



“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”

“Año del Fortalecimiento de la Soberanía Nacional”

## INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE

Nº 001

### “Licencias de software para una solución antimalware, detección y respuesta de amenazas (EDR) y gestor de parches para el Ministerio de la Producción”

#### 1. NOMBRE DEL ÁREA

Dirección General de Tecnologías de la Información - OGTI

#### 2. RESPONSABLES DE LA EVALUACIÓN

Tobias Paul García Campos

Julio César Mamani Amanca

#### 3. CARGO

Especialista en Seguridad de la Información

Coordinadora de Gobierno Digital y Seguridad de la Información

#### 4. FECHA

Enero 2022

#### 5. JUSTIFICACION:

El Ministerio de la Producción requiere contar con una solución que permite garantizar la seguridad de los equipos informáticos; de tal modo que pueda detectar, analizar y eliminar todo tipo de amenazas ya sea de virus, spyware, botnet, malware y variantes de los mismos, brindando protección ante todo tipo de amenazas tanto conocidas como desconocidas.

Debido a los nuevos tipos de amenazas que aparecen a nivel mundial, los cuales intentan burlar el mayor número de controles de seguridad, es necesario considerar funcionalidades específicas que permitan mitigar los riesgos de infección o robo de información que ocasionan en dichos equipos diferentes tipos de archivos con contenido malicioso. Por ello es necesario contar una solución de antimalware robusta para los servidores, por ser una institución de impacto nacional.

#### 6. ALTERNATIVAS:

Actualmente en el mercado existen diferentes soluciones de software correspondientes a antimalware para equipos informáticos de la entidad, en merito a ello se toman en cuenta aquellas que sean compatibles e instalables en la plataforma tecnológica de usuario final.

Tomando en consideración las necesidades y requerimientos del Ministerio de la Producción, tomando en cuenta los nuevos esquemas relacionados con protección ante amenazas no solo conocidas, sino también desconocidas, se ha buscado alternativas de software antimalware en el mercado local que cumplan dichas necesidades y cuenten con soporte técnico local.

Debido e ello, la herramienta de software que sea seleccionada debe contener como mínimo las funcionalidades que permitan el mejor esquema de protección tanto para la seguridad informática como para la seguridad de la información que se maneja en los servidores del Ministerio de la Producción. Teniendo en cuenta la criticidad de la información a ser protegida, a continuación, se detallarán las características y atributos técnicos necesarios para la evaluación del software requerido para la institución, con la aplicación de las respectivas métricas.

Por ello, se ha establecido parámetros mínimos que permitan fortalecer la seguridad en las TI



“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”  
“Año del Fortalecimiento de la Soberanía Nacional”

obteniendo disponibilidad, integridad y confidencialidad, como factores que conllevan a una mejor evaluación. Estos requerimientos se encuentran detallados en el Anexo 01.

En base a las premisas indicadas y a la información obtenida de los productos que hay en el mercado, así como de las cotizaciones referenciales proporcionadas por los proveedores con la finalidad de realizar el análisis de costo beneficio, se está evaluando las siguientes marcas que son de tipo propietario:

- KASPERSKY
- WATCHGUARD
- F-SECURE

## **7. ANALISIS COMPARATIVO TÉCNICO:**

El análisis técnico ha sido realizado según los lineamientos establecidos en la "Guía técnica sobre evaluación de software para la administración pública" aprobado por R.M. N° 139-2004-PCM tal como exige el reglamento de la ley N° 28612 -"Ley que norma el uso, adquisición y adecuación del software en la administración pública":

### **7.1 Propósito de la Evaluación:**

Validar que las alternativas seleccionadas sean las más convenientes para el Ministerio de la Producción.

### **7.2 Identificar el tipo de producto**

Software antimalware para equipos informáticos.

