ESPECIFICACIONES TÉCNICAS PARA EL LICENCIAMIENTO DE ANTIVIRUS PARA LA UNIVERSIDAD DE CUNDINAMARCA
DEL FABRICANTE
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.
El fabricante de las soluciones ofertadas debe contar con experiencia probada en el descubrimiento de vulnerabilidades desconocidas, APTs y malware avanzado y debe haber descubierto al menos dos (2) vulnerabilidades agregadas a la lista de Common Vulnerabilities and Exposures (CVE) durante el 2023.
La Solución debe estar evaluada por laboratorios independientes como AV-Test o AV-Comparatives que garantizan el correcto funcionamiento de la solución en la mayoría de los escenarios
El producto ofrecido debe contar con calificación Tripe A (AAA) en los resultados de SELABS de Enterprise Endpoint Protección del año 2023
El producto ofrecido debe contar con calificación Tripe A (AAA) en los resultados de SELABS de EDR del año 2023
El fabricante debe contar con respaldo de la Auditoria SOC2
ADMINISTRACIÓN
Administración y Monitoreo Centralizados.
Dashboard con información de estado del producto en los clientes.
Integración con directorio activo.
Manejo de consolas esclavas por jerarquía con mínimo 10 niveles de anidación.
Licenciamiento ilimitado de consolas y servidores de administración.
Manejo de grupos jerárquicos de usuarios.
Administración Basada en roles.
Capacidad de Administrar servidores y clientes Linux y clientes Mac a través de la consola de administración.
Administración centralizada del endpoint mediante políticas.
Calendarización de tareas tanto de análisis como de actualización.
Permitir detener o activar escaneo de virus PCs individuales, desde la consola.
Capacidad de recibir notificaciones sobre nuevas versiones de las aplicaciones corporativas del producto. Desde la misma consola de administración
Permitir sincronización de la estructura de Active Directory con la de los grupos de administración.
Permitir la asignación automática de los agentes de actualización (Repositorios en la red para evitar saturaciónes de los canales de comunicacion durante una tarea)
Permitir soporte de modo dinámico de Virtual Desktop Infrastructure (VDI).
Permitir establecer intervalos de tiempo para la transferencia de datos desde el Agente de Red al Servidor.
Bloqueo del endpoint con contraseña para evitar cambios no autorizados.
Permite envío automático de reportes a usuarios específicos de correo.
Reportes exportables mínimo a HTML, PDF y XLS.
Debe permitir la personalización de nuevos reportes.
Debe permitir el descibrimiento de nuevos dispositivos a través de direcciones IP, Grupos de trabajo o Directorio Activo
Debe poder cambiar automáticamente la configuración de los Endpoint al detectar un brote de virus en la red.
Análisis de conexiones cifradas.
Backup automático y calendarizado de configuraciones completas.
Notificaciones de grupos de estaciones a usuarios específicos de correo.
Capacidad para administrar más de 5.000 dispositivos sobre un mismo hardware
Capacidad de visualizar de manera consolidada los dispositivos gestionados, sus características técnicas, como sistema operativo y versión, Nombre de dispositivo y dirección IP, Tipo de procesador, Tipo de infección
La consola de administración debe permitir manejar múltiples políticas de seguridad, pudiendo activar una política específica ante epidemias de virus
Permitir crear políticas especiales para usuarios fuera del alcance de la consola
Controlar a través de políticas todos los componentes mencionados previamente (para estaciones de trabajo y servidores), sin necesidad de consolas adicionales de administración
Delegación de tareas mediante la creación de usuarios con distintos perfiles de administración
Permitir la realización de Backup de las configuraciones realizadas en el sistema.
Comunicación Cifrada o SSL entre servidores y clientes, a través de certificados digitales propios o de terceros
La consola debe permitir la creación de usuarios y perfiles específicos para ejecutar tareas de control o auditoría específicas por parte del personal de Infraestructura y Riesgo Tecnológico, sin que esto afecte las tareas realizadas por el Administrador de la consola.
Distribución de agentes, configuraciones y actualizaciones de forma centralizada
Facilidad para accesar a la consola desde cualquier sitio en la red
Monitoreo permanente y generación reportes de eventos en tiempo real
Permite desde sitio central la distribución masiva del agente
Facilidad en la actualización del agente para usuarios fuera de la red
Establecer políticas por grupos de trabajo y estructuras de herencia
Desactivar y desinstalar el agente de manera segura y remota.
Consola MMC, Web
El Servidor de Administración debe disponer de Compatibilidad con Clúster.
Compatibilidad para administrar hasta 100,000 dispositivos por un único Servidor de administración.
