FICHA TÉCNICA

Términos de Referencia Bitdefender GravityZone Enterprise

Protección estaciones de trabajo y servidores	La plataforma de seguridad de protección para Endpoints (EPP) debe utilizar e integrar al menos las siguientes tecnologías de protección para todo tipo de amenaza de seguridad para los endpoints y red, sea que se trate de un Amenaza Persistente Avanzada o de malware conocido o desconocido. La tecnología de detección y protección antimalware de la solución tiene que abarcar las siguientes capas de protección: • Sistema unificado de prevención, detección avanzada y respuesta y análisis de riesgos **EDR / XEDR,** con características extendidas de análisis y correlación de eventos a nivel de endpoint. • Sistema de identificación de amenazas desconocidas a través de **Sandbox Analyzer** • Análisis integrado de riesgos en los endpoints y Hardening, **Endpoint Risk Managemet** • Sistema de prevención de ataques de Red • Detección y búsqueda basado en la Nube • Detección basada en heurística Avanzada • Detección en la atapa pre-ejecución basado en Machine Learning. • Sistema de prevención de intrusión basado en el host
Administración Centralizada de la solución	La solución debe disponer una consola de administración unificada que se administre en la nube **(Consola WEB)** con capacidad de administrar un número ilimitado de equipos. La solución debe proporcionar un único punto para la implementación, aplicación y administración de las políticas de seguridad para el número de puntos finales solicitados por la institución, siendo estos de cualquier tipo y en cualquier ubicación. La solución debe aportar múltiples capas de seguridad para puntos finales, incluyendo servidores de correo de Microsoft Exchange, asegurando protección antimalware con monitorización del comportamiento, protección contra amenazas de día cero, control de aplicaciones y entorno de pruebas, cortafuego, control de dispositivos, control de contenidos, antiphishing y antispam. La solución debe brindar soporte para múltiples plataformas sin importar el número de portátiles, equipos de escritorio y servidores Windows, Linux y Mac OS X, contando con las tecnologías antimalware mejor valoradas. Además, para sistemas Windows debe brindar una seguridad aún más avanzada con un cortafuego bidireccional, detección de intrusiones, control y filtrado de acceso Web, protección de datos sensibles, y control de aplicaciones y de dispositivos,

	la heurística proactiva dLa solución debe clasificar los procesos maliciosos según su comportamiento, asegurando la detección de nuevas amenazas en tiempo real. La solución debe brindar seguridad para centros de datos virtualizados, protegiendo tecnologia de próxima generación pre-ejecución, que utiliza modelos de Machine Learning especializados, técnicas de análisis del comportamiento entrenados para detectar herramientas de pirateo, exploits y técnicas de ocultación de malware. Bloquea eficazmente los ataques que pasan por alto tanto las defensas tradicionales para endpoints como las denominadas defensas “antivirus de última generacións en sistemas Windows y Linux. La solución debe aporta mejoras significativas de rendimiento e impulsar la consolidación del servidor. Las políticas pueden aplicarse a un pool de recursos de VMware vCenter La solución debe incluir un mecanismo automático de detección de redes que le permita detectar otros puntos finales en la red de la institución. Los puntos finales detectados deben mostrase como puntos finales no administrados en la Consola de Administración. La solución debe permitir instalar los agentes de seguridad en puntos finales físicos y virtuales ejecutando los paquetes de instalación localmente o ejecutando tareas de instalación remotamente desde la Consola de Administración. Adicional la consola WEB de administración, será capaz de gestionar un enlace web (Link de descarga) el cual podrá ser enviado por mail para realizar la instalación remota de clientes fuera de la red corporativa, el mismo que se auto configurará para enlazarse con la consola web, sin intervención del personal de TI El kit de instalación para puntos finales además debe permitir instalar la protección en los puntos finales sin conexión a Internet o con conexiones lentas. Debe utilizar un solo paquete, tanto para sistemas operativos de 32 bits como de 64 bits: – SO Windows: sistemas de 32 bits y 64 bits – SO Linux: sistemas de 32 bits y 64 bits – Mac OS X: solo sistemas de 64 bits La solución debe garantizar que el agente en los equipos administrados ejecute el análisis en tiempo real incluso cuando no haya conexión, cumpliendo las tareas, políticas y requerimientos configurados previamente aun cuando no haya conexión con la Consola de Administración. El agente de seguridad debe detectar automáticamente la configuración del punto final y adaptará la tecnología de análisis.