### **7.3 Especificación del Modelo de Calidad.**

La evaluación del software antimalware se ha realizado bajo los parámetros establecidos en la RM 139-2004-PCM

"Guía Técnica sobre Evaluación de Software en la Administración Pública".

### **7.4 Selección de métricas**

Las métricas fueron identificadas de acuerdo con los criterios establecidos en base a las necesidades técnicas del Ministerio de la Producción.

Según lo establecido en la guía de evaluación y las necesidades institucionales, se definieron las siguientes métricas, así como el puntaje máximo, tal como se muestra a continuación:

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”  
“Año del Fortalecimiento de la Soberanía Nacional”

N°	Atributos	Puntaje Máximo
<b>Atributos Internos y Externos</b>		
1	Funcionalidad	63
2	Eficiencia	10
3	Capacidad de Mantenimiento	2
4	Portabilidad	7
<b>Atributos de Uso</b>		
1	Eficacia	12
2	Productividad	2
3	Seguridad	4
<b>TOTAL</b>		<b>100</b>

El detalle de cada característica que forma parte de los atributos indicados, así como el resultado de la evaluación de los productos en base a las características solicitadas se muestra en el **Anexo 01**.

## 8. ANALISIS COMPARATIVO DE COSTO – BENEFICIO:

### 8.1 Licenciamiento

Se debe incluir licencias con mantenimiento de software (cambios de versión, actualización) por el tiempo del contrato.

El producto ofrecido debe corresponder a las últimas versiones

El licenciamiento debe ser perpetuo.

### 8.2 Software

Los sistemas operativos instalados en los computadores de trabajo desplegadas (Ms Windows, Linux, Android, IOS), cumplen con los requisitos exigidos por los productos de software evaluados.

### 8.3 Hardware necesario para su funcionamiento

El conjunto de equipos (FlexSystem x240 IBM, IBM Storwize V7000) que componen el data center del Ministerio de la Producción, cumplen con los requisitos necesarios para la instalación de los productos de software evaluados.

### 8.4 Soporte y mantenimiento externo

El fabricante de los productos ofertados debe poseer Oficina de representación en Perú, así como personal de soporte técnico que garantice la adecuada y oportuna prestación de la garantía y de servicios. Este servicio debe ser 24x7.

El proveedor deberá prestar su asesoría presencial en la instalación y configuración del software.

### 8.5 Costo

El presente análisis tiene por objetivo seleccionar la mejor alternativa, en ese sentido, se ha decidido dar una valoración de 0.7 a la evaluación técnica y de 0.3 a la evaluación económica, con el fin de garantizar que la solución antimalware, EDR y gestor de parches,



“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”  
“Año del Fortalecimiento de la Soberanía Nacional”

cumpla con los requerimientos técnicos solicitados.

La evaluación estas alternativas incluyen los costos de licencias por suscripción anual y soporte y actualizaciones de la versión de los productos.

En el **Anexo N° 02**, se muestran los resultados del Análisis Comparativo de Costo – Beneficio, así como el cuadro de valoración técnica – económica.

En el **Anexo N° 03**, se muestra Costos Referenciales de la solución.

## 9. CONCLUSIONES

En base al análisis realizado, se evidencia el nivel de cumplimiento de los tres productos evaluados sobre los requerimientos solicitados que corresponde a una solución de software antimalware, detección y respuesta de amenazas (EDR) y gestor de parches para el Ministerio de la Producción, con la capacidad de brindar la protección tanto para amenazas conocidas como desconocidas y con el fin de cumplir con las normativas de seguridad existentes en la entidad.

