	Universidad de San Buenaventura Cali Vicerrectoría Administrativa y Financiera Departamento de Tecnología Gestión de Infraestructura **RFP: Solución de Antivirus**
Fecha:	**Octubre 2024**

Solución de Antivirus

Introducción

La Universidad de San Buenaventura Cali, invita a los proveedores especializados en soluciones de Ciberseguridad a participar en el proceso para la adquisición de una solución integral de antivirus. Esta solución deberá ser capaz de integrarse de manera eficiente con la infraestructura de seguridad existente, que incluye, entre otros componentes, el firewall y el sistema de control de acceso a la red (NAC) de Fortinet El propósito de esta adquisición es reforzar la defensa contra amenazas cibernéticas avanzadas, asegurando la protección y disponibilidad continua de los recursos tecnológicos de la universidad. Buscamos una solución que no solo ofrezca una protección eficaz contra Malware, Spyware, Ransomware y otras amenazas, sino que también permita una gestión centralizada y automatizada, alineada con nuestras políticas de seguridad y operativas actuales.

Objetivo general

Seleccionar una solución de antivirus robusta, escalable y altamente compatible que se integre de manera eficiente con las soluciones de seguridad existentes de la Universidad, tales como el firewall y el sistema de control de acceso a la red (NAC). La solución debe ofrecer protección en tiempo real contra una amplia gama de amenazas avanzadas, garantizando una gestión centralizada y automatizada que optimice las operaciones de seguridad y cumpla con las políticas de ciberseguridad de la institución.

	Universidad de San Buenaventura Cali Vicerrectoría Administrativa y Financiera Departamento de Tecnología Gestión de Infraestructura **RFP: Solución de Antivirus**
Fecha:	**Octubre 2024**

Alcance

La Universidad de San Buenaventura Cali, tiene como objetivo renovar y modernizar su solución de antivirus para mejorar la protección de sus sistemas y datos frente a amenazas cibernéticas avanzadas. El alcance de este proyecto abarca los siguientes elementos clave, sin limitarse únicamente a ellos:

- **Protección Integral de Dispositivos:** La solución debe proporcionar cobertura completa para todos los dispositivos conectados a la red, incluyendo servidores, estaciones de trabajo y cualquier otro dispositivo crítico. Esta protección debe abarcar amenazas como malware, ransomware, spyware y ataques basados en vulnerabilidades conocidas o emergentes.

- **Integración Completa:** Se requiere que la solución de antivirus se integre de forma nativa y eficiente con el firewall y el sistema de control de acceso a la red (NAC) de Fortinet, entre otras, permitiendo una respuesta coordinada ante amenazas. La integración debe facilitar el intercambio de información en tiempo real para mejorar la visibilidad y el control de la seguridad.

- **Gestión Centralizada:** La solución debe ofrecer una consola de administración centralizada desde la cual sea posible gestionar políticas de seguridad, programar actualizaciones automáticas, generar reportes detallados y monitorear el estado de protección en tiempo real de todos los dispositivos de la red.

- **Detección Basada en Comportamiento:** Debe contar con capacidades avanzadas de detección de amenazas basadas en el comportamiento de los dispositivos y usuarios, identificando patrones anómalos que puedan sugerir posibles ataques cibernéticos antes de que se materialicen.

- **Compatibilidad Multiplataforma:** La solución debe ser compatible con múltiples sistemas operativos, incluidos Windows, MacOS y Linux, garantizando una protección uniforme en toda la infraestructura tecnológica de la universidad.

- **Escalabilidad y Flexibilidad:** Se espera que la solución propuesta sea escalable, permitiendo su expansión conforme la universidad crezca o se incorporen nuevos dispositivos y usuarios a la red, sin comprometer el rendimiento ni la seguridad.

