ESPECIFICACIONES TÉCNICAS PARA EL LICENCIAMIENTO DE ANTIVIRUS PARA LA UNIVERSIDAD DE CUNDINAMARCA
DEL FABRICANTE
La herramienta de seguridad debe tener certificación ISO 9001.
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 o CLOUD
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 y posteriores
Windows Server 2003 y posteriores
Compatibilidad con Sistemas Operativos Linux 32 y 64 bits
Ubuntu 16.04 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 6.7 y posterior, CentOS 7.2 y posterior, CentOS 8.0 y posterior,
Oracle Linux 6.7 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 10.13, 10.14, 10.15, 11.7 or 12.6
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 politicas corporativas de seguridad en todos los dispositivos
Código de acceso obligatorio – Politicas de Contraseñas
Administrar características de contraseñas
Borrado de información del dispositivo en caso de robo
Monitorear, detectar y notificar cuando una politica haya sido modificada sobre el dispositivo Móvil
Mantener inventario del dispositivo.
Permitir la generación de informes.
PROTECCION PARA SERVIDORES
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, en una herramienta certificada en procesos ITIL (presentar certificación emitida por fabricante no mayor a 30 días de uso de plataforma de mesa de ayuda)
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 30 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.

DANIEL ANDRÉS ROCHA RAMÍREZ
Director Sistemas y Tecnología
Dirección de Sistemas y Tecnología

JENIFFER CASTILLO FERNÁNDEZ
PROFESIONAL III
Dirección de Sistemas y Tecnología