## 10. FIRMA

-----  
**Tobias Paul García Campos**  
Especialista en Seguridad  
de la Información

-----  
**Julio César Mamani Amanca**  
Coordinador de Gobierno Digital  
y Seguridad de la Información



“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”  
“Año del Fortalecimiento de la Soberanía Nacional”

**ANEXO 01**

## CARACTERISTICAS TÉCNICAS DEL SOFTWARE ANTIMALWARE PARA EQUIPOS INFORMÁTICOS

N°	Atributos	Descripción	Puntaje Máximo	KASPERSKY	WATCH GUARD	F-SECURE
<b>Atributos Internos y Externos</b>						
1	Funcionalidad	Análisis de comportamiento e inteligencia artificial, entrenada por los expertos en seguridad cibernética de la marca, detectando todas las amenazas conocidas y desconocidas. El aprendizaje automático debe mejorar las detecciones al reconocer nuevas tácticas, técnicas y procedimientos emergentes con lanzamientos de procesos asociados, conexiones de red y tipos de aplicaciones.	2	2	2	2
		Proteger contra virus, troyanos, macrovirus, adware, spyware, gusanos, rootkits y todo tipo de programa malicioso (malware) incluyendo la protección contra ransomware.	1	1	1	1
		Sistema de detección de intrusos que realice un análisis de contenido del tráfico de red y además permita proteger de ataques haciendo que cualquier tráfico dañino sea bloqueado.	1	1	1	1
		Permitir realizar un escaneo del equipo en modo seguro bajo línea de comando donde se podrá especificar las opciones para la limpieza de virus y/o mediante un CD, DVD o dispositivo USB booteable para analizar el equipo sin ejecutar el sistema operativo.	1	1	1	1
		Opción que permita evitar escanear archivos grandes (x tamaño) que puedan consumir el performance de la máquina (opcionalmente).	1	1	1	1
		En sistemas operativos Windows deberá contar con una herramienta integrada que permita inspeccionar completamente componentes del sistema (Controladores, Aplicaciones Instaladas, Conexiones de Red y entradas importantes del Registro de Windows), esto con la finalidad de determinar la causa de comportamientos sospechosos en el sistema que puede deberse a incompatibilidad de software, hardware o código malicioso.	1	1	1	1
		Escanear la red por Directorio Activo, Red IP o Dominios, o una tecnología propia de detección de equipos; en busca de nuevos equipos agregados a la red permitiendo identificar equipos con o sin agente endpoint, para posteriormente enviar la tarea de instalación remota o la ejecución de configuraciones de políticas.	1	1	1	1
		Contar con un módulo de detección en tiempo real que proteja contra códigos maliciosos en cada ejecución, uso o creación de archivos en el equipo.	1	1	1	1
		El cliente endpoint debe tener un agente que le permita ser administrado desde una consola centralizada. Este agente debe reportar el estado de todas las soluciones instaladas en la dependencia.	1	1	1	1
		Catalogar a los procesos de los equipos de acuerdo con la reputación basada en la nube. Esta permitirá recopilar información anónima del ordenador afectada con las amenazas detectadas recientemente.	1	1	1	1
		Generar dentro de la misma solución antimalware repositorios de actualización, los cuales deberán ser distribuidas mediante protocolo http, https o protocolos de transferencia de datos	2	2	2	2



“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”  
“Año del Fortalecimiento de la Soberanía Nacional”