Capacidad de hacer distribución remota y programada de las aplicaciones de protección ofertadas de acuerdo con parámetros definidos por el administrador, para que sea instalado en las máquinas clientes
Base de datos SQL o My SQL o MarianaDB
Debe permitir realizar instalaciones de la soluciones de gestion y proteccion de forma Remota
Debe permitir desinstalar otros productos antivirus remotamente
Debe proteger los archivos de instalación a fin de evitar que se corrompan durante la instalación en un equipo infectado
Detección mínima de falsos positivos o falsos virus.
La solución debe disponer de una interfaz de gestión centralizada que permita la instalación, configuración, actualización y administración de todas las soluciones ofertadas de manera integral, unificando la gestión de la seguridad.
El producto debe estar en capacidad de descargar actualizaciones optimizadas en lugar de actualizaciones completas implementadas.
El producto debe estar en capacidad de enviar eventos a sistemas SIEM
Capacidad de elegir cualquier computadora cliente como repositorio de vacunas y de paquetes de instalación, sin que sea necesario la instalación de un servidor administrativo completo, donde otras máquinas clientes se actualizarán y recibirán paquetes de instalación, con el fin de optimizar el tráfico de red;
Capacidad de hacer de este repositorio de actualizaciones desde un Gateway para conexión con el servidor de administración, para que otras máquinas que no logran conectarse directamente al servidor puedan usar este Gateway y así recibir y enviar información al servidor administrativo.
OTRAS CARACTERISTICAS DE GESTION

Inventario básico de software.
Debe poder desactivar el arranque automático de dispositivos extraíbles.
Monitoreo de paquetes enviados por la red.
Compatibilidad certificada con plataforma de virtualización VMware y Xen.
Registrar los eventos asociados con la eliminación y el guardado de archivos en dispositivos USB.
Controlar las descargas de los módulos y controladores DLL
Capacidad de instalar otros servidores administrativos para balancear la carga y optimizar el tráfico de enlaces entre sitios diferentes;
Capacidad de conectar máquinas vía Wake on Lan (siempre y cuando este disponible) para iniciar tareas programadas (análisis de archivos en busca de malware, actualización, instalación, etc.), incluso de máquinas que estén en subredes diferentes del servidor);
Que sea optimizado para servidores de multiprocesadores basados en la tecnología Intel Xeon.
COMPATIBILIDAD
Compatibilidad con Sistemas Operativos Windows 32 y 64 bits
Windows 7 sp1 y posteriores
Windows Server 2003 y posteriores
Compatibilidad con Sistemas Operativos Linux 32 y 64 bits
Ubuntu 20.04 LTS o posterior, Ubuntu 20.04 LTS o posterior,
Red Hat Enterprise Linux 6.7 o posterior, Red Hat Enterprise Linux 7.2 o Posterior, Red Hat Enterprise Linux 8.0 o posterior
CentOS 9.0 y posterior,
Oracle Linux 7.3 y posterior, Oracle Linux 8 y posterior,
SUSE Linux Enterprise Server 12 SP3 y posterior, SUSE Linux Enterprise Server 15 y posterior
Linux ALT
Amazon Linux 2
Linux Mint 18.2, Linux Mint 19
Astra Linux
OS ROSA Cobalt
GosLinux
AlterOS
Pardus OS
RED OS 7.2
Compatibilidad con Sistemas Operativos Mac
macOS 12 - 14
PROTECCIÓN BASICA
Protección contra virus, programas troyanos y gusanos.
Protección contra programas espía y publicitarios.
Análisis de ficheros en modo automático o según horario, debe facilitar recursos para otras aplicaciones durante el análisis.
Capacidad de verificar correos electrónicos recibidos y enviados en los protocolos POP3, IMAP, NNTP, SMTP y MAPI, así como conexiones cifradas (SSL) para POP3 y IMAP (SSL);
Análisis y control de archivos adjuntos por extensión en correo electrónico.
Permitir configurar un salto en el análisis de archivos grandes en correo electrónico según el tamaño que pueda definir el administrador.
Permitir configurar un salto en el análisis de archivos en correo electrónico cuyo análisis tome más de un tiempo determinado según defina el administrador.
Permitir configurar un salto en el análisis de archivos adjuntos en correo electrónico.
Análisis de virus de Internet (para cualquier navegador de Internet).
Permitir la configuración de acciones automáticas ante eventos de posible infección de malware por Internet.
Análisis de tráfico de Internet mínimo para los protocolos: HTTP y FTP.
Análisis y desinfección automática el contenido de los dispositivos de memoria
Que permita acceder a la base de datos del fabricante para revisar reputación de archivos, recursos web, y software
Permitir la creación de URL´s de confianza.
Protección contra acceso de Phishing en los dispositivos
Análisis y defensa para mensajeros instantáneos.
Permitir análisis heurístico de mensajes enviados y recibidos por los servicios de mensajería instantánea.
Rapidez de Escaneo mediante el uso de tecnologías iChecker e iSwift.