Criterios de evaluación

A continuación, se presentan los criterios de evaluación:

Ítem	Clasificación Propuestas	Peso
1	Requerimientos Técnicos	40%
2	Requerimientos Económicos	40%
3	Requerimientos Proveedor	20%
	TOTAL	***100%***

REQUERIMIENTOS TÉCNICOS	FORMA DE EVALUACIÓN
Compatibilidad e Integración	Capacidad de integración con las soluciones actuales (firewall, NAC, etc.).
Protección y Detección de Amenazas	Capacidad de detección proactiva y en tiempo real contra malware, ransomware, spyware y ataques basados en comportamiento.
Gestión Centralizada	Facilidad de uso y funcionalidades de la consola de administración centralizada.
Actualizaciones Automáticas	Frecuencia y automatización en la actualización de las firmas de virus y las definiciones de amenazas.
Compatibilidad Multiplataforma	Soporte para distintos sistemas operativos (Windows, MacOS, Linux).
Escalabilidad	Capacidad de la solución para adaptarse al crecimiento futuro de la red y los dispositivos de la universidad.
Impacto en el Rendimiento	Evaluación del impacto que la solución tiene sobre el rendimiento de los dispositivos y la red.
Detección Basada en Comportamiento	Eficiencia en la detección basada en análisis de comportamiento de usuarios y dispositivos.

	Universidad de San Buenaventura Cali Vicerrectoría Administrativa y Financiera Departamento de Tecnología Gestión de Infraestructura **RFP: Solución de Antivirus**
Fecha:	**Octubre 2024**

REQUERIMIENTOS ECONÓMICOS	FORMA DE EVALUACIÓN
Precio Total	Costo inicial de adquisición (licencias, hardware adicional, etc.).
Costos de Mantenimiento	Gastos recurrentes para actualizaciones, soporte técnico, y renovación de licencias.
Costos Adicionales	Gastos ocultos o adicionales relacionados con la implementación o personalización de la solución.
Valor agregado – Servicios adicionales	Impacto de los valores agregados ofrecidos.

REQUERIMIENTOS PROVEEDOR	FORMA DE EVALUACIÓN
Experiencia del Proveedor	Experiencia previa en proyectos similares (particularmente en el sector educativo o en instituciones con estructuras similares).
Referencias y Casos de Éxito	Evaluación de referencias proporcionadas y casos de éxito en otras organizaciones.
Soporte Técnico	Disponibilidad de soporte técnico, canales de comunicación (teléfono, chat, email), tiempo de respuesta y niveles de servicio (SLA).
Capacidad de Implementación	Habilidad del proveedor para implementar la solución en el plazo y condiciones estipuladas
Certificaciones y Acreditaciones	Certificaciones relevantes en ciberseguridad o soluciones tecnológicas
Reputación en el Mercado	Evaluación de la reputación del proveedor en términos de confiabilidad, innovación y atención al cliente.
Asistencia Post-Venta	Disponibilidad de servicios de formación, consultoría y asistencia técnica después de la implementación.
Actualizaciones y Soporte Futuro	Compromiso del proveedor para actualizar la solución frente a nuevas amenazas y garantizar la evolución tecnológica.

	Universidad de San Buenaventura Cali Vicerrectoría Administrativa y Financiera Departamento de Tecnología Gestión de Infraestructura **RFP: Solución de Antivirus**
Fecha:	**Octubre 2024**

Instrucciones

- Fecha límite para envío de propuestas es 21 de octubre a través del sitio web https://ti.usbcali.edu.co/convocatorias/rfp-solucion-de-antivirus/
- Todas las preguntas o aclaraciones sobre este RFP, pueden hacerlo directamente al correo ginfraestructura@usbcali.edu.co con el asunto "RFP: Solución de Antivirus"
- Las propuestas deben presentarse en formato RAR, Zip o 7zip y no deben superar los 14 MB, este debe incluir:
    - Carta de presentación,
    - Propuesta técnica,
    - Propuesta económica,
    - Documentos adicionales requeridos.

