FICHA TÉCNICA

1. DESCRIPCIÓN TÈCNICA DEL BIEN Y/O SERVICIO:

Componentes en la Solución

- AntiMalware
- Firewall
- Filtro de Contenido Web
- Control de descargas
- Actualizador de Software (Microsoft y Terceros)
- Control de Aplicaciones
- Consola en la nube basada en Security Cloud

Licenciamiento de Software Antivirus	
Descripción	**Requerimientos Mínimos**
Cantidad de licencias	9.184 (SEM) – 1.000 (Municipio de Pereira).
Licencias	Por estaciones de trabajo o servidores.
Versión	La última que el fabricante haya lanzado al mercado.
Idioma	Español – Inglés
Soporte de Idioma	Español – Inglés

Características Solución de Seguridad Informática (Antivirus) con consola en la Nube	
1	El software debe estar integrado por una solución de seguridad tipo multi-endpoint avanzada y contar con gestión central de la misma.
2	Debe contar con seguridad de extremos, es decir, seguridad de administración centralizada para computadoras, dispositivos móviles y servidores junto con la inclusión de administración integrada de dispositivos móviles y parches.
3	Debe incluir herramientas para la administración y aplicación de parches. Microsoft y de terceros. Debe incluir sincronización con WSUS.
4	Incluir además la implementación remota para la eliminación automática de software antivirus antiguo.
5	Incluir una consola cloud de administración unificada, administración automática de parches y actualizaciones de productos y bases de datos.
Portal de administración	
1	Debe contener una consola única de fácil administración, manejo y acceso, adicional, la solución debe poder ser utilizada desde cualquier dispositivo, local y remoto.
2	La consola debe ser unificada para la implementación, la administración y el monitoreo.

FICHA TÉCNICA

3	Administración de parches automática.
4	Preparado para total integración de las herramientas de gestión de terceros.
5	Debe reportar las amenazas en tiempo real.
6	La consola debe estar basada en sistemas automáticos e inteligencia artificial usando tecnologías predictivas y de comportamiento, proporcionadas a través de Security Cloud.
7	La solución debe proveer actualizaciones de seguridad oportunas de más de 2500 aplicaciones de Windows y terceros.
8	Debe estar diseñado para trabajar en conjunto como una solución integral, lo que elimina los conflictos que surgen normalmente al combinar productos de diferentes proveedores.
9	La solución debe tener un desempeño óptimo en el mercado, es decir, que a través de resultados de evaluación técnica con su implementación se obtenga un mejor rendimiento con un menor consumo de recursos.
Solución para PC	
1	Debe proporcionar seguridad con bajo consumo de recursos del equipo en ambientes Windows o Mac, junto con la administración y actualización de parches de seguridad o actualizaciones.
2	La solución debe disponer de protección para Mac, Windows y Linux.
3	Inclusión de análisis heurístico y de comportamiento avanzados.
4	Debe contener administración de parches totalmente integrada.
5	Debe incluir control para transacciones bancarias.
Dispositivos móviles	
1	La solución debe integrar la administración para dispositivos móviles desde consola.
2	Debe proteger y administrar todos los dispositivos móviles con iOS y Android mediante el uso de VPN y administración de dispositivos móviles.
3	Debe contar con un sistema de seguridad móvil de última generación para dispositivos con iOS y Android.
4	Debe incluir seguridad Wi-Fi (VPN).
5	La solución debe brindar protección web y de aplicaciones proactiva.
6	Incluir soporte disponible para MDM de terceros.
Servidores	
1	Debe integrar seguridad para servidores de multiplataforma.
2	Componentes de SharePoint y Exchange adicionales.
3	Componentes EMC Storage.
Características Avanzadas	
1	Control Preventivo
2	Control de contenido web
3	Control de conexión
4	Protección en tiempo real
5	Anti-malware para múltiples motores
6	Cortafuegos: Interactuar con Firewall de Windows
7	Protección de la navegación