Actualizaciones automática de firmas mínimo cada 1 (UNA) hora.
Chequeo y desinfección de malware contenido en archivos comprimidos.
Cuarentena para archivos infectados.
Chequeo y desinfección de malware contenido en memoria.
Chequeo y desinfección de malware contenido en el sector de arranque.
Detección y desinfección en tiempo real de virus residentes.
Reconocimiento de virus por su forma de empaquetamiento.
Defensa proactiva contra los nuevos programas maliciosos (Día Cero).
FIREWALL PERSONAL
Firewall debe permitir crear reglas para filtrado de aplicaciones.
Firewall debe permitir crear reglas para filtrado de paquetes.
Firewall debe permitir configurar las diferentes redes como: local, público o de confianza.
Debe tener un módulo de protección contra ataques de red.
Debe permitir crear excepciones en el módulo de protección contra ataques de red.
PROTECCIÓN AVANZADA
Métodos de detección basados en: Firmas, Heurística, análisis en la Nube de seguridad del proveedor, aprendizaje automático, prevención de vulnerabilidades, detección de comportamiento y motor de reparación.
La solución deberá contar con tecnologías de detección proactiva de amenazas basadas en la nube del mismo fabricante.
Debe ser compatible con el subsistema de Windows para Linux (WSL)
El producto debe contar con un Control de Anomalías Adaptativo, bloqueando acciones atípicas del equipo.
La protección debe incluir como categorías del control de navegación, los sitios web de "criptomonedas y minería".
Capacidad de verificación del cuerpo del correo electrónico y adjuntos usando heurística;
Que permita acceder a la base de datos del fabricante para revisar reputación de archivos, recursos web, y software
CONTROL DE APLICACIONES
Permitir a usuarios seleccionados y / o grupos de usuarios iniciar aplicaciones.
Bloqueo de usuarios seleccionados y / o grupos de usuarios para el uso de las aplicaciones de inicio.
Control de privilegios de aplicaciones que controle la actividad de las mismas para el uso de recursos informáticos
Brindar la posibilidad de monitorear y controlar las aplicaciones, permitir y denegar el acceso a determinadas llaves del registro, archivos y carpetas.

Poder definir cuales aplicaciones están permitidas para ejecutarse, cuales aplicaciones pueden hacer llamados a Dynamic Link Libraries(DLL).
Brindar visibilidad de las aplicaciones que el usuario ha instalado en los equipos
Flexibilidad para aplicar políticas de control por grupos de usuarios, para permitir o bloquear aplicaciones en particular.
Poder manejar el inventario de aplicaciones agrupado ya sea por todos los archivos binarios (.exe,.dll, controladores y secuencias de comandos), por aplicación y fabricante.
Brindar la posibilidad de clasificar por categorías las aplicaciones por ejemplo: fiables conocidas, desconocidas y maliciosas conocidas.
Capacidad de agregar software a una lista de "aplicaciones confiables", donde las actividades de red, actividades de disco y acceso al registro de Windows no serán monitoreadas;
Poder crear listas blancas y listas negras para especificar qué aplicaciones se pueden ejecutar y cuáles no.
CONTROL DE DISPOSITIVOS
Control por tipo de dispositivo a ser conectado
Permitir a los usuarios seleccionados y / o grupos de usuarios acceder a determinados tipos de dispositivos durante períodos específicos de tiempo.
Permitir a los usuarios seleccionados y / o grupos de usuarios ver el árbol de carpetas en dispositivos de memoria.
Permitir a los usuarios seleccionados y / o grupos de usuarios leer el contenido de los dispositivos de memoria.
Permitir a los usuarios seleccionados y / o grupos de usuarios modificar el contenido de los dispositivos de memoria.
Permitir la creación de dispositivos de confianza a los cuales los usuarios tienen acceso total en todo momento.
CONTROL DE NAVEGACIÓN
Control de acceso web para usuarios y / o grupos de usuarios.
Control de acceso web mediante filtro por categoría.
Control de acceso web mediante filtro por tipos de archivos.
Control de acceso web mediante filtro por categoría y tipos de archivos.
Control de acceso web mediante filtro por direcciones URL.
Control de acceso web mediante reglas para determinados nombres de usuarios y / o grupos de usuarios.
Permitir configurar las reglas de control de acceso web mediante horario.
Permitir dar prioridad a cualquiera de las reglas de control de acceso web creadas.
Permitir configurar las reglas de control de acceso web para: permitir, bloquear o alertar el acceso a los diferentes sitios.
Control de acceso web debe tener un diagnóstico de reglas.