Requisitos de la propuesta

Como requisitos a presentar están:

- **Información de la Empresa:** Descripción de la empresa, experiencia en el mercado, casos de éxito relevantes y 3 referencias de clientes.
- **Propuesta Técnica:**
    - Descripción detallada de la solución antivirus propuesta.
    - Esquema de integración con las soluciones actuales (Firewall Fortinet y NAC).
    - Especificaciones técnicas de la solución, incluyendo requisitos de hardware y software.
    - Plan de implementación, capacitación y cronograma.
- **Propuesta Económica:**
    - Costos de licenciamiento (por dispositivo, por usuario, etc.) a 3 años.
    - Costos de mantenimiento y soporte técnico.
    - Términos de pago y condiciones.

	Universidad de San Buenaventura Cali Vicerrectoría Administrativa y Financiera Departamento de Tecnología Gestión de Infraestructura **RFP: Solución de Antivirus**
Fecha:	**Octubre 2024**

Condiciones Generales

- Toda la información proporcionada en este RFP y en las propuestas será tratada con la más estricta confidencialidad.
- La solución propuesta debe respetar todas las leyes de propiedad intelectual y licenciamiento.
- Se aplicarán penalidades en caso de incumplimiento de los plazos acordados o del desempeño prometido.
- Indicar el compromiso Ambiental en la implementación del Proyecto
- Por políticas internas de la universidad, se debe realizar un contrato entre las partes, el cual, una vez firmado, se podrá proceder con el proceso de compra.
- Presentar la propuesta con todos los elementos, bienes y servicios necesarios para la solución, de otro modo no se recibirán propuestas con soluciones parciales.
- Contemplar los equipos a instalar (si los hay), servicios de instalación, puesta en operación y soporte para la solución.
- Presentar las hojas de vida y certificaciones con las que cuenta el personal que realizará la instalación, configuración y soporte a la Universidad
- Presentar las capacitaciones necesarias para su gestión
- Presentar la propuesta a 3 años, cronograma y un plan detallado de implementación y las herramientas a utilizar
- En la respuesta a esta propuesta deben adjuntar la tabla de si cumplen o no lo solicitado

Documentación Adicional

- Certificaciones de seguridad (si aplican).
- Informes de pruebas independientes sobre la efectividad del antivirus.
- Acuerdos de nivel de servicio (SLAs).

	Universidad de San Buenaventura Cali Vicerrectoría Administrativa y Financiera Departamento de Tecnología Gestión de Infraestructura **RFP: Solución de Antivirus**
Fecha:	**Octubre 2024**

Consideraciones

A continuación, se relacionan características y requerimientos que se evalúan en la solución de antivirus propuesta.

Características	Cumple	No cumple
La solución deberá poder realizar exploraciones en estado inactivo para poder brindar de esa forma, una protección proactiva mientras el equipo no está en uso.		
Tener un control web para limitar el acceso a los sitios web por categoría, además de poderle mostrar al usuario una notificación de bloqueo.		
Contar con la capacidad de enviar una tarea para la actualización de los parches del sistema operativo y aplicaciones de terceros.		
Ejecutar un escaneo profundo en los siguientes estados en la computadora: Protector de pantalla activo, sesión de usuario bloqueada, sesión de usuario finalizada.		
La solución debe ser capaz de permitir o negar el uso de los dispositivos en base a los criterios: Fabricante, modelo, número de serie		
Cuando se conecta o usa un dispositivo de almacenamiento, la solución de antivirus deberá hacer el escaneo al menos una vez para hacer uso del mismo.		
Sistema de prevención de intrusiones basado en el host (HIPS) e incluir una inspección a fondo del comportamiento de todos los programas en ejecución, archivos y llaves de registro		
Contar con Inteligencia artificial y Machine Learning.		