	seguros localmente, sin depender de aplicaciones externas o de tareas desde la consola de Administración.				
	El cliente endpoint debe tener un agente que le permita ser administrado desde una consola centralizada. Este agente debe reportar el estado de todas las soluciones instaladas en la dependencia.	2	2	2	2
	Módulo de control de dispositivos de almacenamiento interno que permita definir reglas y/o políticas granulares, por usuarios de dominio o identificador de seguridad de usuario (SID) y hostname, para permitir acceso de solo lectura, lectura/ escritura y bloqueo total de acuerdo a las necesidades de PRODUCE, que incluye como mínimo los siguientes dispositivos: memorias USB, lectora CD/DVD, dispositivos de imágenes (cámaras digitales), dispositivos portátiles (celulares y tabletas), bluetooth, módems, smart card, memoria SD entre otros. Estas políticas deben poder ser aplicadas por usuarios y por equipos (hostnames) clasificados. El postor debe incluir en su oferta, información oficial de la solución a implementar donde indique la gestión de todos los dispositivos de almacenamiento externo mencionados, aplicando reglas y/o políticas. La funcionalidad de bloqueo de dispositivos externos es opcional para equipos con sistema operativo Linux y Mac	2	2	2	2
	Módulo específico contra ransomware que realice el bloqueo de amenazas de día cero y ataques de ransomware como Locky, WannCry, Petya, etc. sin requerir la actualización de firmas. El postor debe incluir en su oferta información oficial de la solución a implementar en idioma inglés o español, donde se indique la protección contra ataques de ransomware.	2	2	2	2
	Contar para servidores Windows con exclusiones automáticas o manuales (configurables a través de la consola de administración). que permitan detectar los procesos críticos del servidor y los archivos críticos del sistema operativo y los agregue automáticamente a la sección de exclusiones	2	2	2	2
	Consola de gestión 100% web y de acceso seguro vía HTTPS y con doble factor de autenticación(opcional) donde se deberá gestionar entre otras cosas: <ul style="list-style-type: none"> <li>➤ El análisis de causa raíz de la detección.</li> <li>➤ El listado de equipos, así como el inventario de aplicaciones utilizadas en cada uno de los endpoints.</li> <li>➤ El análisis detallado de la detección con el listado de direcciones de archivos, procesos, URLs, eventos y demás acciones que ha realizado la detección.</li> <li>➤ Integración con motores de análisis de malware en tiempo real para la verificación automática de firmas de archivos en dicha plataforma.</li> <li>➤ Permitir correlacionar los eventos detectados.</li> <li>➤ Listar todas las detecciones similares presentes en otros endpoints con el fin de tomar acciones de corrección.</li> <li>➤ Permitir realizar el aislamiento de los equipos afectados.</li> <li>➤ Permitir filtrar las amenazas de acuerdo con el grado de riesgo, éstos deben ser configurables por lo menos en (03) niveles.</li> </ul>	2	2	2	2
	Como mínimo 3 consolas de administración: una de ellas destinada a la gestión de antimalware y EDR para la administración de las estaciones de trabajo, laptops, tablets y	2	2	2	2



“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”  
“Año del Fortalecimiento de la Soberanía Nacional”

	móviles; otra destina a la gestión de antimalware y EDR para la administración de servidores de TI y una tercera para la administración del gestor de parches. Todas deben permitir la delegación de tareas mediante la creación de usuarios con distintos perfiles de administración.				
	El servidor de administración remota debe estar en idioma español o inglés y deberá ser compatible al menos con los siguientes sistemas operativos:  ➤ Windows Server 2008 x64 R2 SP1, Windows Server 2008 x64 R2 Core, Windows Server 2012 x64, Windows Server x63 Core, Microsoft SBS 2011 x64 Standard, Microsoft SBS 2011 x64 Esencial. ➤ Opcionalmente Ubuntu 12.04 LTS x86 Server, Ubuntu 12.04 LTS x64 Server, RHEL Server 6 x86 y x64, RHEL 7 x86 y x64, CentOS 5, 6 y 7 en x86 y x64, OpenSUSE 13 x86 y x64, Debian 7 x86 y x64, o superiores	1	1	1	1
	El servidor deberá soportar al menos una de las siguientes bases de datos: Microsoft SQL Server, MySQL, MariaDB, Oracle, PostgreSQL, MongoDB.	1	1	1	1
	Mostrar los equipos detectados en la red.	1	1	1	1
	Permitir la configuración, instalación, desinstalación y administración remota de la solución en las estaciones de trabajo, dispositivos móviles y servidores de TI. De no contar el módulo de despliegue remoto, la instalación será de entera responsabilidad del proveedor	1	1	1	1
	Proporcionar un almacenamiento que permita registrar al menos seis (06) meses de registro de eventos de la consola (logs).	1	1	1	1
	Contar con protección especializada contra ataques de RANSOMWARE y exploits de tipo Día Zero.	1	1	1	1
	Permitir definir exclusiones por tipo de archivos y/o rutas para que no sean analizadas por el antimalware	1	1	1	1
	Analizar archivos comprimidos en al menos los siguientes formatos: .zip, .rar y .tar.	1	1	1	1
	Generación de reportes avanzados en modo gráfico, exportables en formato csv o html que permitan identificar:  - Intentos de infección más repetidos y recientes en la red. - Host con mayor número de infección. - Dispositivos de almacenamiento externos bloqueados por usuario. - Cantidad de estaciones/servidores con o sin endpoint. - Última conexión de los hosts a la consola. - Última actualización de los hosts y la versión del agente instalado.	1	1	1	1
	Esta característica puede ser propia o de terceros y deberá gestionar la detección de vulnerabilidades y parches de software multi-fabricante para estaciones de trabajo y servidores permitiendo:  ➤ Gestionar administrar y analizar las vulnerabilidades del sistema operativo MS Windows, productos Microsoft y de otros fabricantes mediante la aplicación de parches en base a las vulnerabilidades detectadas en los equipos. ➤ Reportar las actualizaciones faltantes del sistema operativo y aplicaciones de terceros en los equipos de la red.	8	7	7	7