	Debe permitir la visibilidad, administración y consulta de los puntos finales físicos y virtuales, gestionándolos desde la consola de administración. La consola debe permitir la creación ilimitada de grupos o carpetas o subgrupos con el fin de permitir una mejor organización y administración de políticas. La consola deber permitir la asignación de políticas basado en reglas de asignación, ya sea por IP, Usuario, DNS, puerta de enlace o Gateway, WINS, DHCP, HOST y tipo de red. **La consola Cloud o web** La solución de seguridad antimalware debe permitir g**estionar en la web a través de una consola alojada en la nube lista y provista en su totalidad por el fabricante** (Cloud) desde un único punto de administración a través de cualquier tipo de dispositivo con acceso internet en cualquier sitios del mundo **sin límite de usuarios**, la consola Web Control Center, facilitara el acceso y la administración de la estrategia general de seguridad, las amenazas a la seguridad global, y el control sobre todos los módulos de seguridad que protegen a los equipos de escritorio virtuales o físicos y a los servidores. El Web Control Center debe ser capaz de abordar las necesidades de incluso las organizaciones más grandes sin la necesidad de utilizar múltiple consola de apoyo. Control Center, una interfaz basada en Web, se debe integrar con los sistemas de monitorización y administración existentes para aplicar fácilmente el sistema de protección a los equipos de escritorio, virtuales y servidores no administrados. Permitir la aplicación y gestión de políticas en los endpoint independientemente de que se encuentren o no en las instalaciones locales. **Soporte para múltiples plataformas,** debe funcionar tanto en equipos Windows como Linux. Permitiendo instalarse todos los componentes deseados simultáneamente con el programa de instalación general o eligiendo los componentes individuales. También debe desplegar el programa como un dispositivo virtual. **Incluir un agente independiente que actúe incluso cuando no hay conexión,** este agente independiente ejecutará todas las tareas, políticas y sucesos directamente en el endpoint, aunque no tenga conexión con la consola. **Una arquitectura de replicador y servidor de comunicación tipo Relay para gestionar la red,** las ubicaciones remotas solo necesitan la implementación de un antivirus con este módulo adicional sin la necesidad de instalar una consola de replicación o una consola esclava o un servidor proxy de la consola, el relay recopilará y reenviará los datos agregados al servidor principal.

	Manejar la comunicación con los agentes, y recopilar y almacenar los datos de las aplicaciones. Ser capaz de manejar decenas de miles de clientes manteniendo su elevada velocidad operativa sin saturar la infraestructura Incluir un **sensor detector de equipos no autorizados,** descubrir todos los equipos de la red que no están protegidos ni administrados y mostrárselos al administrador. El mecanismo automático de detección de red Pensado para detectar los equipos del grupo de trabajo. El mecanismo automático de detección debe utilizar el servicio Microsoft Computer Browser para realizar una detección de red. El servicio Computer Browser es una tecnología de red utilizada por los equipos basados en Windows para mantener listas actualizadas de dominios, grupos de trabajo y los equipos en ellos, y para suministrar estas listas a equipos cliente que lo soliciten. Los equipos detectados en la red por el servicio Computer Browser pueden visualizarse ejecutando el comando de net view en una ventana de símbolo del sistema. Configurar las opciones de notificación siguiendo unos pasos específicos. Ejecutar las políticas directamente en el agente y aplicar políticas específicas para los endpoint incluso cuando no haya conexión con el servidor consola. Otra vez del uso de un usuario con permisos configurado previamente en la política. Recopilar datos necesarios para generar los informes; los registros restantes se deberán almacenar en el cliente para mejorar el rendimiento de la base de datos. Crear múltiples cuentas de usuarios y personalizarlas, los privilegios para cada una se podrán personalizar en forma individual. Se podrá usar en muchas ubicaciones distintas y permitir definir políticas corporativas para los administradores locales. El administrador de licencias permitirá el manejo de todas las licencias en forma transparente, desde cualquier punto a través de un navegador Web **sin tener la necesidad de publicar ningún servicio a la Web**. Limpieza de equipos terminales y servidores de código malicioso y programas inseguros no autorizados instalados.