CONTROL DE ADAPTATIVO DE ANOMALIAS
Debe estar en capacidad de detectar y bloquear acciones que no son típicas de los equipos conectados a una red corporativa
Debe utilizar una serie de reglas, que buscan comportamientos que no se consideran usuales (por ejemplo, el Inicio de Microsoft PowerShell desde una aplicación de ofimática)
Debe contar con un modulo de Aprendizaje inteligente
Se podrán modificar las notificaciones o desactivarlas
Las acciones que se podrán configurar como mínimo deben ser Inteligente, Bloquear y notificar
BORRADO REMOTO
Debe tener un componente en el Endpoint que permita la eliminación de datos de los dispositivos de forma remota basado en reglas de cumplimiento
Los métodos de eliminación deben ser como mínimo inmediato o programado
Debe ser de forma silenciosa, sin interacción por parte del usuario
El alcance debe permitir realizar borrado remoto en los discos duros y en unidades extraíbles
Debe incluir opciones de borrado permanente sin la posibilidad de recuperar o borrado a través del comportamiento del sistema operativos
Se podrá seleccionar rutas en el disco, carpetas predefinidas, archivos o extensiones
CIFRADO
Cifrado de dispositivos extraíbles o removibles
Cifrado de disco duro (full disk encryption: master boot record, OS, system files)
Cifrado a través de BitLocker de MS
Cifrado a través de Filevault de OSX
Cifrado de archivos y carpetas Seleccionadas
Cifrado de dispositivos extraíbles (USB)
Administración centralizada de políticas y llaves
Protección de acceso (Autenticación y Autorización) – Preboot-Authentication
Opciones de recovery de datos (posibilidad dde recuperar contraseñas extraviadas, creación de usuarios generales)
Cifrado de Tipos de archivos para aplicaciones (y descifrado)
El cifrado debe permitir realizar SSO (inicio de sesión único con credenciales de Active Directory)
ADMINISTRACIÓN DE SISTEMAS
Capacidad de realizar instalación remota y flexible de software con despliegues programados o manuales
Envio de mensajes a usuarios
Capacidad de creación, almacenaje, clonado y despliegue de imágenes del sistema desde un lugar central
Capacidad de realizar instalación remota y flexible de software de terceros con despliegues programados o manuales
Poder brindar soporte remoto desde la consola en modalidad de escritorio compartido
Capacidad de sincronizar datos de manera regular con actualizaciones disponibles y hotfixes de servidores, para posteriormente distribuirlos
Capacidad de poder llevar un control de licenciamiento global de aplicaciones (ej winzip, adobe, ect)
GESTIÓN DE VULNERABILIDADES
Generación de informes de amenazas de vulnerabilidad en las aplicaciones, con puntuaciones o niveles de severidad que ayudan a adoptar decisiones para protección de las estaciones.
Desplegar a través de la solución, los parches o actualizaciones que remedien las vulnerabilidades detectadas.
Posibilidad de definir parcheo automático para grupos de aplicaciones de Microsoft
Posibilidad de definir parcheo automático para grupos de aplicaciones de aplicaciones comerciales (ej Chrome, firefox, java, etc)
Posibilidad de definir grupos de prueba para verificar efectividad de parches.
Mostrar las actualizaciones por instalar e instaladas así como también las vulnerabilidades detectadas en los equipos.
Soporte para servicios de actualización de Servidores Microsoft Windows (WSUS)
ADMINISTRACIÓN DE DISPOSITIVOS MOVILES
Soportar SO: IOS – Android – para Smartphone y Tablet.
Integración y compatibilidad con Microsoft Exchange ActiveSync
Debe permitir la definición de auditorías para los cambios de configuración y/o reglas que se realicen
La solución deberá tener un módulo de administración de usuarios que permita gestionar perfiles tales como: Administradores, auditores, revisores, de acuerdo a un nivel de privilegios y roles establecidos por el grupo empresarial.
Distribuir y restringir el uso de recursos/App's
Funcionalidad de una consola de administración y monitoreo sobre los dispositivos
Identificar dispositivos inactivos
Capacidad de aplicar políticas corporativas de seguridad en todos los dispositivos

Código de acceso obligatorio – Políticas de Contraseñas
Administrar características de contraseñas
Borrado de información del dispositivo en caso de robo
Monitorear, detectar y notificar cuando una política haya sido modificada sobre el dispositivo Móvil
Mantener inventario del dispositivo.
Permitir la generación de informes.
PROTECCION PARA MS OFFICE 365
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 no debe requerir cambio alguno en los registros MX de correo o en las aplicaciones de Microsoft Office 365 para su funcionamiento.
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.
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 solucion debe de disponer una visibilidad unificada de las amenazas detectadas por los sevicios de seguridad base de Microsoft Exchange Online mediante la visualizacion de una cuarentena unica.
Debe contar con cuadros de mandos, KPIs y reportes de seguimientos de las detecciones realizadas.
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.
La protección de anti-malware para Microsoft OneDrive debe permitir la exclusión y selección de usuarios protegidos.
