TIPO DE INFORME				No. DE CONTRATO	PERIODO DEL INFORME	
					DESDE (dd/mm/año)	HASTA (dd/mm/año)
PARCIAL		FINAL	X	286-2024	20/11/2024	20/11/2024
CONTRATANTE				E.S.E HOSPITAL SUSANA LOPEZ DE VALENCIA		
N° PROCESO CONTRATACION SECOP						
CONTRATISTA				SOLUCIONES TECNOLOGICAS APLICADAS DE COLOMBIA SAS		
No. DE IDENTIFICACIÓN				NIT 900.593.363-7	**EXPEDIDA EN**	N/A
No. TELÉFONO y/o CELULAR				6028353677		
SUPERVISOR y/o INTERVENTOR				ROBERT CAMACHO		
No. DE IDENTIFICACIÓN				CC 76.306.787	**EXPEDIDA EN**	POPAYÁN
No. TELÉFONO y/o CELULAR				311 364 2114		
APOYO A LA SUPERVISION				LUCY XIMENA IBARRA HERNANDEZ	**EXPEDIDA EN**	
IDENTIFICACION				CC. 66.858.564		
No. TELÉFONO y/o CELULAR						
IMPUTACIÓN PRESUPUESTAL				938 del 31/oct/2024	**VALOR TOTAL DEL CONTRATO**	$33.616.000
FORMA DE PAGO				UNICA CUOTA	**PAGO No.**	
VALOR A PAGAR				TREINTA Y TRES MILLONES SEISCIENTOS DIECISÉIS MIL PESOS M/CTE		
PAGO SEGURIDAD SOCIAL						
IBC al sistema de Seguridad Social (40% del Ingreso mensual) Y / O Certificación de pago de aportes al sistema de seguridad social y parafiscales					**PERIODO COTIZADO**	PENSIÓN 2024-10 SALUD 2024-11
EPS					**VALOR PAGADO**	$ 512.000
ARL					**VALOR PAGADO**	$ 67.100
CCF					**VALOR PAGADO**	$ 512.000
AFP					**VALOR PAGADO**	$ 2.178.000
VALOR TOTAL PLANILLA				$3.269.100	**PLANILLA No.**	**9477402072**
Certificación de pago de aportes al sistema de seguridad social y parafiscales				**SE ADJUNTA CERTIFICACIÓN EXPEDIDA A LOS DIECINUEVE (19) DÍAS DEL MES DE NOVIEMBRE DE 2024 POR EL CONTADOR.**		

OBJETO DEL CONTRATO
COMPRA DE LICENCIA DE SOFTWARE ANTIVIRUS PARA EL ÁREA DE SISTEMAS DE INFORMACIÓN DEL HOSPITAL SUSANA LÓPEZ DE VALENCIA E.S.E.

ESPECIFICACIONES TECNICAS REQUERIDAS

Soluciones Tecnológicas Aplicadas de Colombia SAS con Nit 900593363-7 entrega el producto ESET PROTEC ENTRY con las siguientes protecciones:

1.1.1. Primer componente: Generalidades son las siguientes:

- ✓ 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.
- ✓ Debe tener un caché local para aumentar el rendimiento de los entornos virtuales, garantizando que el archivo sólo se explora una vez.
- ✓ El producto debe tener un control web para limitar el acceso a los sitios web por categoría, además de poderle mostrar al usuario una notificación de bloqueo.
- ✓ El bloqueo web deberá poder asignarse por un rango de tiempo, por grupo y por equipo.
- ✓ Deberá tener la capacidad para actualizar los parches del sistema operativo.
- ✓ Dentro del módulo de firewall deberá contar con la funcionalidad de bloqueo de exploits.
- ✓ "La solución de anti-malware debe ejecutar un escaneo únicamente 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 con base a los siguientes criterios:

- Fabricante
- Modelo
- Número de serie"

- ✓ La solución debe ser capaz de definir un listado específico de usuarios quienes pueden hacer uso de los dispositivos. Para dispositivos de almacenamiento, la solución debe permitir configurar únicamente de los siguientes permisos:

- Lectura/Escritura
- Bloqueo
- Solo de lectura
- Advertir"

- ✓ Cuando se conecta o usa un dispositivo de almacenamiento, la solución de anti-malware debe proporcionar las siguientes opciones:

- Escanear
- No realizar ninguna acción
- Recordar esta acción"

- ✓ La solución debe tener sistema de prevención de intrusiones basado en el host. El sistema HIPS debe tener los siguientes modos de configuración:

- Modo automático
- Modo inteligente
- Modo interactivo
- Modo basado en políticas
- Modo aprendizaje"

- ✓ La solución deberá contar con aprendizaje automático avanzado mediante "machine learning" y este a su vez deberá tener cuatro umbrales: Intenso, Balanceado, Cauteloso y Desactivado.
- ✓ El HIPS debe incluir una inspección a fondo del comportamiento de todos los programas en ejecución, archivos y llaves de registro
- ✓ Debe contar con filtrado para mantener libre de SPAM a los clientes de correo, por ejemplo Outlook.
- ✓ La solución debe capaz de verificar las comunicaciones usando protocolos SSL.
- ✓ La solución de anti-malware debe contar con un firewall personal. El firewall debe tener los siguientes modos de configuración:

- Modo automático
- Modo interactivo
- Modo basado en políticas
- Modo aprendizaje"

- ✓ Las reglas de firewall creadas deberán ser capaces de permitir todas las siguientes acciones:

- Denegar
- Permitir
- Preguntar"

- ✓ La solución anti-malware debe ser compatible con entornos de virtualización basados en citrix y deben contar con el aval de dicho Fabricante.
- ✓ La solución deberá permitir la creación de exclusiones por ruta, detección y su hash (SHA-1).
- ✓ Capacidad de sincronizar su licenciamiento con la nube y la consola de administración en sitio o en la nube.