“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”  
“Año del Fortalecimiento de la Soberanía Nacional”

	<ul style="list-style-type: none"> <li>➤ Comparar periódicamente el software instalado en el antimalware e identificar las actualizaciones faltantes y las vulnerabilidades encontradas.</li> <li>➤ Descargar a la Consola Central los paquetes y/o programas necesarios para corregir las vulnerabilidades y parches encontrados con el fin de optimizar el uso de ancho de banda en la red.</li> <li>➤ Contar con una opción para visualizar las vulnerabilidades y actualizaciones pendientes encontradas en la red y que antimalware se encuentran afectadas por cada una de ellas.</li> <li>➤ Permitir enviar mediante una política la actualización centralizada de programas y vulnerabilidades en programas de Microsoft y Sistemas Operativos, Java, Mozilla, Google, Adobe, Services Pack, Winzip y otras aplicaciones usadas en entornos corporativos.</li> <li>➤ Permitir la instalación automática y centralizada de actualizaciones, parches y/o correcciones de vulnerabilidades en el sistema operativo y aplicaciones existentes en el antimalware de acuerdo con las políticas definidas por el administrador de la consola.</li> <li>➤ Permitir programar la instalación de actualizaciones según su importancia (Crítico, Crítico y Vulnerable y Todas) en forma centralizada.</li> <li>➤ Permitir programar la instalación automática basado en un día y hora.</li> <li>➤ Búsqueda y análisis de aplicaciones vulnerables al inicio de sesión del equipo o según una programación establecida en la consola central.</li> <li>➤ Permitir excluir la instalación de actualizaciones según el tipo de software el cual deberá poder definirse por diversos criterios como: <ul style="list-style-type: none"> <li>▪ Nombre del producto</li> <li>▪ ID del Bulletin de seguridad del fabricante</li> <li>▪ Service Pack</li> <li>▪ Nombre del parche</li> <li>▪ Severidad o Gravedad de la actualización</li> </ul> </li> <li>➤ Descargar las actualizaciones desde la consola central o desde el repositorio más cercano con la finalidad de no consumir el ancho de banda de la institución.</li> </ul>				
	Sistema de detección y respuesta de amenazas (EDR) integrado al software antimalware y no deberá requerir la instalación de un agente separado.	4	4	4	4
	Permitir crear repositorios o consolas distribuidas que gestionen las actualizaciones tanto del producto, firmas de malware y gestionar centralizadamente en cada punto las descargas del módulo del control de vulnerabilidades y parches con la finalidad de minimizar el uso del ancho de banda. Los repositorios de actualizaciones deberán soportar como mínimo los mismos sistemas operativos Windows y Linux que la consola central	1	1	1	1
	Reconocer un incidente y ser enviado al Fabricante desde la misma consola para su análisis e investigación de la amenaza con el fin de contar con mayor detalle de esta, así como recibir información para su reconocimiento y posterior respuesta frente a incidentes iguales o similares.	4	4	4	4
	El EDR usará la automatización de procesos para detener y contener las amenazas inmediatamente. También deberá proporcionar una visualización del ataque con todos los puntos	4	4	4	4