Debe contar con protección frente a virus, troyanos y otras clases de malware para MS Teams.
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.
Debe contar con protección basada en firmas mediante aprendizaje automático junto con análisis conductuales y heurísticos avanzados.
Debe usar una combinación de SPF (marco de directivas de remitente), DKIM (DomainKeys Identified Mail), validación de correo electrónico de DMARC (Autenticación de mensajes, informes y conformidad basada en dominios) y el método de detección de similitudes para detectar y prevenir spoofing y phishing de correos electrónicos, ataques BEC y spam.
Debe proveer heurística mediante redes neurales de aprendizaje profundo.
Debe incluir protección contra ataques de inyección de código y mailsploit/spoofing que son posibles debido a los errores de los clientes de correo.
Debe contar con mecanismo de detección de spam al nivel de la dirección IP.
Debe poder rastrear el intercambio de datos confidenciales de texto o imágenes que se almacenan y transmiten dentro y fuera de su organización, por lo que puede considerar acciones para impedir posibles fugas.
PLATAFORMA DE ENTRENAMIENTO
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.
La solución propuesta debe ser 100% en nube
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
PROTECCION PARA SERVIDORES FISCOS Y VIRTUALES
Compatibilidad con herramientas de administración jerárquica del almacenamiento (HSM Systems).
Debe contar con modulos Anti-Cryptor
Debe ejecutar controles sobre las aplicaciones que se ejecutar con el fin de evitar el inicio de aplicaciones no autorizadas
Debe permitir definir listas blancas para deispositivos externos que se conecten a los servidores protegidos
Debe permitir la gestion del firewall del SO desde las politicas de seguridad definidas de manera centralizada
brinda la capacidad de proteger la memoria del proceso contra vulnerabilidades
Proteccion para archivos y sistemas NTFS
Capacidad de auto proteger los procesos para evitar alteraccion y corrupcion en la solucion antimalware
Debe permitir el envio de eventos a SIEM desde el mismo Endpoint
DETECTION AND RESPONSE (EDR)

La solucion debe contar con un sensor incluido que se integre al Endpoint para validar el comportamiento de las aplicaciones
debe ser acapaz de realizar Análisis de raíz de la causa, en por lo menos tres niveles de profundidad
debe ser capaz de realizar Escaneo de indicadores de compromiso (IoC), importarlos y validarlos en servidores publicos para visualizar el impacto y las referencias de los indicadores
Acciones de respuesta automáticas y configurables
Debe realizar Aislamiento de los dispositivos con tiempo programados,
Debe realizar escaneos del host
Debe impedir que procesos seleccionados se ejecuten en los dispositivos protegidos
Debe ser capaz de realizar Aislamiento del Endpoint en caso de malware o comportamietos sopechosos que puedan desencadenar un brote de malware
Debe ser administrado desde la misma consola del Endpoint
Compatibilidad con estaciones de trabajo Windows y servidores Windows
Debe tener la capacidad de establecer conexion remota por RDP y escritorio remoto compartido a los dispositivos incluso cuando estos se encuentran ailados por el componente de EDR
Descubra las conexiones de la amenaza y su historial con la visualización de ruta de propagación de ataques.
REQUERIMIENTOS ADICIONALES
El Oferente debe ser Partner Platinum Especialista en Hybrid Cloud Security, con el fin de que garantice conocimiento certificado al momento de que se escalen incidentes o requerimientos
Debe contar con un sistema de mesa de ayuda con registros de tickets
Debe contar con un sistema de mesa de ayuda en línea, que le permita al cliente interactuar con la herramienta para dar seguimiento de tickes y cumplimientos de SLAs
SERVICIOS
El contratista deberá hacer una presentación de las nuevas funcionalidades que el fabricante libere en la versión actualizada con el fin de que, si la Entidad lo requiere, se adopten y entren en operación. Estas implementaciones las realizará el contratista con el acompañamiento de los ingenieros del área de servicios tecnologicos que serán los administradores del software.
El servicio de mantenimiento preventivo se realizará mensualmente y será programado por la entidad en un cronograma específico. El servicio de mantenimiento correctivo será solicitado por la entidad cuando se requiera.
Soporte presencial, remoto y telefónico, 5x8x12 (es decir, cinco (5) días a la semana, ocho (8) horas al día por doce (12) meses), de lo cual debe allegar un informe escrito de cada actividad realizada.
Los mantenimientos se programarán con el supervisor del contrato en un horario que no afecte la operación normal del servicio de la Insitutución, garantizando el correcto funcionamiento y operatividad de los productos y de la plataforma informática de la Universidad de Cundinamarca.
