Gobernación de Casanare
NIT:892099216-6

FICHA TÉCNICA

Es de gran importancia para la Gobernación de Casanare a través de la Dirección de Tecnologías de la Información y las Comunicaciones TIC, encontrar en el mercado productos de alta calidad, que cumplan con los requerimientos solicitados para el proceso con objeto: ADQUISICIÓN DEL SOFTWARE DE PROTECCIÓN Y SEGURIDAD ANTIVIRUS PARA EL ASEGURAMIENTO DE ESTACIONES DE TRABAJO Y SERVIDORES DE LA GOBERNACIÓN DE CASANARE.

Lo anterior teniendo en cuenta las siguientes especificaciones técnicas:

Ítem	01
Denominación de bien o servicio	Software de seguridad y protección
Denominación técnica del bien o servicio	Software solución Antivirus/Kaspersky Next EDR Optimum
Grupo / clase / familia a la que pertenece el bien o servicio	43233205
Unidad de medida	Unidad
Descripción general	El fabricante de las soluciones ofertadas debe contar con, al menos, 25 años de presencia en el mercado global. El fabricante de las soluciones ofertadas debe contar con un equipo de investigación global y con presencia de por lo menos cinco (5) analistas de investigación de amenazas basados en países de Latinoamérica, dedicados a la investigación y el análisis de amenazas para la región. Se debe proveer una solución tecnológica que incluya una poderosa protección de endpoints basada en IA, controles de seguridad flexibles y características de EDR incorporadas. La solución debe contar con una consola fácil de usar, opciones de implementación en la nube y/o on-premises, así como también una variedad de funciones que simplifiquen la vida del usuario, reduciendo la complejidad y aumentando la eficiencia. La solución debe proteger endpoints y servers, sean estos Windows, Linux, macOS, así como también dispositivos móviles iOS y Android. La solución debe disponer de una única licencia que debe permitir el uso de la consola nube u on-premise, como así también de todos los endpoints y servers que disponga la organización, independientemente del sistema operativo del dispositivo en cuestión. La solución debe permitir la implementación de puntos de distribución en diferentes segmentos de red o ubicaciones geográficas de la organización que permita la distribución de actualizaciones, sondeo de red, instalación remota de aplicaciones, obtención de información sobre equipos de un grupo de administración, y/o difusión de dominio, entre otras. La solución debe incluir una infraestructura de servicios en la nube que brinde acceso a la base de conocimientos del fabricante, ofreciendo un recurso en línea que permita conocer la reputación de los archivos, los

	recursos web y el software, garantizando respuestas más rápidas ante nuevas amenazas, mejorando el rendimiento de algunos componentes de protección y reduciendo el riesgo probable de que se produzcan falsos positivos. La solución debe contar con la capacidad de eliminar remotamente cualquier solución antivirus (propia o de terceros) que esté presente en los endpoints y servidores, sin la necesidad de la contraseña de remoción del actual antivirus; La solución debe disponer de la capacidad de instalar remotamente la solución de antivirus en los endpoints y servidores Windows, a través de la administración compartida, login script y/o GPO de Active Directory; La solución debe contar con la capacidad de generar paquetes personalizados (autoejecutables) conteniendo la licencia y configuraciones del producto; La solución debe disponer de la capacidad de importar la estructura de Active Directory para encontrar máquinas; La solución debe contar con la capacidad de monitorear diferentes subnets de red con el objetivo de encontrar máquinas nuevas para que sean agregadas a la protección; La solución debe disponer de la capacidad de, al detectar máquinas nuevas en el Active Directory, subnets o grupos de trabajo, automáticamente importar la máquina a la estructura de protección de la consola y verificar si tiene el antivirus instalado. En caso de no tenerlo, debe instalar el antivirus automáticamente; La solución debe combinar protección basada en firmas, análisis heurístico y de comportamiento, junto con tecnologías asistidas por la nube para proteger los endpoints contra amenazas de malware conocidas, desconocidas y avanzadas. La solución debe permitir habilitar la protección con contraseña con el fin de restringir el acceso de los usuarios a la solución en la estación de trabajo según los permisos que se le otorgaron (por ejemplo, permiso para salir de la aplicación). Las solución debe proporcionar mecanismos de autoprotección con el fin de evitar que otras aplicaciones realicen acciones que puedan interferir con el funcionamiento de la solución propuesta. La solución debe permitir realizar un análisis personalizado para cualquiera de los siguientes objetos: Memoria del sistema, Objetos cargados en el inicio del sistema operativo, Copia de seguridad del sistema operativo, Buzón de correo de Microsoft Outlook, Unidades de disco duro, Unidades extraíbles y unidades de red o Cualquier archivo seleccionado. La solución debe permitir analizar archivos compuestos de formatos ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros archivos comprimidos. La solución debe incorporar un componente de protección frente a amenazas web que permita evitar la descarga de archivos maliciosos de Internet y también bloquee sitios web maliciosos y de phishing. La solución debe analizar tráfico HTTP, HTTPS y FTP.

