



PERÚ

Ministerio
de Agricultura y Riego

AGRO RURAL

Unidad de Tecnologías
de la Información

"Año de la Lucha contra la Corrupción y la Impunidad"

Informe Técnico Previo de Evaluación de Software N°001-2019

Sustento Técnico para la Adquisición de Licencia de Software Antivirus Corporativo

1. **NOMBRE DEL ÁREA**

Unidad de Tecnologías de la Información

2. **RESPONSABLE DE LA EVALUACIÓN**

Juan Javier Arias Dominguez

3. **CARGO**

Asistente en Administración de Redes

4. **FECHA**

23 de Setiembre de 2019

5. **JUSTIFICACIÓN**

El Programa de Desarrollo Productivo Agrario Rural AGRO RURAL de acuerdo a las políticas de Seguridad de la Información, en el cual se indica que el principal activo son los datos alojados en nuestros servidores y equipos informáticos, requiere adquirir una solución de Antivirus que asegure la adecuada protección de la información y minimice los riesgos de propagación entre computadoras, mediante el empleo de programas no deseados o software malicioso.

En base a las nuevas amenazas es necesario considerar funcionalidades específicas para mitigar los riesgos con que actúan los softwares de código malicioso o malware. Por lo cual se requieren software antivirus confiable por ser una institución de ámbito nacional.

Por lo expuesto y en el marco de la ley N° 28612 "Ley que norma el uso, adquisición y adecuación del software en la Administración Pública" se procede a evaluar algunas soluciones de antivirus para uso corporativo.

6. **ALTERNATIVAS**

Tomando como referencia los últimos 3 software antivirus utilizados en la Institución en los últimos 5 años se ha realizado una evaluación real sobre las funcionalidades que estas marcas han ofrecido durante su uso.

Debido a la velocidad con que avanza la tecnología, la aparición de nuevas amenazas a la seguridad de la información tienen la misma velocidad, en tal sentido la elección de las marcas evaluadas no debe excluir otras alternativas existentes en el mercado que puedan incluir mayores funcionalidades contra estas nuevas formas de ataque.

En virtud de lo anterior, se han establecido parámetros en base a la experiencia y a las mejores prácticas utilizadas, estableciendo criterios que fortalezcan la seguridad de la información en base a métricas.





"Año de la Lucha contra la Corrupción y la Impunidad"

Se realizó la evaluación los siguientes productos:

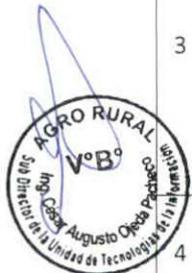
- ✓ Eset
- ✓ Kaspersky
- ✓ Sophos

7. ANALISIS COMPARATIVO TÉCNICO

De acuerdo a los criterios de evaluación requeridos por la infraestructura de la entidad, se han evaluado los productos listados en el numeral seis. A continuación el detalle de lo evaluado:

CUADRO N°1: CUADRO DE EVALUACIÓN BASADO EN MÉTRICAS

Nº	Métricas	Descripción	Puntaje Máximo	ESET	Kaspersky	SOPHOS
Métricas Internas						
1	Sistemas Operativos Soportados	Estaciones y Servidores Windows (32-64 bits): Microsoft Windows: 7/8/10 Microsoft Windows Server: 2008 / 2012 / 2016 / 2019 Estaciones y Servidores Linux (32-64 bits) Distribuciones basadas en Debian y/o RedHat	10	10	10	10
2	Protección	Debe tener instalado los siguientes componentes: Antivirus, antispyware, firewall, control web, antispam, IDS o HIPS y control de dispositivos extraíbles.	10	10	10	10
3	Antivirus	Debe tener la capacidad de analizar, estudiar y reconocer el comportamiento de los códigos maliciosos (malware). Debe tener un módulo de revisión de antivirus residente, ejecutándose en la memoria del sistema operativo y un módulo de revisión antivirus de forma manual por el usuario. Deberá contar con tecnología que evite que los códigos maliciosos desactiven componentes del sistema.	10	10	10	10
4	Administración	Diseñada para trabajar en ambiente de red, con administración centralizada.	5	5	5	5
	Consola	Debe permitir la gestión, monitoreo y administración de los equipos con el agente antivirus instalado que se encuentra en la red LAN, WAN y equipos con conexiones a internet. Debe permitir recibir y generar reportes de los equipos que cuenten con el agente de antivirus instalado. Tener la capacidad de cambiar la configuración de múltiples clientes a la vez sin la intervención del usuario final. La consola deberá realizar búsquedas de estaciones de trabajo y/o servidores.	10	10	10	10