## “Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”

## “Año del Fortalecimiento de la Soberanía Nacional”

		<p>finales afectados, y una guía sobre cómo aislar y remediar la amenaza.</p> <p>El EDR permitirá realizar acciones de supervisión y marcado de las amenazas, configurable por lo menos en (03) criterios: nuevo, en proceso, cerrado o sus equivalentes.</p> <p>Capacidad de escanear y ejecutar los archivos recopilados, en un ambiente aislado para un análisis profundo basado tecnología sandbox opcionalmente de análisis local, utilizando el laboratorio de virus interno, sin enviar la muestra fuera de la red</p> <p>Sistema de reportes de EDR el cual deberá permitir configurar lo siguiente:</p> <ul style="list-style-type: none"> <li>➤ El envío de reportes diarios, semanales o mensuales de la detección de amenazas.</li> <li>➤ Programar el envío automático de alertas por correo frente a la detección de una amenaza.</li> </ul>					
			3	3	3	3	3
			2	1	1	1	1
			3	3	3	3	3
2	Eficiencia	<p>Instalación de sensores livianos desplegados en las versiones de los Sistemas Operativos de las estaciones de trabajo, dispositivos móviles (laptops y tablets con sistema operativo Windows) y servidores de TI. Opcionalmente en Windows 2003 Server, Windows 2003 Server R2 y Windows 7</p> <p>Detecta, detiene, bloquea y evita la instalación, propagación e infección de todo tipo de amenazas.</p> <p>La solución antimalware no debe afectar el performance del equipo, servidor o dispositivo móvil. No debe consumir más del 18% de los recursos de memoria y CPU.</p>	4	4	4	4	4
			2	2	2	2	2
			4	3	3	3	3
3	Capacidad de Mantenimiento	<p>Permite realizar Rollback de firma de malware para casos en los que las firmas generen problemas o incompatibilidades con alguna aplicación específica.</p> <p>La consola de antimalware debe tener la capacidad de conectarse automáticamente a internet y descargar las actualizaciones necesarias para todos los productos activados. Dicha conexión deberá poder configurarse por periodos como hora o día.</p>	1	1	1	1	1
			1	1	1	1	1
4	Portabilidad	<p>Instalarse en su última versión, sobre las plataformas Windows Server 2003, Windows 7, Windows 8, Windows 8.1, Windows 10, Vmware, Hyper-V. Contar con Soporte para plataformas de 32 y 64 bits. Sobre las plataformas Linux de 32 y 64 bits, en distribuciones basadas en Debian y RedHat tales como: Centos, Fedora, Mandriva, OpenSuse, Ubuntu, Suse, FreeBSD etc. Y otras plataformas como Mac OS X 10.6 o posterior de 32 y 64 bits.</p> <p>La consola de acceso al servidor deberá ser 100% web, siendo compatible con los siguientes navegadores: Mozilla Firefox, Chrome, Safari y Opera (opcional).</p> <p>Integrarse con el Directorio Activo ya sea para el despliegue como para la configuración de políticas.</p>	3	2	2	2	2
			2	2	2	2	2
			2	2	2	2	2
<b>Sub Total</b>			<b>82</b>	<b>79</b>	<b>78</b>	<b>78</b>	<b>78</b>
<b>Atributos de Uso</b>							
1	Eficacia	<p>Detecta y brinda contra amenazas: a) Antes de su ejecución, b) En ejecución, c) Después de su ejecución. (revisar)</p> <p>Tiene la capacidad de remediar cualquier cambio realizado en los procesos del equipo (causado por algún tipo de infección o amenaza) a su estado de correcto funcionamiento.</p> <p>La solución antimalware debe permitir un análisis forense de lo</p>	4	4	4	4	4
			4	4	4	4	4
			4	4	4	4	4