FICHA TÉCNICA

	La solución debe bloquear el tráfico HTTP que no cumple con los estándares RFC. La solución debe incluir un componente de protección frente a amenazas en el correo que permita analizar los archivos adjuntos de mensajes de correo electrónico entrantes y salientes en busca de virus y otras amenazas. La solución de protección frente a amenazas en el correo debe ser compatible con POP3, SMTP, IMAP y NNTP. La solución debe incluir un componente de protección frente a amenazas en la red que monitoree el tráfico de red entrante en busca de actividad característica de los ataques de red. La solución debe bloquear el equipo que realiza el ataque y restringir el envío de paquetes de red durante un periodo determinado de al menos una hora. La solución debe permitir activar y administrar la protección contra los siguientes tipos de ataques a la red, mínimamente: Inundación de red (flooding) ataques de tipo "Port scan", Ataques de spoofing de MAC. La solución debe incluir un componente de Firewall de escritorio que bloquee las conexiones no autorizadas al equipo mientras se trabaja en Internet o en la red local. El componente de firewall de escritorio debe incluir un componente prevención de intrusiones en el host que proporcione acceso controlado de las aplicaciones a los recursos, procesos y datos personales del sistema operativo mediante el uso de derechos de aplicación. El componente de firewall de escritorio debe controlar la actividad de la red sobre el protocolo seleccionado: TCP, UDP, ICMP, ICMPv6, IGMP y GRE. El componente de firewall de escritorio debe, de forma predeterminada, crear un conjunto de reglas de red para cada grupo de aplicaciones que la solución detecta en el equipo. La solución debe incluir un componente de prevención de ataques a nivel de USB impide que dispositivos USB infectados que emulan un teclado se conecten al equipo. El componente de prevención de ataques a nivel de USB debe permitir que los dispositivos USB que el sistema operativo identifique como teclados y que estén conectados al equipo antes de instalar el componente se consideren autorizados después de la instalación del componente. El componente de prevención de ataques a nivel de USB debe bloquear automáticamente el dispositivo USB si el código de autorización se introduce incorrectamente un número de veces especificado. El componente de prevención de ataques a nivel de USB debe permitir utilizar un teclado en pantalla para autorizar dispositivos USB que no permitan introducir caracteres aleatorios (p.ej., escáneres de códigos de barras). La solución debe incluir un componente de protección AMSI diseñado para ser compatible con Antimalware Scan Interface de Microsoft. El componente de protección AMSI debe permitir configurar el análisis de protección AMSI para archivos compuestos, como archivos de almacenamiento, paquetes de distribución o archivos en formatos de Office. Los derechos de las aplicaciones debe incluir los siguientes parámetros de acceso:

FICHA TÉCNICA

	- Acceso a recursos del sistema operativo (por ejemplo, opciones de inicio automático y claves de registro) - Acceso a datos personales (como archivos y aplicaciones). El componente de prevención de intrusiones en el host debe activar la protección del acceso a audio y vídeo, de manera que se evite que los ciberdelincuentes puedan usar programas especiales para intentar obtener acceso a dispositivos que graban audio y vídeo (como micrófonos o cámaras web), controlando cuándo las aplicaciones reciben una transmisión de audio o vídeo y protege los datos contra la interceptación no autorizada. La solución debe incluir un componente de motor de reparación que le permita revertir las acciones realizadas por aplicaciones maliciosas en el sistema operativo. El componente de motor de reparación debe permitir anular la actividad de malware en el sistema operativo a los siguientes tipos de actividad de malware: - Elimina los archivos ejecutables que el malware ha creado (en cualquier tipo de soporte, excepto unidades de red) - Elimina los archivos ejecutables creados por programas en los que el malware se ha infiltrado - Restaura los archivos que el malware ha modificado o eliminado - Elimina las claves del registro que el malware ha creado - No restaura las claves del registro que el malware ha modificado o eliminado - Finaliza los procesos iniciados por el malware - Finaliza los procesos en los que haya penetrado una aplicación maliciosa - No reanuda procesos que el malware haya suspendido - Bloquea la actividad de red del malware - Bloquea la actividad de red de los procesos en los que el malware se ha infiltrado. La solución debe incluir un componente de control web que permita regular el acceso de los usuarios a los recursos web. El componente de control web debe permitir supervisar tráfico HTTP y HTTPS. El componente de control web debe permitir configurar el acceso a los sitios web a través de estos criterios: - Categorías de sitios web - Tipo de datos - Direcciones individuales El componente de control web debe permitir la creación de reglas de acceso a recursos web mediante el uso de filtros y acciones que la solución realiza cuando el usuario visita recursos web. El componente de control web debe utilizar al menos los siguientes filtros: - Filtrar por contenido y tipo de datos - Filtrar por direcciones de recursos web - Filtrar por nombres de usuarios y grupos de usuarios. El componente de control web debe permitir seleccionar alguna de las siguientes acciones: - Permitir - Bloquear - Advertir

