INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE

REPÚBLICA DEL PERÚ
SECTOR ENERGÍA Y MINAS
INGEMMET
INSTITUTO GEOLÓGICO MINERO Y METALÚRGICO

1. **NOMBRE DEL ÁREA:**
   Oficina de Sistemas de Información.

2. **RESPONSABLE(S) DE LA EVALUACIÓN**
   Ing. Juan Torres Sosa.

3. **CARGO(S)**
   Responsable de la evaluación Software de protección antivirus

4. **FECHA**
   Lima, 18 de Enero del 2018

Instituto Geológico Minero y Metalúrgico – Oficina de Sistemas de Información – INGEMMET

5. **JUSTIFICACIÓN:**
   Con la adquisición del Software de protección antivirus, se permitirá brindar protección contra virus, malware, spyware, adware y otras amenazas dentro de las estaciones de trabajo y servidores; así como también controlar el riesgo de que se afecte la integridad de la información y el normal desarrollo de las actividades de la institución.

   Se ha procedido a evaluar según lo establecido en la Ley Nº 28612, ley que norma el uso, adquisición y adecuación del software en la administración pública, las características más importantes establecidas para el Software de de protección antivirus.

Oficina de Sistemas de Información – Ing. Juan Torres Sosa – INGEMMET

6. **ALTERNATIVAS**
   Se ha evaluado los siguientes Software:
   - SOPHOS ENDPOINT SECURITY
   - KASPERSKY ENDPOINT SECURITY

7. **ANÁLISIS COMPARATIVO TÉCNICO**
   Se realizó aplicando la parte 3 de la Guía de Evaluación de Software.

   7.1 Propósito de la Evaluación:
   Determinar las características de calidad mínimas para el producto final, Software de protección antivirus requerido por el INGEMMET.

   7.2 Identificar el tipo de producto.
   Software de protección antivirus requerido por el INGEMMET.

   7.3 Especificación del Modelo de Calidad.
   Se ha aplicado el Modelo de calidad de Software descrito en la Parte 1 de la Guía de Evaluación de Software aprobado por Resolución Ministerial Nº 139-2004-PCM.

   7.4 Selección de Métricas.
   Las métricas han sido seleccionadas en base al análisis de información de requerimiento de Calidad para el software solicitado, los requerimientos de calidad en los niveles técnicos y operativos, y requerimientos de calidad que demanda nuestra arquitectura de Red.

7.5 Selección de requisitos de Calidad.

Hemos determinado los siguientes requisitos de calidad que debe de cumplir el Software que permite la protección de antivirus requerido por el INGEMMET.

Cuadro 7.1

Requisitos de Calidad para el Software de protección antivirus

Para el INGEMMET

ITEM	CALIDAD
	REQUERIMIENTOS DE CALIDAD INTERNA
1	Debe trabajar en Sistemas Operativos Windows 7, Windows 8 o superior de (32 o 64 bits).
2	Debe trabajar en Sistemas Operativos Linux (32 o 64 bits).
3	Debe trabajar con plataforma de virtualización VMWare y Xen.
4	Que permita protección contra virus, programas troyanos, gusanos, programas espía y publicitarios (anti-spyware, HIPS (Host Intrusión Prevention)).
5	Que permita el análisis de ficheros en modo automático o según horario
6	Que permita análisis de virus de Internet a través de cualquier navegador
7	Que permita análisis del correo electrónico mínimo para protocolos: POP3, IMAP, NNTP y SMTP.
8	Que permita análisis y control de archivos adjuntos por extensión en correo electrónico.
9	Que permita análisis de tráfico de Internet mínimo para los protocolos: HTTP y FTP.
10	Que realice análisis y desinfección automática el contenido de los dispositivos de memoria
11	Que realice el Chequeo y desinfección de malware contenido en archivos comprimidos.
12	Que permita detección y desinfección en tiempo real de virus residentes.
13	Que permita enviar a cuarentena archivos infectados.
14	Que permita el Chequeo y desinfección de malware contenido en memoria o en el sector de arranque.
	REQUERIMIENTOS DE CALIDAD EXTERNA
15	Permitir, bloquear a usuarios seleccionados y / o grupos de usuarios iniciar aplicaciones.
16	Control de acceso web mediante filtro por categoría y tipos de archivos.
17	Permitir configurar las reglas de control de acceso web para: permitir, bloquear o alertar el acceso a los diferentes sitios.
18	Brindar la posibilidad de monitorear y controlar las aplicaciones, permitir y denegar el acceso a determinadas llaves del registro, archivos y carpetas.
19	Que permita definir que aplicaciones están permitidas para ejecutarse, cuales aplicaciones pueden hacer llamados a Dynamic Link Libraries (DLL).
20	Brindar visibilidad de las aplicaciones que el usuario ha instalado en los equipos.
21	Que permita aplicar políticas de control por grupos de usuarios, para permitir o bloquear aplicaciones.
22	Que permita crear listas blancas y listas negras para especificar qué aplicaciones se pueden ejecutar.
23	Realizar instalación remota y flexible de software con despliegues programados o manuales
	REQUERIMIENTOS DE CALIDAD DE USO
24	Que permita Integración con directorio activo.
25	Que permita la protección de trafico de correo electrónico contra malware y spam centralizadamente
26	Que permita de Manejo de grupos jerárquicos de usuarios.
27	Que permita administrar servidores y clientes Linux y clientes Mac a través de la consola de administración.
28	Permitir detener o activar escaneo de virus PCs individuales, desde la consola.
29	Que permita poner en cuarentena a los endpoints al detectar un brote de virus en la red.
30	Que permita manejar múltiples políticas de seguridad, pudiendo activar una política específica, desde La consola de administración.
31	Que tenga la Capacidad de visualizar de manera consolidada los dispositivos gestionados, sus características técnicas, como sistema operativo, Nombre de dispositivo y dirección IP, Tipo de infección.
32	Que permita Monitoreo permanente y generación reportes de eventos en tiempo real
33	Que permita accesar a la consola desde cualquier sitio en la red
34	Que permita distribución de agentes, configuraciones y actualizaciones de forma centralizada
35	Que permita desinstalar el agente de manera segura y remota.