CAPACITACION
El oferente deberá diseñar un Plan de Capacitación para la administración de las soluciones objeto del presente proceso, ofrecido a mínimo seis (06) Ingenieros del Área de Servicios Tecnologicos adscrita a la Dirección de Sistemas y Tecnología de la Universidad de Cundinamarca que incluya el uso y administración del software, antivirus, control de dispositivos, Control de Aplicaciones, Cifrado, Antispam, las actualizaciones, funcionalidades de los productos adquiridos en el presente contrato. La intensidad horaria no debe ser inferior a 20 horas. Todos los costos para esta transferencia de conocimientos estarán a cargo del proponente
DOCUMENTACION
Se debe entregar totalmente documentada la metodología de implementación y configuración de la herramienta ofertada siguiendo las recomendaciones de mejores prácticas de la casa matriz.
El oferente deberá disponer de un sitio web de base de conocimiento en el cual se pueda realizar consulta de la documentación de la solución implementada, a su vez la metodología de implementación y configuración de la herramienta ofertada siguiendo las recomendaciones de mejores prácticas de la casa matriz.

ESPECIFICACIONES TÉCNICAS PARA EL LICENCIAMIENTO DE ANTIVIRUS PARA LA UNIVERSIDAD DE CUNDINAMARCA
La solución debe contar con tecnologías proactivas para la detección de amenazas avanzadas o de día 0, incluyendo malware, ransomware, exploits y ataques web.
Debe ofrecer protección en tiempo real contra ataques conocidos y desconocidos.
Debe incluir capacidades de análisis heurístico y de comportamiento para identificar y bloquear nuevas amenazas.
La solución debe contar con un firewall integrado para proteger las máquinas virtuales contra ataques no autorizados.
Debe permitir la definición de reglas de firewall granulares para controlar el tráfico de red entrante y saliente.
Debe incluir mecanismos de prevención de intrusiones (IPS) para detectar y bloquear intentos de intrusión en tiempo real.
La solución debe permitir el control granular de las aplicaciones que se pueden ejecutar en las máquinas virtuales.
Debe permitir la definición de listas blancas y negras de aplicaciones.
Debe incluir la capacidad de bloquear la ejecución de aplicaciones no autorizadas.
La solución debe ofrecer una consola de administración centralizada para gestionar la seguridad de todas las máquinas virtuales desde una única ubicación.
La consola debe permitir la visualización del estado de seguridad de las máquinas virtuales, la configuración de las políticas de seguridad y la gestión de las licencias.
Debe ser posible acceder a la consola de administración de forma remota a través de un navegador web.
La solución debe ser escalable para adaptarse a entornos de nube privada de cualquier tamaño, desde pequeñas implementaciones hasta grandes infraestructuras.
Debe permitir la gestión de miles de máquinas virtuales desde una única consola de administración.
Debe ofrecer un rendimiento óptimo sin afectar al rendimiento de las máquinas virtuales.
Compatibilidad con sistemas operativos: Microsoft Windows Server 2012 R2 Standard o superior Red Hat Enterprise Linux (RHEL) 6.6 o superior SUSE Linux Enterprise Server (SLES) 12 SP1 o superior
El servidor de administración debe tener conectividad de red a los agentes de protección que se instalarán en las máquinas virtuales.

ESPECIFICACIONES TÉCNICAS PARA EL LICENCIAMIENTO DE PROTECCION DE APLICACIONES PARA LA UNIVERSIDAD DE CUNDINAMARCA
INFORMACIÓN 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.
El fabricante de las soluciones ofertadas debe contar con experiencia probada en el descubrimiento de vulnerabilidades desconocidas, APTs y malware avanzado y debe haber descubierto al menos dos (2) vulnerabilidades agregadas a la lista de Common Vulnerabilities and Exposures (CVE) durante el 2023.
CARACTERÍSTICAS GENERALES
Debe ser una solución de seguridad del lado del servidor que proporcione protección antivirus, análisis del tráfico HTTP y comprobación de la reputación de archivos y URL para soluciones de terceros implementadas en la Organización.
La solución debe ofrecer una protección completa para una amplia gama de dispositivos contra malware, troyanos, gusanos, rootkits, spyware y adware.
La solución debe poder utilizarse con diversos productos y servicios, como aplicaciones de escritorio, soluciones de servidor, servidores proxy y gateways de correo, entre otras.
El Motor de Análisis debe poder funcionar en estos dos modos: - Modo HTTP - Modo ICAP
Cuando la solucion funcione en Modo HTTP el Motor de Análisis debe funcionar como un servicio tipo REST que recibe solicitudes HTTP de aplicaciones cliente, analiza los objetos pasados en estas solicitudes y devuelve respuestas HTTP con los resultados del análisis.
Cuando la solución funcione en Modo ICAP el Motor de Análisis debe funcionar como un servidor ICAP que analiza el tráfico HTTP que pasa a través de un servidor proxy, por ejemplo, y las URL que solicitan los usuarios, y filtra las páginas Web que contienen contenido malicioso.