	La herramienta permitirá realizar acciones en caso de ser necesario. Además de mostrar los informes a través de la consola basada en la Web, se pueden exportar en formato PDF, Excel y guardar en una ubicación predefinida, y enviarse como una notificación por correo electrónico. La solución deberá contar con un módulo de protección que proteja las aplicaciones más comunes como: lectores de PDF, navegadores web, clientes de correo, etc en caso de que se trate de explotar una vulnerabilidad. Protección contra vulnerabilidades: Mejora la detección de las Vulnerabilidades y Exposiciones Comunes (CVE) en los protocolos más utilizados, como SMB, RPC y RDP. Brinda protección contra las vulnerabilidades para las cuales aún no se publicó o desarrolló la revisión necesaria. Protección ante botnets: Protege ante las infiltraciones por malware de tipo botnet, previniendo el envío de spam y evitando que se lleven a cabo ataques de red desde la endpoint. Desinstalación de soluciones de seguridad: la solución deberá ser capaz de desinstalar la solución que se encuentra instalada actualmente. Deberá contar con la posibilidad de sincronizarse con Active directory en su versión clous y on premise Debe permitir generar grupos de clientes dinámicos (paramétricos). La consola de gestión debe mostrar la lista de servidores y estaciones que tienen el antivirus instalado, conteniendo la siguiente información mínima: nombre de la máquina, versión de antivirus, versión del motor, fecha de la vacuna, la última fecha de verificación, política aplacada, ip, sistema operativo y el estado. Se deberá poder visualizar el estado de la red desde paneles portlets o widgets que sean completamente personalizables, tanto en cantidad como en contenido. Dicha información será en tiempo real y se podrá elegir si verla en formato grafico o tabla
Protección para Plataformas Windows, Linux y Mac	**La solución EndPoint deberá proteger las siguientes plataformas:**

	Sistemas operativos de escritorio ● Windows 10 ● Windows 8.1 ● Windows 8 ● Windows 7 **Sistemas operativos integrados y de tablets** ● Windows 10 IoT Enterprise ● Windows Embedded 8.1 Industry ● Windows Embedded 8 Standard ● Windows Embedded Standard 7 ● Windows Embedded Compact 7 ● Windows Embedded POSReady 7 ● Windows Embedded Enterprise 7 **Sistemas operativos de servidor** ● Windows Server 2019 ● Windows Server 2019 Core ● Windows Server 2016 ● Windows Server 2016 Core ● Windows Server 2012 R2 ● Windows Server 2012 ● Windows Small Business Server (SBS) 2011 ● WindowsServer2008R2 **SISTEMAS OPERATIVOS LINUX** ● Ubuntu 14.04 LTS o superior ● Red Hat Enterprise Linux / CentOS 6.0 o superior

	● SUSE Linux Enterprise Server 11 SP4 o superior ● OpenSUSE Leap 42.x ● Fedora 25 o superior(1) ● Debian 8.0 o superior ● Oracle Linux 6.3 o superior ● Amazon Linux AMI 2016.09 o superior ● Amazon Linux 2 **SISTEMAS OPERATIVOS Mac OS X** ● MacOSBigSur(11.0)* ● MacOSCatalina(10.15) ● MacOSMojave(10.14) ● MacOSHighSierra(10.13) ● MacOSSierra(10.12) ● OSXElCapitan(10.11) **NAVEGADORES SOPORTADOS** ● Internet Explorer 8+ ● Mozilla Firefox 30+ ● Google Chrome 34+ ● Safari 4+ ● Microsoft Edge 20+ ● Opera 21+ **VIRTUALIZADORES SOPORTADOS** ● VMware vSphere 6.7 actualización 2a, 6.7 actualización 1, 6.7, 6.5, 6.0, 5.5, 5.1, 5.0 con VMware vCenter Server 6.7 actualización 2a, 6.7 actualización 1, 6.7, 6.5, 6.0, 5.5, 5.1, 5.0 ● VMware Horizon/View 7.7, 7.6, 7.5, 7.1, 6.x y 5.x ● VMware Workstation 11.x, 10.x, 9.x, 8.0.6