Selección de atributos de Calidad.

Los atributos de calidad que se utilizarán para la evaluación del Software de protección antivirus requerido por el INGEMMET, de acuerdo a lo especificado en la parte 2 de la Guía de Evaluación de Software se muestran en el siguiente cuadro:

Cuadro 7.2

Atributos de calidad tomados en cuenta en la Evaluación	
ATRIBUTOS INTERNOS	Características del Software que determinan su habilidad para satisfacer las necesidades propias e implícitas.
ATRIBUTOS EXTERNOS	Características del Software que determinan su habilidad para satisfacer las necesidades explicitas e implícitas
ATRIBUTOS EN USO	Características del Software que determinan los requerimientos de los usuarios finales de manera que satisfagan sus necesidades

Asignación de puntajes a los atributos de Calidad.

Los puntajes establecidos a los atributos de calidad seleccionados de acuerdo a nuestras necesidades se muestran en el siguiente cuadro:

Cuadro 7.3

Métricas adoptadas de acuerdo a la Necesidad	
Tipo de Atributo	Puntaje
ATRIBUTOS INTERNOS	40
ATRIBUTOS EXTERNOS	27
ATRIBUTOS EN USO	33
TOTAL	100

Nota: La escala de evaluación que se ha tomado es de 1 a 100

Evaluación de los criterios de calidad para las alternativas de Software de protección antivirus requerido por el INGEMMET tomados como referencia.

Cuadro 7.4
Evaluación de criterios de Calidad

ITEM	CALIDAD	CALIFICACION		
	REQUERIMIENTOS DE CALIDAD INTERNA	Puntaje Max.	Sophos Endpoint Security	Kaspersky Endpoint Security
1	Debe trabajar en Sistemas Operativos Windows 7, Windows 8 o superior de (32 o 64 bits).	4	4	4
2	Debe trabajar en Sistemas Operativos Linux (32 o 64 bits).	3	3	3
3	Debe trabajar con plataforma de virtualización VMWare y Xen.	3	3	3
4	Que permita protección contra virus, programas troyanos, gusanos, programas espía y publicitarios (anti-spyware, HIPS (Host Intrusión Prevention)).	3	3	3