“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”  
 “Año del Fortalecimiento de la Soberanía Nacional”

		ocurrido en los equipos, permitiendo realizar una correlación de eventos que brinde visibilidad detallada de las amenazas presentadas.				
2	Productividad	La consola de administración debe desplegar actualizaciones compactas e incrementales que eviten la generación de archivos de gran tamaño, evitando que impacte de manera negativa los recursos como ancho de banda y previniendo la saturación de la red.	1	1	1	1
		La consola de administración debe desplegar las actualizaciones a los agentes clientes de forma automática y de la manera óptima en relación de seguridad y performance.	1	1	1	1
3	Seguridad	Luego de cinco (05) intentos no satisfactorios de inicio de sesión desde una misma dirección IP, el servidor deberá bloquear de forma temporal los intentos posteriores de esta dirección IP por un tiempo determinado.	1	1	1	1
		Controlar a través de políticas todos los componentes mencionados anteriormente (para estaciones de trabajo, dispositivos móviles y servidores de TI) sin necesidad de consolas adicionales para la creación de políticas.	1	1	1	1
		Configurar mediante una política para evitar desinstalación de los Antimalware aun cuando el usuario en el antimalware tenga privilegios de administrador.	1	1	1	1
		Permitir bloquear y/o desactivar mediante políticas el acceso a las opciones de configuración del Antimalware.	1	1	1	1
		<b>Sub Total</b>	<b>18</b>	<b>18</b>	<b>18</b>	<b>18</b>
		<b>Total</b>	<b>100</b>	<b>96</b>	<b>96</b>	<b>96</b>



“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”  
“Año del Fortalecimiento de la Soberanía Nacional”

## ANEXO 02

### Costos referenciales de la solución antimalware, EDR y gestor de parches

N°	Producto	Costo Total (S/)(* )
1	Kaspersky	390,000.00
2	WatchGuard	417,000.00
3	F-Secure	661,272.00

(\*) Expresado en soles (S/), incluye el 18% de IGV.

### Análisis Costo – Beneficio

N°	Producto	Costo Total (S/)(* )	Beneficio	Costo / Beneficio
1	Kaspersky	390,000.00	96	97.20%
2	WatchGuard	417,000.00	96	95.26%
3	F-Secure	661,272.00	96	84.90%



“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”

“Año del Fortalecimiento de la Soberanía Nacional”

### ANEXO 03

#### Costos referenciales de la solución antimalware, EDR y gestor de parches

##### a) Kaspersky

Kaspersky				
Ítem	Cant.	Descripción	Precio Unit.	Precio Total
1	2400	Kaspersky Endpoint Security for Business Advanced, Endpoint Detection and Response Optimum. • Kaspersky Business Software Support – 3 años.	S/ 150.00	S/ 360,000.00
2	1	Servicios • Instalación de Kaspersky Security Center (Cloud u On-Premise) y despliegue de agentes Kaspersky Endpoint Security. • Instalación de Kaspersky Vulnerability & Patch Management. • Instalación y configuración de Kaspersky Endpoint Detection and Response – EDRO.	S/ 10,000.00	S/ 10,000.00
3	1	Soporte Técnico – 3 años • Soporte técnico On-Line (telefónico – e-mail) – Bafing. • Soporte técnico control remoto – Bafing. • Soporte técnico On-Site – Bafing	S/ 15,000.00	S/ 15,000.00
4	1	Capacitación • En Kaspersky Security Center, Kaspersky Vulnerability & Patch Management y Kaspersky Endpoint Detection and Response – EDRO. - 05 personas - 12 horas efectivas.	S/ 5,000.00	S/ 5,000.00
<b>TOTAL</b>				<b>S/ 390,000.00</b>