	● VMware Player 7.x, 6.x, 5.x ● Citrix XenServer 7.x, 6.5, 6.2, 6.0, 5.6 o 5.5 (incluyendo hipervisor Xen) ● Citrix Virtual Apps y Desktops 7 1808, 7 1811, 7 1903, 7 1906 ● Citrix XenApp y XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR ● Citrix VDI-in-a-Box 5.x ● Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2 o Windows Server 2008 R2, 2012, 2012 R2 (incluyendo Hyper-V Hypervisor) ● Red Hat Enterprise Virtualization 3.0 (incluyendo KVM Hypervisor) ● Oracle VM 3.0 ● Oracle VM VirtualBox 5.2, 5.1 ● Nutanix Prism con AOS 5.5, 5.6 (Enterprise Edition) ● Nutanix Prism versión 2018.01.31 (Community Edition)
EDR / XEDR (ENDPOINT DETECTION AND RESPONSE)	La solución es una plataforma de detección y respuesta de punto final que admite una solución modular de seguridad de la información capaz de proteger cualquier entorno empresarial en un método escalable y de alta disponibilidad. Es un componente de correlación de eventos, capaz de identificar amenazas avanzadas o ataques en curso. Como parte de la plataforma integral e integrada de **Endpoint Protection, EDR /XEDR** reúne la inteligencia del dispositivo en toda la red empresarial. Esta solución viene en ayuda del esfuerzo de los equipos de respuesta a incidentes para investigar y responder a amenazas avanzadas. La Solución debe proporcionar información detallada de los incidentes detectados, un mapa interactivo de incidentes y acciones correctivas • Detección y visualización de actividades sospechosas • Detección de anomalías • Análisis de causa raíz • Etiquetado de eventos MITRE • Puntuación de confianza respecto a la amenaza • Indicadores de ataque • Shell de comandos remotos • Investigación guiada de incidentes • Opciones avanzadas de contención de amenazas • Análisis de Sandbox • Servicio opcional de detección y respuesta administradas

Componentes EDR /XEDR

La solución deberá tener estos componentes principales:

1. El sensor EDR, que recopila y procesa datos para informar datos sobre el punto final y el comportamiento de la aplicación.
2. Security Analytics, un componente de back-end utilizado para interpretar los metadatos recopilados por el sensor EDR.
3. Tecnología de correlación de eventos entre terminales conocida como eXtended Endpoint Detection and Response XEDR. Capacidad XDR para detectar ataques avanzados en múltiples puntos finales en infraestructuras híbridas (estaciones de trabajo, servidores o contenedores, ejecutando varios sistemas operativos)

Detección posterior al compromiso de actividad sospechosa

La solución deberá supervisar los eventos de punto final en busca de signos de ataque y genera un incidente cuando se detecta dicha actividad.

1. ras tiene la capacidad de basar los sistemas en función de los indicadores de ataque MITRE y la inteligencia de amenazas de la solución
2. Cualquier desviación de la línea de base se informa como incidente en nuestro módulo EDR.

Investigación de incidentes y visualización

1. La solución proporcionara soporte para el análisis de incidentes al proporcionar herramientas para ayudar a filtrar, investigar y tomar medidas en todos los eventos de seguridad detectados por el sensor EDR durante un intervalo de tiempo específico.
2. La solución asigna un valor de puntaje de confianza que indica el grado de certeza de que un evento de seguridad es peligroso.
3. La solución se integra con la base de conocimiento ATT & CK de MITRE y etiqueta los eventos de seguridad de manera adecuada.
4. Los eventos de seguridad se pueden buscar por nombres de archivo, direcciones IP, nombres de host o IOC. También proporciona una función de búsqueda avanzada que permite al usuario pasar por eventos pasados según un criterio complejo. Las consultas predefinidas están diseñadas para casos de búsqueda de eventos de seguridad útiles.
5. La solución proporcionara una visualización sofisticada de eventos de seguridad con información específica o acciones con la siguiente información:
   a. La pestaña Resumen proporciona una visión general del impacto del evento e información detallada sobre cada nodo de evento.
   b. La función de línea de tiempo recopila información sobre el desarrollo de eventos de seguridad en un orden cronológico.
   c. Remediation Actions recopila información sobre las acciones de bloqueo que La solución realiza automáticamente en el evento de seguridad actual.
6. La solución puede bloquear archivos / procesos de la lista usando los valores hash MD5 / SHA256. Puede hacerse desde el incidente de seguridad o importarse desde un archivo CSV.

Contención de amenazas

Cuando se detecta una amenaza de seguridad, La solución proporciona las siguientes acciones correctivas para la contención de amenazas.