FICHA TÉCNICA

8	Control de Redes
9	Configuración de recursos de emergencia
Antivirus	
1	Debe contener diferentes motores que permitan una rápida respuesta a nuevos tipos de virus.
2	La solución debe funcionar con un bajo nivel de detecciones incorrectas y falsas alarmas.
3	Debe soportar varios formatos de archivo (ZIP, ARJ, LZH, CAB, RAR, TAR, GZIP, BZIP2, hasta seis niveles de anidación).
4	Debe actualizar de manera automática los archivos de definición de virus.
5	La solución debe integrar un sistema de seguridad en la nube como servicio de detección para identificar aplicaciones y sitios web y a su vez proteger contra malware y otros.
Control de contenido web	
1	Debe contener un control web de contenido que permita restringir el uso improductivo e inapropiado de Internet y gestionar en los usuarios el contenido web al cual se le permite acceder desde la red de la empresa.
3	Debe proporcionar fácil exclusión de sitios de confianza del contenido web.
4	La solución debe ser capaz de controlar y proteger contra sitios web dañinos revisando la reputación del sitio en Security Cloud.
Otras características	
1	Especificar si desea bloquear o permitir archivos basados en condiciones tales como la extensión de archivo, los cuales podrán ser aplicados por perfiles a la red de usuarios.
2	Permitir la administración de sitios permitidos y denegados.
3	Incluir control de conexiones para sitios seguros.
4	Deberá tener plugins para los navegadores, para monitoreo en tiempo real de la navegación, mínimo con los navegadores más utilizados.

Además de lo anterior, la solución antivirus debe contener:

Item	Descripción
1	Se requiere que la consola de administración sea centralizada tanto para la red LAN como para la WAN en ambiente CLOUD Únicamente. La consola debe incluir mínimo los siguientes componentes Filtro de Contenido, Control De Aplicaciones, Firewall, Control de descargas, Actualizador de Software de Microsoft y por lo menos 2500 de software de terceros para administrar y gestionar los parches.
2	Su administración, gestión, con el fin de ahorrar costos se solicita que el producto sea 100% en ambiente Cloud.
3	Control de Aplicaciones: la solución debe controlar todo tipo de aplicaciones, que violan la seguridad en la red.
4	El producto a ofertar debe ser multiplataforma Windows, MAC y Linux como mínimo. Y debe ser compatible con la última generación de Browser.
5	Categorías del filtrado web, con el fin de controlar la navegación de cada usuario, la solución antivirus debe generar bloqueo a diferentes tipos de sitios.
6	La solución debe proporcionar control de dispositivos.

FICHA TÉCNICA

7	Detectar y actualizar parches de Microsoft y software de terceros, de forma automática o manual o programada desde la consola de administración.
8	A nivel de prevención, debe contener un motor inteligente, heurístico y anti-malware capacidad de detección de 0 días.
9	El control web debe restringir la navegación a sitios web basados en categorías.
10	Debe tener un control de conexión, el cual debe monitorear la seguridad adicional para transacciones sensibles, como banca en línea, bloqueando los demás puntos de navegación del equipo.
11	La solución debe proporcionar una protección de varios motores anti-malware.
12	Debe tener modulo Firewall más una capa adicional de protección que funciona dinámicamente con Control de aplicaciones.
13	La protección a la navegación debe proactivamente evitar que los usuarios tengan acceso a sitios que contienen enlaces o contenido malintencionado.
14	Debe controlar y administrar las descargas como ejecutables, archivos críticos o de oficina desde internet, con la posibilidad de generar restricciones o perfiles diferentes a cada usuario, grupo o toda la organización.
15	El fabricante debe proporcionar servicios con herramientas de escaneo de vulnerabilidades, control y administración de monitoreo para la organización. Esta herramienta puede ser anexa y para optimizar recursos, deberá ser Cloud. La solución debe ser del mismo fabricante e incluida en la propuesta. El escaneo de vulnerabilidades desde un portal web, debe poder encontrar vulnerabilidades como SQL Injection y Cross-Site Scripting y generar los respectivos informes, los cuales deben ser entregados. El servicio debe estar incluido mínimo 3 veces en el tiempo de licencia vigente del contrato.