FICHA TÉCNICA

	La solución debe incluir un componente de control de dispositivos que administre el acceso de los usuarios a dispositivos instalados o conectados al equipo (por ejemplo, discos duros, cámaras o módulos wifi), con el fin de proteger el equipo de infecciones cuando se conectan los dispositivos; y se evitan pérdidas o fugas de datos. El componente de control de dispositivos debe permitir crear reglas del acceso para los siguientes tipos de dispositivo, mínimamente: - Discos duros - Unidades extraíbles (incluidas las unidades flash USB) - Disquetes - Unidades de CD/DVD - Dispositivos portátiles (MTP) - Impresoras locales - Impresoras de red - Módems - Unidades de cinta - Dispositivos multifuncionales - Lectores de tarjetas inteligentes - Dispositivos Windows CE USB ActiveSync - Adaptadores de red externos - Bluetooth - Cámaras y escáneres El componente de control de dispositivos debe proporcionar funciones de Anti-Bridging con el fin de impedir establecer conexiones de red simultáneas en un equipo para prevenir la creación de puentes de red. La solución debe incluir un componente de control de aplicaciones que permita gestionar el inicio de aplicaciones en los equipos de los usuarios. El componente de control de aplicaciones debe realizar un inventario de los archivos con los siguientes formatos: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX y SCR, cuando se añade contenido manualmente. La solución debe incluir características básicas de Endpoint Detection and Response (EDR). La solución debe contar, dentro de su licenciamiento, con integración y acceso con un Portal de Inteligencia contra Amenazas, que permita consultar información sobre la reputación de archivos y URLs. La solución debe permitir establecer exclusiones de aislamiento de red. Es decir que las conexiones de red que cumplan las condiciones de la exclusión especificada no se bloquearán en los dispositivos después de que se active el aislamiento de red. La solución debe incluir, dentro de su licenciamiento, un SandBox basado en Nube que permita detectar amenazas complejas en los equipos de los usuarios. La solución debe permitir crear tareas de análisis de IoC de forma automática en respuesta a una amenaza detectada por el Sandbox basado en nube. La solución debe permitir ejecutar una de las siguientes acciones de respuesta disponibles para los IoC detectados: - Aislar el dispositivo de la red. - Ejecutar análisis de áreas críticas. - Poner la copia en cuarentena y eliminar el objeto La solución debe incluir un componente de cifrado de datos que permita cifrar las carpetas y los archivos almacenados en las unidades locales