A. Remediación rápida:

La solución puede aplicar acciones correctivas desde esta sección como una solución temporal al evento de seguridad.

1. Matar: evita que un proceso se ejecute en el entorno. Esto crea una tarea de proceso de eliminación en el punto final local. Los procesos System32 y de la solución de seguridad están excluidos de esta acción.

	2. Archivo de cuarentena: almacena el elemento en cuestión y evita que ejecute su carga útil. 3. Aislar host: La solución ísla el host de la red. El punto final objetivo retiene la comunicación con los servicios de solución de Seguridad 4. Instalar parches: esto permite instalar parches de seguridad faltantes en el punto final de destino. **B. Acciones de red:** La solución proporciona esta solución para la contención de ataques en toda la red 1. Agregar archivo a la lista de bloqueo: el archivo es una pregunta que se puede agregar a una lista de bloqueo y se puede evitar que el ataque se propague lateralmente en la red. 2. Agregar archivo como excepción: para un archivo no malicioso, esta opción se puede usar para excluir actividades legítimas. **C. Investigar acciones:** La solución aprovecha los componentes internos y las soluciones de terceros para una mayor investigación. 1. Virustotal 2. Sandbox 3. Google **D. Conexión remota** 1. La solución puede conectarse remotamente al host para investigar rápidamente los ataques, recopilar datos forenses y remediar las infracciones. 2. Elimina la incertidumbre y reduce en gran medida cualquier tiempo de inactividad que resulte de un ataque. 3. Permite que un usuario / administrador autorizado acceda de forma segura a puntos finales administrados directamente desde la consola. 4. Después de conectarse con éxito al punto final remoto, se pueden ejecutar varios comandos de shell personalizados directamente en el sistema operativo para remediar la amenaza al instante o recopilar datos para una mayor investigación. Además de los casos de uso anteriores, el módulo EDR también proporciona visualización de los eventos de seguridad que están bloqueados por las capas preventivas. **E. Defensa contra ataques sin archivos:** Detecte y bloquee malware basado en scripts, sin archivos, ofuscado y personalizado, con reparación automática. **F. Capacidades de prevención avanzadas como** PowerShell Defense, Exploit Defense y detección de anomalías, bloqueo de ataques al principio de la cadena de ataque, antes de la ejecución
Protección en tiempo real	El análisis dLa solución en tiempo real debe evitar que entren en el sistema nuevas amenazas de malware, La solución debe analizar los archivos locales y de red cuando

	se acceda a ellos (al abrirlos, moverlos, copiarlos o ejecutarlos), al análisis de los sectores de arranque y al de las aplicaciones potencialmente no deseadas (APND).
Filtrado de correo electrónico malicioso.	El módulo de protección de correo electrónico dLa solución debe ofrecer protección multicapa contra las amenazas y phishing mediante una combinación de varios filtros y motores de análisis en la capa de protocolo (POP3 y SMPT) para determinar si los mensajes de correo electrónico son maliciosos.
Filtrado de Navegación	La solución que controla el Tráfico HTTP / FTP del Explorador de Windows debe Permitir o denegar el tráfico HTTP y FTP desde el Explorador de Windows. La solución debe tener la capacidad de crear reglas de cortafuego adicionales para otras aplicaciones instaladas en los puntos finales, esto debe crearlo además de las reglas predeterminadas por defecto.
Remote Troubleshooting	La solución deber permitir recopilar registros básicos y avanzados de forma remota. Con fin de facilitar a el análisis en profundidad del problema y proporcionar una resolución más rápida.
Protección Proactiva	La solución debe poseer tecnología de detección proactiva he innovadora que debe utilizar avanzados métodos heurísticos para que pueda detectar nuevas amenazas potenciales en tiempo real, debe monitorizar continuamente las aplicaciones que se están ejecutando en el punto final en busca de acciones indicativas de malware. Cada una de estas acciones debe puntuarse y calcular una puntuación global para cada proceso.
Consumo de recursos de Memoria del Endpoint	La solución debe utilizar menos de ~220 MB cuando se ejecute un análisis completo
Exclusión de archivos del análisis en tiempo real	La solución deberá contar con la opción para realizar exclusiones de archivos del análisis en tiempo real.
Control de acceso web	La suite de Seguirdad deberá contar con un control de acceso web, con categorías para definir qué sitios pueden ser accedidos o no dentro de la red. Limitar el acceso a los sitios Web por categoría y por grupo de usuarios para lograr una eficaz aplicación de las políticas corporativas cuyo objetivo es maximizar el cumplimiento de directivas de seguridad y la productividad de los empleados.
Análisis manual de búsqueda de códigos maliciosos.	La solución deberá contar con la opción de correr un análisis manual de búsqueda de códigos maliciosos. Ofrecer detección avanzada de malware furtivo mediante la exploración minuciosa del contenido de los protocolos seguros HTTPS y POP3S, así como de los archivos comprimidos.
ERM (Administración de Riesgos)	El módulo de gestión de riesgos de punto final (ERM) ayudara a identificar y remediar una gran cantidad de riesgos de red y sistemas operativos a nivel de punto final, mostrando el porcentaje de vulnerabilidad en la infraestructura. El puntaje de riesgo de la compañía se calcula teniendo en cuenta una amplia lista de indicadores de riesgos y vulnerabilidades de aplicaciones conocidas, mostrándole su evolución en el tiempo.