Métricas Externas						
1	Eficacia	Debe tener la capacidad de reconocer el malware que no se encuentre en su base de datos, mediante el uso de un sistema de heurística avanzada.	10	10	10	10
2	Actualización de firmas	Las actualizaciones de firmas y componentes del antivirus deberán ejecutarse de manera centralizada, desatendida e incremental.	5	5	5	5
3	Control de dispositivos	El software de antivirus deberá permitir el acceso de solo lectura, lectura/escritura o bloquear dispositivos, como: USB, CD-ROM y módems de Internet.	10	10	10	10
5	Alertas	Deberá de generar alertas ante un evento específico mediante el envío de mensajes de correo o notificaciones vía SNMP.	5	5	5	5
Métricas de Uso						
1	Facilidad de uso e instalación	El uso de interface del producto debe ser fácil, amigable e intuitiva.	5	4	5	4
2	Implementación	Instalación, Despliegue, Impacto.	5	5	4	4
3	Manejo de consola administrativa	La interface de consola debe ser amigable e intuitiva.	5	4	4	5
4	Generación y Personalización de Reportes	Se podrán generar una amplia variedad de reportes predefinidos o personalizados y presentar alertas en las PCs y consola. Los reportes podrán ser obtenidos de forma automática o a intervalos de tiempo predefinidos.	5	5	4	5
	Soporte Local	Cuenta con un representante local, que brindará el soporte respectivo cuando se requiera.	5	5	5	5
TOTAL			100	98	97	98

8. ANÁLISIS COMPARATIVO COSTO-BENEFICIO

Para este análisis se ha considerado los costos para un total de 600 licencias para estaciones de trabajo y servidores de datos.

A continuación se detalla los costos obtenidos de las consultas realizadas. Los montos son referenciales.

CUADRO N° 2.- COSTOS REFERENCIALES DE LICENCIAS POR 1 AÑO

Software	Costo Total
ESET	32,922.00
KASPERSKY	35,923.00
SOPHOS	34,652.00





9. CONCLUSIONES

- ✓ Los software Antivirus de ESET y Sophos según el Cuadro N° 1 de la evaluación basada en métricas, obtienen el mayor puntaje basado el primero en el bajo impacto al momento de la implementación debido a ser el software utilizado actualmente en la institución y el segundo debido a la mejor experiencia en el manejo de su consola de administración.
- ✓ En el análisis comparativo de costos Cuadro N° 2 el software de ESET tiene el menor costo, los mismos que son solo referenciales, sin perjuicio de otras alternativas que se puedan encontrar en el estudio mercado.
- ✓ De acuerdo al análisis y evaluación realizados, se puede observar que las soluciones antivirus evaluadas han alcanzado puntuaciones óptimas para su consideración, por encima de 95 sobre 100.
- ✓ En tal sentido, las tres soluciones cumplen con los requerimientos mínimos a nivel de protección correspondiente al software antivirus corporativo que necesita la Institución, sin perjuicio de otras alternativas que se puedan encontrar en el estudio de mercado.

10. FIRMAS

PROGRAMA DE DESARROLLO PRODUCTIVO
AGRARIO RURAL - AGRO RURAL

.....
Ing. Cesar Augusto Ojeda Pacheco
Sub Director de la Unidad de Tecnologías
de la Información

Ing. Cesar Augusto Ojeda Pacheco

Sub Director - Unidad de Tecnologías de la Información

Juan Javier Arias Dominguez

Asistente en Administración de Redes