ITEM	CALIDAD	CALIFICACION		
5	Que permita el análisis de ficheros en modo automático o según horario	2	2	2
6	Que permita análisis de virus de Internet a través de cualquier navegador	3	3	3
7	Que permita análisis del correo electrónico mínimo para protocolos: POP3, IMAP, NNTP y SMTP.	3	3	3
8	Que permita análisis y control de archivos adjuntos por extensión en correo electrónico.	2	2	2
9	Que permita análisis de tráfico de Internet mínimo para los protocolos: HTTP y FTP.	3	2	3
10	Que realice análisis y desinfección automática el contenido de los dispositivos de memoria	3	3	3
11	Que realice el Chequeo y desinfección de malware contenido en archivos comprimidos.	3	3	3
12	Que permita detección y desinfección en tiempo real de virus residentes.	3	3	3
13	Que permita enviar a cuarentena archivos infectados.	2	2	2
14	Que permita el Chequeo y desinfección de malware contenido en memoria o en el sector de arranque.	3	3	3
	REQUERIMIENTOS DE CALIDAD EXTERNA			
15	Permitir, bloquear a usuarios seleccionados y / o grupos de usuarios iniciar aplicaciones.	3	3	3
16	Control de acceso web mediante filtro por categoría y tipos de archivos.	3	3	3
17	Permitir configurar las reglas de control de acceso web para: permitir, bloquear o alertar el acceso a los diferentes sitios.	3	3	3
18	Brindar la posibilidad de monitorear y controlar las aplicaciones, permitir y denegar el acceso a determinadas llaves del registro, archivos y carpetas.	3	3	3
19	Que permita definir que aplicaciones están permitidas para ejecutarse, cuales aplicaciones pueden hacer llamados a Dynamic Link Libraries (DLL).	4	2	4
20	Que permita visualizar las aplicaciones que el usuario ha instalado en los equipos.	2	1	2
21	Que permita aplicar políticas de control por grupos de usuarios, para permitir o bloquear aplicaciones.	3	3	3
22	Que permita crear listas blancas y listas negras para especificar qué aplicaciones se pueden ejecutar.	3	3	3
23	Realizar instalación remota y flexible de software con despliegues programados o manuales.	3	3	3
	REQUERIMIENTOS DE CALIDAD DE USO			
24	Que permita Integración con directorio activo.	3	3	3
25	Que permita la protección de trafico de correo electrónico contra malware y spam centralizadamente	3	1	3
26	Que permita de Manejo de grupos jerárquicos de usuarios.	3	3	3
27	Que permita administrar servidores y clientes Linux y clientes Mac a través de la consola de administración.	3	1	3
28	Permitir detener o activar escaneo de virus PCs individuales, desde la consola.	2	2	2
29	Que permita poner en cuarentena a los endpoints al detectar un brote de virus en la red.	2	2	2
30	Que permita manejar múltiples políticas de seguridad, pudiendo activar una política específica, desde La consola de administración.	3	3	3
31	Que tenga la Capacidad de visualizar de manera consolidada los dispositivos gestionados, sus características técnicas, como sistema operativo, Nombre de dispositivo y dirección IP, Tipo de infección.	2	2	2
32	Que permita Monitoreo permanente y generación reportes de eventos en tiempo real	3	3	3

Oficina de Sistemas de Información INGEMMET

Oficina de Sistemas de Información
Ing. Juan Torres Sosa
INGEMMET

ITEM	CALIDAD	CALIFICACION		
33	Que permita accesar a la consola desde cualquier sitio en la red	3	2	3
34	Que permita distribución de agentes, configuraciones y actualizaciones de forma centralizada	3	3	3
35	Que permita desinstalar el agente de manera segura y remota.	3	1	3
	Totales	**100**	**89**	**100**

Nota: La escala de evaluación que se ha tomado es de 1 a 10

8. ANÁLISIS COMPARATIVO COSTO – BENEFICIO

Para la elaboración del análisis de costo beneficio se han tomado en cuenta los criterios solicitados en el punto 8 del reglamento de la Ley Nº 28612, los cuales son:

Criterios mínimos:

- Licenciamiento
- Hardware necesario para su funcionamiento
- Soporte y mantenimiento externo
- Personal y mantenimiento interno
- Capacitación

Criterios adicionales:

- Impacto en el cambio de plataforma.
- Garantías Comerciales Aplicables.

Estos criterios se expresan en el siguiente cuadro:

Cuadro 8.1

ITEM	Criterios a Evaluar	Sophos Endpoint Security	Kaspersky Endpoint Security
1	Licenciamiento	Requiere	Requiere
2	Cantidad de Licencias referenciales	1	1
3	Costo referencial en Nuevos Soles, por la cantidad de Licencias requeridas	S/. 53,898.00	30,550.00
4	Hardware Necesario para su Funcionamiento	Intel / AMD, 1 Ghz, 1 GB de. RAM, 2 GB de espacio libre en Disco Duro, Adaptador de video SVGA	Intel / AMD, 1 Ghz, 1 GB de. RAM, 2 GB de espacio libre en Disco Duro, Adaptador de video SVGA
5	Soporte y Mantenimiento Externo	Requiere	Requiere
6	Personal y mantenimiento Interno	Requiere	Requiere
7	Capacitación para el Uso del Software de Protección Antivirus	No se requiere capacitación	Requerido para el personal encargado
8	Costo referencial, en Nuevos Soles, por Capacitación para la cantidad de personal que se especifica.	S/. 0.00	S/. 0.00
9	Garantía Comercial	El proveedor proporciona Garantía Comercial	El proveedor proporciona Garantía Comercial
10	Impacto en el cambio de la Plataforma	No habría impacto porque hay experiencia en el uso del software.	No habría impacto, porque la herramienta brinda beneficios respecto al consumo de recursos en servidores