	Desglose de la puntuación y las principales configuraciones incorrectas y los widgets de aplicaciones vulnerables hacen que sea más fácil ver dónde su entorno es más vulnerable a los ataques y qué dispositivos son los más afectados. Este módulo deberá contar con al menos 300 indicadores de gestión de Hardening para la generación del nivel de riesgo
Human Risks Analytics	El módulo de gestión de riesgos debe incluir un analizador de riesgos humanos. El cual debe validar los siguientes aspectos: • Verificar si el usuario ha enviado credenciales a través de conexiones HTTP inseguras desde el último escaneo. • Verificar si el usuario ha navegado o no sitios marcados como phishing o fraude desde el último análisis. • Verificar si el usuario ha estado expuesto a una gran cantidad de amenazas desde el último análisis. • Verificar si el usuario ha estado expuesto a una amenaza de un dispositivo extraíble (por ejemplo, unidad flash, disco duro externo) desde el último escaneo. • Verificar si el usuario ha accedido a archivos maliciosos a través de una carpeta compartida de red desde el último análisis. • Verificar si el usuario ha accedido a alguna URL maliciosa desde el último análisis. • Verificar si el usuario no ha cambiado la contraseña de inicio de sesión de la cuenta (local o de dominio) durante más de 30 días. • Verificar si el usuario usa las mismas contraseñas en diferentes sitios externos. • Verificar si el usuario usa las mismas contraseñas compartidas entre sitios web internos y externos. • Verificar si el usuario no ha cambiado la contraseña de inicio de sesión para las cuentas HTTP (internas o externas) durante más de 30 días.
Defensa de ataques de RED	Tecnología enfocada en detectar técnicas de ataque a la red diseñadas para obtener Acceso a puntos finales específicos como: • Ataques de fuerza bruta • Ataques de red • Ladrones de contraseñas • Ataques Laterales.
Anti-Exploit Avanazdo	Anti-Exploit proporciona protección en ejecución contra intentos de explotación dirigidos a vulnerabilidades conocidas y desconocidas en aplicaciones de uso común y aplicaciones propias, como el navegador, Microsoft Office o Adobe Reader, así como contra intentos específicos de post-explotación en modo kernel.
Control de Dispositivos	Control de Dispositivos: permite prevenir las infecciones de fugas y malware datos sensibles a través de dispositivos externos conectados a extremos aplicando bloqueo normas y excepciones a través de la política a una amplia gama de tipos de dispositivos (tales como unidades Flash USB, dispositivos Bluetooth, reproductores de CD/DVD, dispositivos de almacenamiento, etc.).