##### b) Watchguard

#### DATOS DEL CLIENTE

Nombre **MINISTERIO DE LA PRODUCCION**

N°	DESCRIPCIÓN	CANTIDAD	P.U.	PRECIO TOTAL
1	Watchguard EPDR 3 años (versión upgrade de Panda Adaptive Defense 360)	2,400	S/. 160	S/. 384,000
2	Servicios de implementación	1	S/. 12,000	S/ 12,000
3	Soporte Técnico por 3 años	1	S/. 15,500	S/ 15,500
4	Capacitación Certificada de los productos	1	S/. 5,500	S/ 5,500
Total incluido IGV				S/ 417,000



“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”  
 “Año del Fortalecimiento de la Soberanía Nacional”

c) F-Secure

Descripción	IGV	P.U.	Cant.	Total (Base imp.)
F-SECURE ELEMENTS ENDPOINT PREMIUM + ENDPOINT DETECTION AND RESPONSE PARA ESTACIONES - CLOUD 3AÑOS INCLUYE: [CARACTERÍSTICAS ENDPOINT] > Doble motor antimalware > Antitransomware, Heurística Avanzada, Inteligencia Artificial > Tecnología DataGuard que mejora la protección antitransomware > HIPS, Detección de Vulnerabilidades y Prevención de Explotaciones > Control de Aplicaciones completo con centro de control que permite implementar IoC (Indicadores de Compromiso) para la generación de políticas de seguridad. > Control de Dispositivos completo > Control de Navegación web > Protección de Navegación Web > Gestión de Firewall Avanzado > Gestión de Vulnerabilidades con Aplicación de Parches Multifabricante > Inventario de aplicaciones con vulnerabilidades y/o parches faltantes. > Soporte para repositorios en Windows y Linux > Sistema de Aislamiento de Equipos > SANDBOX en la nube con F-Secure Cloud basado en el proyecto BlackFin ganador del Premio a la Excelencia en Inteligencia Artificial 2021 > Permite detectar y bloquear malware nuevo y desconocido en 5 minutos o menos > Sistema programador de tareas para: Apagado y Reinicio de equipos, Hibernación, Instalación de Parches, Escaneos, etc. > Integración con Sistemas SIEM, SOAR, SOC [CARACTERÍSTICAS EDR] > Brinda visibilidad instantánea del estado de la seguridad IT de la empresa > Detecta ataques rápidamente y responde en base a guías expertas > Permite elevar casos a F-Secure para ser revisados por especialistas de la marca. > Tecnología SandBox Broad Context Detection > Buscador de Eventos para la búsqueda de amenazas > Respuestas automatizadas > Análisis de Causa Raíz > Integración con la Técnicas y Tácticas de Ataque de Mitre Att&k > Visualización de Indicadores de Compromiso > Aislamiento de Equipos ** automatizado ** > Inventario de Aplicaciones	18%	211.00	2400	506,400.00
SOPORTE PROFESIONAL LOCAL > Implementación de la solución de hasta el 80% > Capacitación inicial y durante el período de licenciamiento por cambio de				
versiones > Soporte vía correo, teléfono y mensajería instantánea > Monitoreo de la plataforma en forma remota > Emisión de reportes mensuales del estado de la solución > Sistema de Mesa de Ayuda en proceso de Certificación de Calidad ISO 9001:2015	18%	1,500.00	36	54,000.00

Condiciones de pago:	Según EETT, Contrato u OC	Total (Base imp).	560,400.00
Tipo de pago:	Según Contrato	Total impuesto 18%	100,872.00
		<b>Total</b>	<b>661,272.00</b>