8.1 Asignación de puntajes para los criterios a evaluar

Para poder medir los criterios indicados en el Cuadro 8.1 se ha elaborado una escala de puntajes y pesos para cada criterio, las cuales se indican en el siguiente cuadro:

Cuadro 8.2

Escala de puntajes y pesos

ITEM	PARAMETRO (Referido al Elemento a evaluar)	PUNTAJE	PESO
1	REQUIERE	0	1
	NO REQUIERE	10	
2	MAYOR CANTIDAD DE LICENCIAS	0	1
	IGUAL CANTIDAD DE LICENCIAS	5	
	MENOR CANTIDAD DE LICENCIAS	10	
3	MENOR COSTO	10	1
	MAYOR COSTO	0	
4	MENOS HARDWARE	10	1
	IGUAL HARDWARE	5	
	MAYOR HARDWARE	0	
5	REQUIERE	0	1
	NO REQUIERE	10	
6	REQUIERE	0	1
	NO REQUIERE	10	
7	PARA TODO EL PERSONAL	0	1
	SOLO PARA PERSONAL TECNICO	10	
8	MENOR COSTO	10	3
	MAYOR COSTO	0	
9	SE PROPORCIONA GARANTIA	10	3
	NO SE PROPORCIONA GARANTIA	0	
10	ALTO IMPACTO	0	10
	MEDIANO IMPACTO	5	
	NO HAY IMPACTO	10	

Nota 1: Los Ítem del cuadro 8.2 son los mismos a los del cuadro 8.1

Nota 2: La escala de evaluación que se ha tomado es de:

- **de 1 a 10 para los puntajes**
- **de 1 a 10 para los pesos**

8.2 Resultados de la Evaluación

El cuadro que a continuación se muestra es el resultado de la evaluación de costo beneficio del Software de protección antivirus.

Cuadro 8.3

RESULTADOS DE EVALUACIÓN DE COSTO BENEFICIO

ITEM	Criterios a Evaluar	Sophos Endpoint Security	Kaspersky Endpoint Security
1	Licenciamiento	10	10
2	Cantidad de Licencias	5	5
3	Costo referencial en Nuevos Soles, por la cantidad de licencias requeridas	0	10
4	Hardware Necesario para su Funcionamiento	5	5
5	Soporte y Mantenimiento Externo	10	10
6	Personal y mantenimiento Interno	0	0
7	Capacitación para el Uso del Software	0	10
8	Costo referencial, en Nuevos Soles, por Capacitación para la cantidad de personal que se especifica.	0	0
9	Garantía Comercial	30	30
10	Impacto en el cambio de la Plataforma	100	100
	Puntaje Total	**160**	**180**

Nota1: Los Ítem del cuadro 8.3 son los mismos a los del cuadro 8.1 y cuadro 8.2

Nota2: Los valores resultados en el cuadro 8.3 están referidos al cálculo PUNTAJE x PESO del cuadro 8.2

9. CONCLUSIONES

De acuerdo con la evaluación de los criterios de calidad requeridos para el INGEMMET, los cuales se indican en el Cuadro 7.4; para el **Software de protección antivirus**, el que cumple con un mayor número de criterios de calidad es el software **Kaspersky Endpoint Security.**

De acuerdo con la evaluación de los criterios tomados en cuenta para el análisis de costo beneficio, los cuales se indican en el Cuadro 8.3; se debe optar por el Software de **protección antivirus** y que brinda mayores beneficios para el INGEMMET, este es el software **Kaspersky Endpoint Security** por obtener el mayor puntaje en la evaluación de costo beneficio.

10. FIRMAS

Responsable	Firma
Ing. Juan Torres Sosa **Responsable de la evaluación**	

Responsable de la Aprobación	Firma
Miriam Araya Carrasco. **Directora (e) de la Oficina de Sistemas de Información.**	MIRIAM ARAYA CARRASCO DIRECTORA (e) Oficina de Sistemas de Información INGEMMET