	Que los bloqueos a dispositivos puedan realizarse por marca, modelo, número de serie o usuario.
Cifrado de Disco (Opcional)	La solución debe contar con la opción de adicionar como Add-on la protección de los datos de toda la unidad de disco duro del endpoint aprovechando los mecanismos de cifrado proporcionados por Windows (BitLocker) y Mac (FileVault). Se basa en el cifrado nativo de los dispositivos para garantizar la total compatibilidad y maximizar el rendimiento, sin la necesidad de instalar un agente adicional, ni un servidor de claves, gestionado todo de la misma consola de administración. Debe poseer opción para establecer reglas para excluir unidades del cifrado.
Administración Integrada De Parches (Opcional)	La solución debe contar con la posibilidad de adicionar como Add-on una herramienta de gestión y administración de parches de sistema operativo y aplicaciones permitiendo mantener actualizada toda su base instalada de Windows: estaciones de trabajo, servidores físicos y virtuales. Disponible en la versión elite de las soluciones y en soluciones on premise.
Exclusión de archivos	La solución deberá contar con la opción de realizar exclusiones de archivos del análisis del motor por demanda.
Análisis Programados	La solución y la consola de administración remota deberán permitir realizar análisis programados (en demanda) de los discos duros locales. Esta programación se podrá configurar en forma diaria, semanal, mensual.
Cortafuegos de escritorio	La solución deberá contar con un cortafuego de escritorio (Firewall Personal) que cuenta con un filtrado dinámico de paquetes que provea de monitoreo y filtrado de trafico de Red, y tenga total protección para IPv4 e IPv6 y con la opción de agregar reglas y servicios al cortafuego en forma autónoma y centralizada. Impedir el acceso no autorizado a la red corporativa. Ofrecer una fácil instalación, gran capacidad de personalización de reglas y un modo de aprendizaje inteligente para crear reglas de firewall automáticamente basándose en el tráfico de red observado. Combinar perfiles personalizados de firewall con zonas de redes de confianza. Debe poseer distintos modos del módulo de firewall entre los cuales debe tener uno que permita aprender la conducta del usuario generando las reglas permisivas automáticamente. Debe poseer opción para importar y exportar reglas. Esta solución no deberá provocar interrupciones con el Firewall de la Institución.
Actualización a través de repositorios de actualización de la	La consola de administración deberá permitir actualizar a través de repositorios de actualización a todas las estaciones protegidas con la posibilidad de tener redundancia de repositorios de actualización en forma automáticas (Fail-over).

solución de todas las estaciones protegidas	
La actualización de la base de datos de firmas de códigos maliciosos	Las actualizaciones de las bases de datos de firmas de códigos maliciosos de la solución antivirus deberán ser incrementales, evitando de esta manera la saturación del ancho de banda en su despliegue.
Opción de apagado luego de escaneo.	La herramienta antivirus debe permitir el apagado luego de la exploración o Repetición de las exploraciones programadas activadas por el administrador. Esto con el objetivo de ayudar a extender la vida útil del hardware y ahorrar energía y recursos
Programación y actualizaciones diferidas.	La herramienta antivirus debe contar con una selección opcional para la recepción de actualizaciones provenientes de servidores especiales con 12 horas de retraso para brindar tiempo a los administradores del sistema para evaluar el impacto en su red y asegurar una migración organizada.
Reportes	La consola de administración deberá contar con reportes gerenciales detallados con información de configuraciones, actualizaciones de los productos, alertas, estadísticas, etc., las cuales pueden ser exportadas a archivos csv y/o pdf. Deberá permitir generar reportes gráficos tipo barra, pastel, etc., para una vista rápida de la situación de la solución.
Alerta en consola y notificación vía correo electrónico y SNMP	La solución deberá permitir que las acciones de notificación incluyan correo electrónico, SNMP, y entradas de registro.
Compatibilidad con la estructura organizacional del Directorio Activo	La consola de administración web y on premise deberá permitir la detección de clientes no registrados sincronizando la estructura del grupo a través de Active Directory.
Análisis de aplicaciones y procesos	Debe permitir clasificar las aplicaciones en al menos 3 grupos según sus características y poder configurar el motor antivirus para que las analice o no. Debe otorgar una puntuación a los procesos en ejecución del sistema para medir su nivel de riesgo
Análisis de procesos	Deberá poseer una herramienta integrada para ver los procesos en ejecución, los servicios, las conexiones establecidas, claves de registro importantes, programas instalados, actualizaciones de sistema operativo instaladas, logs del equipo, drivers instalados, tareas programadas del sistema, archivo hosts, system.ini y win.ini. Análisis de causa raíz de las amenazas detectadas y bloqueadas por nuestras tecnologías preventivas, con opciones complejas de filtrado de incidentes y representación gráfica de incidentes, así como capacidades de aislamiento, lista de bloqueo y conexión remota.
Análisis de archivo comprimidos	La solución ofertada deberá detectar virus en archivos compactados, con profundidad máxima (16), en los siguientes formatos: .zip, .rar, .arj, .cab, .lzh, .tar, .gz, ace, izh, upx y otros