La solución debe incuir una interfaz gráfica de usuario, basada en web, que le permita configurar fácilmente el comportamiento del Motor de Análisis, revisar sus eventos de servicio y resultados de escaneo.
La interfaz gráfica debe proporcionar un panel con información sobre todos los objetos escaneados, los cuales deben poderse exportar en formato CSV.
La interfaz gráfica debe permitir enviar eventos de la aplicación a Syslog en formato CEF.
Todos los eventos de servicio son visibles en el panel de control de la interfaz gráfica de usuario.
La solución debe permitir actualizaciones de las bases de datos antivirus de forma automática.
La solución debe permitir restaurar automáticamente las bases de datos dañadas.
La solución debe proporcionar una arquitectura resistente y tolerante a fallos.
La solución debe incluir código fuente para el cliente HTTP y el servicio ICAP el cual debe ser proporcionado en un kit de distribución para su personalización.
La solución debe incluir documentación completa y compatibilidad con API multiplataforma. API similares para las versiones Linux/UNIX y Windows.
El Motor de Análisis debe soportar una arquitectura de cluster. Esta característica le permita administrar centralizadamente las instancias, ver los resultados de análisis con estadísticas para cada instancia en clúster, ver información sobre el estado del Motor de Análisis para cada instancia agrupada.
La solución debe cumplir con el Reglamento General de Protección de Datos (GDPR).
REQUISITOS DEL SISTEMA
La solución debe funcionar en sistemas operativos Linux de 64 bits y Microsoft Windows de 64 bits.
El sistema debe permitir la instalación en un servidor físico o virtual
CARACTERÍSTICAS DE PROTECCIÓN
La solución debe proporcionar protección contra amenazas con el fin de poder analizar archivos y bloques de memoria RAM utilizando la base de datos antivirus y el módulo de heurística avanzada.
La solución debe ser compatible con el análisis de ejecutables comprimidos, archivos, macros de Microsoft Office, mensajes de correo electrónico y bases de datos de correo electrónico.
La solución debe proporcionar características de filtrado Web que permitan analizar URLs específicas (en modo HTTP) o URLs que los usuarios solicitan desde un servidor proxy (en modo ICAP).
La solución debe proporcionar tecnologías para la comprobación de reputación de archivos y URL.
La solución debe permitir la detección de malware y poder reaccionar instantáneamente ante las amenazas emergentes.
La solución debe proporcionar información sobre la reputación de los archivos y los recursos de Internet, garantizando que las aplicaciones reaccionen a las amenazas más rápidamente sin esperar a que se actualice la base de datos de aplicaciones y reduciendo la probabilidad de falsos positivos.
La solución debe filtrar las URL maliciosas, de phishing y de adware.
La solución debe realizar detección de objetos multiempaquetados y objetos empaquetados mediante utilidades de compresión "grises" (utilizadas frecuentemente para ocultar programas maliciosos del software antivirus).
La solución debe incluir un analizador heurístico avanzado y tecnologías de detección basadas en aprendizaje automático.
La solución debe poder realizar la desinfección de archivos infectados, archivos comprimidos y objetos codificados.
La solución debe incluir un motor antivirus actualizable. es decir que las tecnologías de detección y la lógica de procesamiento deben poder actualizarse o modificarse mediante actualizaciones periódicas de la base de datos antivirus.
La solución debe soportar de forma nativa multithreading y debe poder procesar varias tareas simultáneamente.
La solución debe permitir ajustar el número de procesos e hilos de escaneo para aumentar el rendimiento del Motor de Análisis.
La solución debe incluir un componente para reconocer y omitir determinados formatos de archivo durante el proceso de análisis, admitiendo docenas de formatos, incluidos archivos ejecutables, de documentos, multimedia y archivos comprimidos.
Análisis de firmas
La solución debe pernitir realizar analisis de firmas basado en la búsqueda de una cadena predefinida en los archivos escaneados. El análisis de firmas también debe incluir la detección basada en el hash de todo el archivo malicioso. Las firmas tradicionales permiten detectar objetos específicos con gran precisión. Otras tecnologías basadas en firmas, como las firmas heurísticas de estructura y SmartHash, pueden detectar malware desconocido y polimórfico.
La solución debe pernitir, dentro del analisis de firmas, detectar objetos específicos con gran precisión, incluyendo otras tecnologías basadas en firmas, como las firmas heurísticas de estructura y SmartHash, que permitan detectar malware desconocido y polimórfico.
El análisis de firmas debe poder detectar ataques específicos con gran precisión y pocos falsos positivos.
La solución debe tener una base de datos de antivirus que se actualice con frecuencia y garantice el máximo nivel de protección frente a malware, troyanos, gusanos, rootkits, spyware y adware conocidos.