	Universidad de San Buenaventura Cali Vicerrectoría Administrativa y Financiera Departamento de Tecnología Gestión de Infraestructura **RFP: Solución de Antivirus**
Fecha:	**Octubre 2024**

Aislamiento del equipo en la red sin pérdida de administración		
Con capacidad de verificar comunicaciones SSL para detectar cualquier amenaza oculta.		
Contar con un firewall de host.		
Controlar todas las comunicaciones entrantes y salientes utilizando direcciones IP.		
Permitir que las reglas sean aplicadas de acuerdo con la ubicación del dispositivo red interna o externa.		
El producto debe de poder determinar, mediante la configuración, si el dispositivo se encuentra dentro o fuera de la organización.		
Integración con directorio activo.		
Administración basada en Nube.		
Contar con la ejecución administración remota (Scrips, instalación por consola, administrador de tareas)		
Compatibilidad con múltiples sistemas operativos (Windows, Linux, Android y Mac).		
Acceso a la consola de antivirus con doble factor de autenticación, sin ningún add-on o software adicional.		
Contar con des instalador de antivirus de terceros.		
Módulo para la protección contra ransomware.		

	Universidad de San Buenaventura Cali Vicerrectoría Administrativa y Financiera Departamento de Tecnología Gestión de Infraestructura **RFP: Solución de Antivirus**
Fecha:	**Octubre 2024**

Obtener a través de la consola de administración de seguridad el inventario de aplicaciones y de hardware de cada uno de los equipos protegidos.		
Desde la consola de administración de seguridad de punto final debe manejar la tecnología de Sandboxing en nube para el análisis de posibles amenazas, cifrado de los discos de almacenamiento de los equipos e integrarse con la solución de detección y respuesta del punto final.		
Control de acceso a consola para administradores y técnicos permitiendo crear perfiles granulares.		
La solución de protección en servidores debe incluir la detección y bloqueo de intrusiones, agregar a lista negra aquellas direcciones que han sido identificadas con este comportamiento malicioso.		
La solución deberá agregar de forma automática las exclusiones que correspondan a aplicaciones críticas del servidor.		
Optimizar el rendimiento de infraestructuras mixtas (hardware y virtuales) siendo capaz de eliminar la duplicidad de exploraciones en archivos, excluyendo los archivos ya explorados y limpios.		
La solución deberá ser capaz de cifrar los equipos con sistemas operativos Windows y MacOS.		
La solución deberá disponer de diversas posibilidades de recuperación de password de cifrado para usuarios remotos que se vean bloqueados.		
La solución deberá poder programar las tareas de cifrado sobre los equipos.		

	Universidad de San Buenaventura Cali Vicerrectoría Administrativa y Financiera Departamento de Tecnología Gestión de Infraestructura **RFP: Solución de Antivirus**
Fecha:	**Octubre 2024**

La solución de cifrado debe permitir anular la contraseña de inicio de sesión de la estación de trabajo.		
La solución debe permitir actualizar aplicaciones de terceros		
La solución debe detectar vulnerabilidades y exposiciones comunes (CVE).		
Permitir generar Informes de vulnerabilidades del software y los dispositivos más vulnerables.		
Contar con una visión general unificada a través de una única consola, con soporte multilingüe.		
Permitir lanzar actualizaciones y parches inmediatos a través de opciones personalizables, tareas o de forma manual.		
Proporcionar un inventario actualizado de parches con nombre del parche, nueva versión de la aplicación, CVE, gravedad/importancia del parche, aplicaciones afectadas.		
Se debe poder obtener un análisis en profundidad de detalle de la configuración del computador.		
Contar con soporte técnico en español.		
Oficinas de la marca en Latinoamérica y presencia local en el país.		
Contar con laboratorio de análisis y detección de malware en Latinoamérica.		
El Fabricante deberá tener presencia comprobable en Colombia.		
El Fabricante no deberá tener sanciones o restricciones a nivel global por parte de entidades de control.		