Gestión de Políticas	La consola de administración deberá definir y hacer cumplir consistentemente las políticas a lo largo de la red. El Administrador de Políticas facilitará la importación/exportación, para permitir la aplicación y combinación de las políticas de diversas maneras.
Gestión Multi-plataforma	La consola de administración deberá permitir administrar de forma remota desde una única consola todos los equipos de su red, ejecutando las versiones antivirus en clientes finales y servidores de las diferentes plataformas (Windows, Linux, Mac OS)
Certificaciones	**AV TEST**, haber obtenido el premio de la mejor solución por desempeño en los últimos 5 años. Para el segmento corporativo Enterprise. **Virus Bulletin** Que el fabricante haya detectado absolutamente todas las amenazas in the wild en las pruebas. El antivirus deberá tener aprobados los 5 últimos premios VB100 otorgados por la institución de análisis de software antivirus "Virus Bulletin". **Av- Comparatives** La solución antivirus deberá haber alcanzado al menos **25 certificación** AV-Comparatives ADVANCE+ en los últimos 3 años y al **menos haber obtenido el premio Producto del año en este periodo.** La solución deberá contar con certificaciones para trabajar en ambientes virtuales como VMWare y Citrix.
Servidor de Aplicaciones en Unidades Anexas	El oferente deberá asignar como mínimo a un técnico que acudirá a las oficinas del contratante para la instalación de la solución. El oferente se comprometerá a dejar listas las consolas de administración de la contratante con el total de usuarios respectivos conectados al servidor.
Actualización de versiones	El oferente será responsable de la actualización de la solución antivirus en los equipos y servidores de la contratante a la última versión estable liberada por el fabricante durante el tiempo que dure el licenciamiento.
Soporte Técnico	El oferente estará obligado a prestar el servicio de soporte y resolución de problemas o incidentes en los sitios de instalación de la solución antivirus cuando el problema lo amerite. El soporte técnico estará vigente durante el periodo de licenciamiento y deberá tener las siguientes características mínimas: • Disponibilidad los 365 días al año. • Atención inmediata vía telefónica, e-mail o asistencia remota para análisis de daños y posible solución. • Máximo 2 horas para atención presencial en el sitio del incidente cuando se lo requiera por parte de la contratante. • Debe contar un sistema de registro de incidentes mesa de ayuda. • El fabricante debe contar con soporte 24*7, sin costo adicional, ya sea por correo, chat on line y conexión remota

Capacitación	El oferente deberá capacitar a 4 (o más) funcionarios técnicos de la entidad contratante en el manejo de la solución antivirus y de las nuevas versiones que puedan generarse durante el tiempo que dure el licenciamiento. Deberá proveer de charlas y seminarios de concienciación sobre temas de seguridad de la información, las mismas que deberán ser impartidas por personal calificado y de preferencia por analistas y especialistas de malware directamente del fabricante. El oferente deberá contar con un responsable directo del fabricante, el mismo que deberá efectuar visitas periódicas para de esta manera poder informar sobre el seguimiento en la parte de atención al cliente en lo comercial y en lo técnico por parte del oferente.
Experiencia	• El oferente deberá contar con experiencia en la implementación de la solución en el sector público de mínimo 4 años. • Deberá adjuntar copias de contratos y actas de entrega/recepción de clientes con más de 800 o más licencias instaladas. • El oferente deberá ser calificado **por el fabricante** como Gold Partner para la distribución de la solución. • El oferente deberá contar con personal certificado y calificado para la prestación del soporte técnico durante el tiempo de licenciamiento (adjuntar certificados).
ESPECIFICACIONES GLOBALES DEL FABRICANTE	
	• El fabricante debe poseer más de 500 millones de usuarios a nivel mundial • El fabricante debe poseer un sistema de alerta temprano basado en cloud capaz de manejar más de 7 billones de interacciones al día • El Cloud deber tener la capacidad de bridar una respuesta máxima de 20ms • El Cloud debe estar equipado con más 1000 servidores virtuales, con capacidad de procesar más de 60 TB por mes, manejar más de 500K conexiones activas en cualquier momento • el Cloud debe permitir un número ilimitado de equipos administrados