La solución debe incluir heurística avanzada que permita analizar un script o un archivo ejecutable, emulando su ejecución en un entorno artificial seguro. Si se descubre una actividad sospechosa durante el análisis del comportamiento del objeto emulado, se debe considerar malicioso. Este método debe ayudar a detectar malware nuevo y desconocido.
La solución debe permitir construir hashes inteligentes que permitan identificar grupos de archivos similares y detectar eficazmente malware desconocido de familias de malware conocidas, empleando varios niveles de precisión en la detección de malware muy polimórfico.
Los hashes inteligentes deben funcionar de forma offline y online.
La solución debe incluir el uso de técnicas de aprendizaje automático para aumentar la tasa de detección de las tecnologías de análisis existentes
La solución debe proporcionar las siguientes acciones con los objetos maliciosos: - Desinfectar o eliminar - Desinfectar u omitir - Borrar - Omitir
La solución debe proporcionar la comprobación de la suplantación de identidad y la URL maliciosa
La solución debe proporcionar la comprobación de los archivos con la coincidencia de la reputación en el servicio de reputación de la nube
La solución debe desinfectar o eliminar los objetos infectados dentro de los ejecutables o archivos comprimidos, según la configuración definida por el usuario (archivos ARJ, CAB, RAR y ZIP)
La solución debe tener la posibilidad de especificar los formatos de los objetos a escanear
La solución debe tener la posibilidad de obtener estadísticas sobre los objetos escaneados
MODO HTTP
La solución debe funcionar como un servicio de tipo REST que recibe peticiones HTTP de aplicaciones cliente, escanea los objetos pasados en estas peticiones y devuelve las respuestas HTTP con los resultados del escaneo.
La solución debe soportar dos versiones del Protocolo de solicitud: - Texto simple - JSON
La solución debe estar en capacidad de escanear objetos contenidos en el cuerpo de una petición http del cliente
La solución debe estar en capacidad de escanear objetos que se encuentran en el host con la solución
La solución debe permitir escanear objetos que se encuentran en el host con la solución
La solución debe permitir configurar la ruta completa del directorio desde el que se realizará el escaneo de objetos en la configuración de la solución
La solución debe permitir comprobar la reputación de las URL
La solución debe permitir especificar reglas para filtrar por tamaño de objeto
La solución debe tener la capacidad para trabajar en un entorno de alta carga y especificar la configuración para: - el número de procesos de escaneo e hilos de escaneo - la longitud de la cola de escaneo - el número máximo de conexiones TCP activas a la solución
La solución estar en capacidad de trabajar a través del protocolo TLS cuando se ejecuta en modo de servicio tipo REST
MODO DE INTEGRACIÓN ICAP
La solución debe funcionar como un servidor ICAP que escanea el tráfico HTTP que pasa a través de un servidor proxy y las URLs que son solicitadas por los usuarios y filtra las páginas web que contienen contenido malicioso
La solución debe permitir comprobación de solicitudes y respuestas
La solución debe permitir especificar lo que el producto debe escanear en cada uno de los tipos de consulta: - El cuerpo de la solicitud/respuesta - La URL a la que se dirige la solicitud - Analizar todo
La solución debe permitir especificar reglas de filtrado: - Por el tamaño del objeto en el cuerpo de la solicitud/respuesta - Por el tipo de objeto en el cuerpo de la solicitud/respuesta - Por la URL contenida en los campos Host y URL
La solución debe tener la posibilidad de especificar máscaras de URL para el filtrado web
La solución debe tener la capacidad de comenzar a transmitir el objeto escaneado antes de que se complete su escaneo.
La solución debe tener la capacidad de especificar las plantillas HTML que ICAP debe enviar dependiendo del resultado del escaneo
La solución debe tener la capacidad de especificar los scripts que ICAP debe ejecutar dependiendo del resultado del escaneo
La solución debe tener la capacidad para trabajar en un entorno de alta carga y especificar la configuración para el número de procesos de escaneo e hilos de escaneo
ADMINISTRACIÓN Y REPORTES
La solución debe tener la capacidad para gestionar el producto mediante: - Interfaz web - Archivos de configuración - Scripts de gestión de productos
La solución debe proporcionar la capacidad de utilizar la interfaz gráfica de usuario (GUI) para la gestión y la supervisión que: - Permite configurar los ajustes de la aplicación y gestionarla. - Le permite supervisar el estado de funcionamiento de la aplicación, el estado del archivo clave o del código de activación utilizado y el número de objetos escaneados y detectados. -Proporciona información sobre todos los objetos escaneados en un panel de control. - Ofrece la posibilidad de exportar la información en formato CSV.
La solución debe permitir tolerancia a los fallos mediante un módulo que supervise la presencia y el cuelgue de los procesos en el Sistema
La solución debe tener la capacidad de realizar copias de seguridad de las bases de datos antivirus