	Universidad de San Buenaventura Cali Vicerrectoría Administrativa y Financiera Departamento de Tecnología Gestión de Infraestructura **RFP: Solución de Antivirus**
Fecha:	**Octubre 2024**

Los indicadores de compromiso de la solución EDR /XDR deben combinar comportamiento y reputación.		
La solución de EDR / XDR debe tener la capacidad de detectar ataques sin archivo.		
La solución de EDR/ XDR deberá permitir modificar los indicadores de compromiso según la necesidad de la institución.		
La solución de EDR / XDR deberá mostrar alertas en la consola de administración y en el equipo del usuario.		
La solución debe mostrar el ID de la técnica MITRE ATT&CK		

	Universidad de San Buenaventura Cali Vicerrectoría Administrativa y Financiera Departamento de Tecnología Gestión de Infraestructura **RFP: Solución de Antivirus**
Fecha:	**Octubre 2024**

Inventario de equipos

A continuación, se detalla el inventario general de los equipos de cómputo que serán protegidos con la solución de antivirus. Es importante destacar que la cantidad de servidores y endpoints puede incrementarse con el tiempo. Por esta razón, se ha estimado una cotización basada en 200 licencias para servidores y 1000 licencias para endpoints.

DESCRIPCIÓN	SISTEMA OPERATIVO	ARQUITECTURA	CANTIDAD
Host de virtualización	Win Server 2019 Datacenter	x64	3
Windows Server Virtual	Windows Server 2012 Std - Windows Server 2022 Std	x64	77
Linux Server Virtual	CentOS 9 – Ubuntu 2022	x64	63
Usuarios Administrativos	Windows 10 - Windows 11. Desde 22H2	x86, x64	560
Usuarios Administrativos	MacOs - Moterrey - Sequoia	Intel i5 – Chip M1- Chip M3	36
Usuarios Académicos	Windows 10 - Windows 11. Desde 22H2	x64	420
Usuarios Académicos	MacOs - Sonoma - Sequoia	Intel i5 – Chip M1- Chip M3	16
Otros			25
Total			1200

	Universidad de San Buenaventura Cali Vicerrectoría Administrativa y Financiera Departamento de Tecnología Gestión de Infraestructura **RFP: Solución de Antivirus**
Fecha:	**Octubre 2024**

Requerimientos

A continuación, se establecen otros requerimientos con las que debe contar la solución ofertada.

- **Gestion de la solución:** Se requiere una solución basada en la nube que garantice una gestión remota, flexible y escalable. La plataforma debe ofrecer actualizaciones automáticas y en tiempo real para asegurar una protección óptima contra las últimas amenazas y de día 0.
- **Tipo de solución:** Se requieren propuestas para soluciones EDR, XDR o una combinación de las mismas que garanticen la seguridad de nuestros servidores y los endpoints, una respuesta ágil ante incidentes y una detección proactiva de amenazas en toda nuestra infraestructura.
- **Directorio Activo:** La solución debe contar con integración con directorio activo permitiendo la gestión de usuarios y equipos.
- **Despliegue:** El proceso de instalación deberá generar el menor impacto en las operaciones de los usuarios de la Universidad. Además, contar con diferentes opciones de despliegue (manual, política o desde nube).
- **Reportes y Auditorías:** La solución deberá contar con reportes de tipo ejecutivo, estado de amenazas, detalle de amenazas detectadas, incidentes, licencia y versiones instaladas de solución de antivirus, vulnerabilidades de sistemas y aplicaciones, versiones de aplicaciones Windows y de terceros, auditoria de políticas.
- **Roles:** La solución deberá contar con diferentes niveles de acceso y permisos para los usuarios administradores y técnicos.

Cronograma del proceso

El cronograma a seguir para el proceso es el siguiente:

- **Publicación del RFP:** 10 de octubre de 2024
- **Fecha Límite para Presentación de Propuestas:** 21 de octubre de 2024
- **Evaluación de Propuestas:** 22 al 25 de octubre 2024
- **Presentación de Resultados a comité:** 11 al 15 de noviembre
- **Inicio de Implementación:** Diciembre 2024 y Enero de 2025