ANEXO TENICO 1
SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA CONTRATACIÓN

EVALUACIÓN ASPECTOS TECNICOS HABILITANTES		CUMPLE / NO CUMPLE	
		SI	NO
El Software ofertado debe cumplir con las siguientes caracteristicas técnicas:			
DESCRIPCIÓN	REQUERIMIENTOS MÍNIMOS		
Licencias	2500 licencias de solución de seguridad avanzada (on-premise o nube) para estaciones de trabajo y servidores por el término de un (1) año.		
Versión	La última versión liberada por el fabricante a la fecha de inicio del contrato. Debe ser compatible con el idioma del sistema operativo en el cual se instalará la solución de seguridad.		
Administración	Consola local de administración centralizada, con alta disponibilidad, balanceo y cifrado TLS 1.3.		
Protección de Nueva Generación	Motor antimalware, Machine Learning, HIPS, análisis de comportamiento y bloqueo de exploits. Protección avanzada contra amenazas 0-day mediante sandboxing en la nube.		
EDR	Inclusión de plataforma de monitoreo en tiempo real, caza de amenazas y respuesta automatizada a incidentes.		
Control de Dispositivos	Bloqueo granular de dispositivos como USB, Bluetooth, impresoras, cámaras, Wi-Fi, según usuario, grupo o ubicación.		
Cobertura de Protocolos	Inspección de protocolos HTTP/HTTPS, SMTP/IMAP/POP3, FTP/SFTP, SMB, WebDAV.		
Mantenimiento	Soporte 7×24 (idiomas: Español/Inglés), severidad 1: respuesta ≤ 1 h, restauración ≤ 4 h. Incluye actualizaciones de módulos y versiones durante 12 meses.		
Capacitación	Capacitación certificada de 16 horas (8 h administración y 8 h nivel avanzado). Incluir entrenamiento en herramientas de detección de amenazas, automatización y reportes.		
Actualización	Suscripción a la base de datos por un periodo de un (1) año.		
Soporte de Idioma	Debe soportar como mínimo español e inglés.		
Aplicación de políticas por grupos	La consola de administración debe permitir agrupar los agentes en grupos para facilitar la configuración y administración de los mismos.		
Detección y Prevención	Funcionalidad de detección y prevención de intrusos a nivel de host para estaciones de trabajo y servidores.		
Notificaciones de Ataques	Servicio de alertas de ataques, con notificación a administradores por eventos críticos, enviados por e-mail.		
Firewall de Escritorio	Firewall bidireccional, IDS/IPS adaptable con políticas centralizadas para bloqueo de lateral movement, exploits y brute-force.		
Protección en Aplicaciones de Mensajería	Detección, análisis y solución de virus que se propagan por aplicaciones de mensajería y carpetas compartidas.		
Análisis de Reputación de Archivos	La solución debe tener la capacidad de analizar la reputación de archivos.		
Protección en Tiempo Real	Análisis y desinfección de archivos, programas, páginas web, correos electrónicos, unidades de disco y memorias USB en tiempo real, bloqueando archivos sospechosos.		
Firewall de host	Firewall de host con centralización de políticas desde consola que permita programar la validez de la regla de Firewall, crear reglas diferenciadas por aplicaciones, Permitir la creación de una zona de confianza, permitiendo que ciertas IP, protocolos o aplicaciones se comuniquen en la red		
Análisis por Demanda	Opción de iniciar procesos de búsqueda, detección y erradicación de amenazas desde la consola remota.		
Control de aplicaciones	Debe proporcionar una vista de riesgo de las aplicaciones existentes en endpoints y permitir la reducción de privilegios sin cambiar la funcionalidad de las aplicaciones comunes		
Aislamiento de Aplicaciones	Reducción del riesgo y la exposición a las aplicaciones		
Integración con Correo Electrónico	Agentes para sistemas de correo electrónico, con soporte para antispam y análisis de adjuntos.		

ANEXO TENICO 1
SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA CONTRATACIÓN

EVALUACIÓN ASPECTOS TECNICOS HABILITANTES		CUMPLE / NO CUMPLE	
		SI	NO
Control de dispositivos	Controlar el uso de dispositivos con comunicación infrarroja, firewire, PCMCIA, puertos serie y paralelo, a través de mecanismos de permisos y bloqueo, identificando por el "ID de Clase" y el "ID de Dispositivo" del Dispositivo		
Integración con Directorio Activo	Opción para conexión y sincronización con Directorio Activo para facilitar la administración y control de los clientes desde una consola centralizada.		
Protección de Directorio Activo	Protección contra la escalada de privilegios y el movimiento lateral en un entorno de Active Directory		
Integridad de host	Funcionalidades de control de integridad		
	Condiciones del antivirus (verificar firmas, y servicio de antivirus		
	Condiciones del archivo (Comprobar existencia de Archivo, Antigüedad, compara tamaño, comparar versión)		
	Condiciones parches (Verificar Servicie Pack y parche instalado)		
	Condiciones de registro (Verificar si una llave existe, establecer valor del registro, verificar si el valor del registro existe)		
	Condiciones de utilidad (Verificar servicio en ejecución o Proceso)		
Configuración de Políticas	Configuración de políticas adaptables a usuarios individuales o grupos de usuarios.		
Reportes	Generación de informes personalizables (virus detectados, estaciones infectadas, versión de antivirus, etc.).		
Escalabilidad	Actualización automática para 2500 máquinas administradas, de forma inteligente y sin intervención del usuario.		
Repositorios Distribuidos	Administración de repositorios distribuidos que optimicen la carga del servidor central y distribución a través de la red.		
Soporte Multiplataforma	Compatibilidad con Windows, macOS, Linux y dispositivos móviles iOS y Android.		
Cuarentena e Informe	Capacidad de almacenar archivos sospechosos en cuarentena para su posterior análisis y restauración.		
Instalación/Desinstalación	Permitir instalación o desinstalación desde la consola remota.		
Motor de Detección	Detección avanzada mediante firmas, Machine Learning, sandboxing, HIPS, protección contra ransomware, botnets, exploits y ataques dirigidos.		
Entregables del Proyecto	a) Documento de arquitectura y dimensionamiento. b) Plan de implementación (piloto-masivo-optimización). c) Plan de pruebas y acta de aceptación. d) Manuales administradores/usuarios.		

Victor Julio Gómez Carvajal
Jefe Oficina Sistemas de Información - TICS

Proyectó: Andrés Felipe Cubillos Garcia - Profesional Especializado