia tecnológica y libre concurrencia.

PROINVERSION requiere proteger la información digital, almacenada en los equipos informáticos de la institución, de ser alterada, eliminada o copiada sin previo conocimiento del usuario responsable; mediante el empleo de programas no deseados como virus informáticos, troyanos, gusanos y otros modos de ataque dentro de la red institucional.

Este informe tiene como propósito, analizar las alternativas para implementar la solución que garantice identificar los peligros de este tipo de riesgo, lo cual ayudará a tomar acciones antes que las amenazas informáticas impacte negativamente en los recursos (activos) de la infraestructura de nuestra red. Así mismo se requiere que la solución permita implementar el Control de Acceso a la Red (NAC) en todas las áreas de la institución para comprobar que todos los equipos que acceden a la red que cumplan con las normativas y políticas de seguridad.

La vigencia de las licencias de nuestro actual antivirus finaliza el 29 de Septiembre del 2015, por lo que se requiere adquirir una solución de seguridad, para protección de las computadoras, laptops y servidores con los que cuenta la institución. La cantidad de licencias proyectadas para el presente año son de 330 para cubrir el parque informático, que garantice una adecuada protección a la red, aplicativos, bases de datos y servicios de Internet tales como: Portal Web, Correo Electrónico, Intranet y otros, de programas como los virus troyanos, Adware, Spyware, gusanos, rootkits y todo tipo de programa malicioso (malware) que dañen o afecten la integridad de la información, así como también pueda controlar el uso y/o instalación de aplicaciones que causen un impacto negativo en la productividad de los usuarios y en el uso de ancho de banda de la red.

5. ALTERNATIVAS

Para realizar este análisis comparativo técnico, se eligieron los siguientes productos:

- Bitdefender Endpoint Security
- Sophos Endpoint Protection Business
- Symantec Endpoint Protection 12.1

6. ANÁLISIS COMPARATIVO TÉCNICO

Este análisis será realizado aplicando lo dispuesto en la parte 4 de la guía de Evaluación de Software aprobada mediante Resolución Ministerial Nº 139-2004-PCM "Guía Técnica sobre Evaluación de Software en la Administración Pública"

Consideraciones previas:

Los productos serán evaluados en un entorno Windows Server 2008R2, y las computadoras personales con sistema operativo Windows Vista Business Edition SP1, Windows 7, Windows 8, Windows 8.1y Windows 10.

La adquisición del software para el Área de Tecnologías de la Información es requerida para renovar el sistema de protección antivirus de los equipos informáticos de PROINVERSION

7. MÉTRICAS DE EVALUACIÓN

Tenemos las siguientes métricas:

ITEM	ATRIBUTOS	DESCRIPCIÓN
	ATRIBUTOS INTERNOS	
1	Sistemas Operativos Estaciones de Trabajo	▲ Windows Vista /7/8/10/ de 32/64 bits ▲ La solución deberá soportar las versiones de 32 y 64bits.
2	Sistemas Operativos Servidores de Red	▲ Microsoft Windows Server 2003 32/64 bits, Windows Server 2008, 2008R2 y Windows Server 2012, 2012R2. ▲ Red Hat Linux, Opensuse Linux, Ubuntu Linux, Centos, Debian. ▲ La solución deberá soportar las versiones de 32 y 64bits para las plataformas descritas.
3	Actualizaciones de firmas	▲ Deben ser manuales y automáticas (programadas) del fichero de firmas de virus, del motor de búsqueda en los servidores y 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 Pérdida de Información	▲ La solución debe contar con un sistema del mismo fabricante que permita controlar o bloquear el uso de dispositivos USB, Grabadores CD/DVD, Floppy Drives, Lectores CD/DVD, HDD Externos y dispositivos Wireless como Wi-Fi; mediante la creación y administración de políticas de Uso de Dispositivos, las cuales permitan cumplir con los requerimientos de seguridad de la información.

6	Control y Productividad en la Red	▲ El sistema de control de aplicaciones y filtros debe ser mantenida por el fabricante y podrá opcionalmente actualizar categorías en forma automática. No se aceptarán soluciones que necesiten la intervención del administrador de la solución para mantener al día dichas categorías y/o listas de aplicaciones a controlar. ▲ El sistema deberá de contar con informes históricos de auditoria que permitan controlar la instalación de software no autorizado por la Institución.
7	Compatibilidad	▲ Con los sistemas operativos en las versiones antes mencionadas.
8	Instalación	▲ La instalación del software a las computadoras de los usuarios debe ser mediante: o Sincronización con el Directorio Activo de Microsoft o Servidor de Autenticación en Linux. o La Consola de Administración e Instalación mediante CD o recurso UNC (formato de dirección para especificar la ubicación del recurso).
ATRIBUTOS EXTERNOS		
9	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. Con posibilidad de integrar gestión y administración en la nube.
10	Protección y Defensa frente a malware en Estaciones y Servidores	▲ La solución de seguridad para estaciones y servidores debe ser Integrada; es decir debe incluir un único agente que brinde protección frente a virus, spyware, adware, rootkits, comportamientos sospechosos, detección web de ataques de scripts maliciosos, hackers (firewall personal) y aplicaciones potencialmente peligrosas en todos los protocolos de la red.