FICHA TÉCNICA

	y extraíbles, o las unidades extraíbles y los discos duros por completo, con el fin de minimizar el riesgo de filtraciones de información que se puede producir en caso de pérdida o robo del equipo portátil, unidad extraíble o disco duro, o cuando usuarios y aplicaciones no autorizados acceden a los datos. El componente de cifrado de datos debe ofrecer las siguientes características de protección de datos: - Cifrado de archivos en unidades locales del equipo - Cifrado de unidades extraíbles - Gestión de reglas de acceso de las aplicaciones a los archivos cifrados - Creación de paquetes cifrados - Cifrado de disco completo El componente de cifrado de datos debe permitir realizar cifrado de disco completo con la tecnología de cifrado propietaria del fabricante. El componente de cifrado de datos debe ser compatible con los sistemas de archivos FAT32, NTFS y exFAT. El componente de cifrado de datos debe incluir los siguientes estados de cifrado: - No cumple la directiva; cancelado por el usuario. El usuario ha cancelado el cifrado de datos. - No cumple la directiva debido a un error. Error de cifrado de datos; por ejemplo, falta una licencia. - Aplicando la directiva. Reinicio necesario. Cifrado de datos en curso en el equipo. Reinicie el equipo para completar el cifrado de datos. - No se ha especificado ninguna directiva de cifrado. El cifrado de datos está desactivado en la configuración de directiva. - No compatible. Los componentes de cifrado de datos no están instalados en el equipo. - Aplicando la directiva. El cifrado y el descifrado de datos está en curso en el equipo. La Solución de Seguridad debe integrarse con Microsoft Office 365 de manera nativa mediante Microsoft Office 365 API sin influir ni requerir cambios en los flujos de tráfico de correo electrónico. La solución debe disponer de una consola de gestión que permita la configuración y administración multi-usuario de todas las capacidades ofertadas de manera integral, facilitando la gestión de la seguridad en Microsoft Office 365. La solución debe de validar de Spam, Phishing, Ransomware, BEC, amenazas conocidas y desconocidas en tiempo real para correos electrónicos entrantes, salientes y aquellos que fluyen internamente en la propia instancia de Microsoft Office 365. La solucion debe utilizar heurística avanzada, aislamiento de procesos, aprendizaje automático y otras tecnologías de última generación para proteger a las empresas que utilizan Microsoft Exchange Online, Microsoft Teams, Microsoft OneDrive y Microsoft SharePoint Online contra el ransomware, archivos adjuntos maliciosos, spam, phishing, correos electrónicos que comprometen la seguridad de la empresa (BEC) y amenazas desconocidas. La solución debe cumplir con el Reglamento General de Protección de Datos (RGDP) y protección de los datos. La solución debe de contar con tecnologías de detección Anti-Spam, Anti-Phishing, Anti-Malware, Anti-Ransomware, Anti-BEC & capacidades de filtrado de contenido.

FICHA TÉCNICA

	La solución debe de contar con tecnologías proactivas para la detección de amenazas avanzadas o de día 0. La solución debe de contar con tecnologías de detección avanzadas para la detección y neutralización de amenazas del tipo Ransomware. La solución debe disponer de capacidades de escaneo bajo demanda sobre buzones de correo pudiendo seleccionar. - Grupos de usuarios - Usuarios - Todos los usuarios La solución debe poder clasificar los correos basura en dos categorías: Spam y correos masivos y poder definir las acciones a tomarse en cada uno de los casos. La solución debe contar con capacidades de generar direcciones de lista blanca y negra para cada uno de los módulos de seguridad que propone. La solución debe disponer de funciones de validación y autentificación del remitente de manera automática que incluyan: - DKIM - DMARK - SPF La solución debe de disponer de modulo anti malware para la detección oportuna de amenazas conocidas, desconocidas y avanzadas en Microsoft Exchange Online, Microsoft OneDrive, Microsoft SharePoint Online y Microsoft Teams bajo tecnologías de: - Firmas, - Análisis heurísticos - Comportamiento. La solución no debe almacenar datos sensibles como usuarios y contraseñas y para esto debe de poder integrase con Microsoft Office 365 mediante OAuth 2.0 La protección de anti-malware para Microsoft SharePoint Online debe permitir la exclusión y selección de sitios protegidos. Debe disponer de un módulo de supervisión de fuga de datos con el objetivo del descubrimiento de información confidencial transmitida y almacenada por los usuarios en los buzones de correo de Exchange Online, en los almacenamientos de OneDrive y en los sitios de SharePoint Online de la organización relacionadas con datos de tarjetas de crédito. La solución debe contar con capacidades de escaneo retrospectivo de amenazas que incluya los buzones de correo y de Ms Office 365 y los repositorios de datos de OneDrive. La solución propuesta debe incluir formación en ciberseguridad dentro de la aplicación. La solución propuesta debe dividir el entrenamiento en varios módulos, donde cada uno de los modulo debe estar en una serie de secciones. Los modulos propuestos deben incluir teoría relevante y capacidad de realizar tareas interactivas en un entorno simulado. La solución propuesta debe permitir descargar un certificado que acredite los logros una vez completadas todas las secciones de un módulo. Los modulos propuestos deben ser de entrenamientos en ciberseguridad agnósticos entre los que se encuentren Respuestas a Incidentes, Software Malicios, Aseguramiento de Directorio Activo y Seguridad para servidores, entre otros.

Gobernación de Casanare
NIT:892099216-6

FICHA TÉCNICA

Calidad mínima	N/A
Patrones de desempeño mínimo	N/A



JAVIER FONSECA ROSAS
DIRECTOR TÉCNICO
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES TIC

Proyectó: Yadira Piedrahíta Beltrán / profesional contratada