11	Escaneo	▲ Permitir configurar la detección sobre todos los archivos, o tipos de archivos, comprimidos (cualquier formato de comprensión, 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.
12	Productividad	▲ No deberá consumir muchos recursos de memoria y procesador en los equipos finales.
ATRIBUTOS DE USO		
13	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.
14	Facilidad de Uso	▲ Toda la solución deberá incluir capacitación a cuatro (04) usuarios en la manipulación y administración de la Consola.
15	Seguridad del Producto	▲ El producto debe contar con medidas de seguridad para que el usuario de la estación de trabajo no alterar las políticas corporativas a la vez que está integrado con el agente NAC de la solución.
16	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.
17	Eficacia	▲ Deberá ser capaz de permitir al área de TI de la entidad lograr las metas específicas con exactitud e integridad, de acuerdo a las especificaciones técnicas y requerimiento de la organización.

Niveles, escalas para las métricas

ITEM	ATRIBUTOS	ESCALAS
	ATRIBUTOS INTERNOS	
1	Sistemas Operativos Estaciones de Trabajo.	5
2	Sistemas Operativos Servidores de Red.	5
3	Actualizaciones de firmas.	5
4	Protección Proactiva.	7
5	Protección contra la Pérdida de Información.	7
6	Control y Productividad en la red.	7
7	Compatibilidad.	5
8	Instalación.	6
	ATRIBUTOS EXTERNOS	
9	Consola de Administración.	5
10	Protección y Defensa frente a malware en Estaciones y Servidores.	6
11	Escaneo.	5
12	Productividad.	5
	ATRIBUTOS DE USO	
13	Alertas y Reportes	6
14	Facilidad de uso	7
15	Seguridad del Producto	6
16	Proveedor	7
17	Eficacia	6
	PUNTAJE TOTAL	100

El análisis técnico y calificación de las métricas realizado a las tres (03) alternativas de software se muestra en el siguiente cuadro:

Item	Atributos	Symantec EndPoint Protection	BitDefender Security Protection	Sophos Endpoint Protection	Puntaje
ATRIBUTOS INTERNOS					
1	Sistemas Operativos Estaciones de Trabajo	5	5	4	5
2	Sistemas Operativos Servidores de Red	4	4	2	5
3	Actualizaciones de firmas	3	5	2	5
4	Protección Proactiva	5	7	3	7
5	Protección contra la Pérdida de Información	3	3	3	7
6	Control y Productividad en la red	5	7	2	7
7	Compatibilidad	5	5	2	5
8	Instalación	4	6	4	6
ATRIBUTOS EXTERNOS					
9	Consola de Administración	3	5	3	5
10	Protección y Defensa frente a malware en Estaciones y Servidores	4	6	3	6
11	Escaneo	3	5	3	5
12	Productividad	4	5	2	5
ATRIBUTOS DE USO					
13	Alertas y Reportes	5	4	3	6
14	Facilidad de uso	5	7	5	7
15	Seguridad del Producto	4	6	3	6
16	Proveedor	6	6	5	7
17	Eficacia	6	6	3	6
Total		74	92	52	100

8. ANÁLISIS COSTO BENEFICIO

COSTO

El presente documento tiene la finalidad de obtener las mejores características técnicas disponibles en el mercado para la solución que requiere PROINVERSIÓN por lo que la obtención del costo no es materia del presente. Sin embargo, de acuerdo a los procedimientos administrativos, la obtención del precio referencial será realizada previa

a la convocatoria y corresponde al área responsable realizar el análisis de costo respectivo.

BENEFICIO

La adquisición del Software para Antivirus Corporativo permitirá:

- Proteger las PC de virus informáticos, malware, troyanos, gusanos, etc, son programas maliciosos que pueden robar, borrar, modificar la información contenida en los discos duros del equipo y/o tomar el control de la PC para iniciar ataques informáticos a otros objetivos dentro o fuera de la red.
- Permite restricción en el uso de aplicaciones específicas como por ejemplo. el uso de ares, desde la consola de antivirus se puede establecer políticas que impidan que los usuarios usen este tipo de aplicaciones.
- La solución antivirus incluye la protección de PC de usuario y servidores.
- Permite restringir el uso de dispositivos de almacenamiento externo como USB para impedir que el usuario pueda inadvertidamente contagiar de virus su PC o para que no extraiga información sensible.

9. CONCLUSIONES

ÉL Área de Tecnologías de la información tiene la necesidad de contar con nuevas licencias de software antivirus, dado que la solución actual está por caducar en el corto plazo.

Técnicamente las tres (03) alternativas evaluadas cumplen con los requerimientos funcionales de la entidad.

En la evaluación técnica, la solución BitDefender Security Protection ha obtenido el mayor puntaje (un total de 92 puntos) en control y productividad en la red, protección proactiva, en protección y defesa frente a malware en estaciones y servidores.

En conclusión, por los motivos ya señalados, se recomienda adquirir el Software Antivirus de cualquiera de las marcas que obtuvieron el puntaje mayor a 70 puntos, ya sea Symantec Endpoint Protection, Sophos Endpoint Protection y BitDefender Security Protection.

La cantidad de Licencias del software de antivirus a adquirir para Proinversión es de 330 licencias entre estaciones de trabajo, servidores y equipos portátiles. Esto incluye actualización de las versiones durante ese periodo.

Por ello como mejor alternativa se sugiere el software BitDefender, por las observaciones mencionadas y por el resultado del análisis para PROINVERSIÓN.

10. FIRMAS

Rodolfo Alberto Sánchez Espinoza
Asistente en Soporte Técnico

Ruben Dario Valdez Guillen
Asistente en Soporte Técnico

Victor Hugo Chávez Gómez
Jefe de Tecnologías de la Información