1.1.2. Segundo componente: Consola de administración debe ser las siguientes:

- ✓ Deberá permitir la ejecución remota de scripts, batch files y paquetes personalizados a través de la consola, de terceros.
- ✓ Deberá ser una solución 100% cloud que pueda ser usada y administrada desde cualquier tipo de navegador web compatible con sistemas operativos Windows, Linux y Mac.
- ✓ Debe permitir generar grupos de clientes dinámicos y grupos estáticos, al igual que debe permitir la sincronización con Microsoft Active Directory con el propósito de facilitar la gestión de pólíticas y de usuarios reportados a la consola de administración.
- ✓ El Fabricante debe proporcionar al menos tres diferentes formas de realizar la instalación de la consola de administración.
  - Instalador todo en uno
  - Instalación por componentes
  - Aparato virtual"
- ✓ La consola de Administración deberá ser Cloud y deberá contar con los estándares de seguridad requeridos para este tipo de ambientes.
- ✓ La solución debe activar el acceso a la consola con doble factor de autenticación, deber estar integrada a la misma consola de antimalware, sin ningún add-on o software adicional.
- ✓ La solución debe contar con un portal de administración de licencias que permita realizar procesos de control y auditoría sobre el uso adecuado del licenciamiento.
- ✓ La solución debe contar con des-instalador de anti-malware de terceros.
- ✓ La solución debe contar con un módulo específico para la protección contra ransomware.
- ✓ La solución deberá tener la capacidad para aplicar durante cierto periodo de tiempo las reglas de control de dispositivo y de control de acceso web a través de la consola de administración.
- ✓ La solución deberá contar con etiquetas independiente al LDAP, para identificar y buscar objetos similares.

- ✓ La solución debe obtener a través de la consola de administración el inventario de aplicaciones y de hardware de cada uno de los equipos protegidos y debe permitir generar el informe en xls, cvs, pdf.
- ✓ La solución debe a través de la misma consola de administración de seguridad manejar la tecnología de Sandboxing en nube para el análisis de posibles amenazas, cifrado de los discos de almacenamiento e integrarse con la solución de detección.
- ✓ A través de la consola de administración de seguridad del endpoint debe ser posible administrar dispositivos móviles iOS y Android y tener una base de datos independiente a la del resto de los equipos de endpoint (servidores y estaciones de trabajo).
- ✓ La solución debe tener el mecanismo para desinstalar otras soluciones anti-malware presentes en el endpoint. Este mecanismo debe ser y estar:
    - Integrado al paquete de instalación de la solución de protección del endpoint.
    - Disponible solamente a través de la misma consola de administración de protección al endpoint."

1.1.3. Tercer componente: Solución para dispositivos móviles:

- ✓ La solución de anti-malware debe realizar análisis a las aplicaciones instaladas, archivos .DEX, .SDK y .APK.
- ✓ La solución de anti-malware ofertada deberá analizar memoria interna y tarjeta SD para cualquier tipo de archivo.
- ✓ La solución debe ser capaz de mostrar un listado de las aplicaciones instaladas, controlar el tiempo del uso de aplicaciones y tener el detalle de los permisos que usan los aplicativos del dispositivo móvil.
- ✓ La protección del dispositivo móvil debe contar con una protección en tiempo real, además de contar con un sistema de reputación de archivos.
- ✓ Deberá poder administrar las aplicaciones que deberían estar instaladas en los dispositivos móviles.
- ✓ Debe tener la capacidad para detectar de forma automática aplicaciones no deseadas y no seguras para usar en el dispositivo móvil.
- ✓ La solución debe poder enviar mensajes SMS al administrador cuando existen usuarios no autorizados manipulando el dispositivo móvil.
- ✓ La solución será capaz de proteger y seleccionar los navegadores web a utilizar.
- ✓ La solución de anti-malware deberá ser inteligente para optimizar la batería del dispositivo y ejecutar el análisis al dispositivo únicamente cuando esté completamente cargado o conectado a la energía eléctrica.
- ✓ La solución será capaz de detectar nuevas tarjetas instaladas en el dispositivo y bloquearlas.
- ✓ Es importante que la solución sea capaz de generar códigos de verificación SMS temporales al administrador para ejecutar tareas de desbloqueo de dispositivos o regresar a configuración de fábrica.
- ✓ La solución será capaz de mantener un control de aplicaciones, bloquearlas según los permisos de la aplicación o por categoría, deberá limitarse a instalar aplicaciones únicamente desde Google Play, y poder bloquear cualquier aplicación en el momento que se necesite.
- ✓ La solución será capaz de evitar ataques de suplantación de identidad de sitios web.

1.1.4. Cuarto componente: Solución para servidores:

- ✓ 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 debe ser compatible e integrable con la consola de administración de seguridad la cual debe ser Cloud.

OBLIGACIONES DEL CONTRATISTA

OBLIGACIONES	ACTIVIDADES REALIZADAS	SOPORTE
1.Informar a los supervisores del contrato acerca de cualquier eventualidad relacionada con la ejecución del contrato.	No se presentaron inconformidades.	N/A
2.No ceder ni subcontratar las actividades del objeto del contrato.	STAC no subcontrato ni cedió el contrato.	N/A
3.Entregar las licencias de software según las especificaciones técnicas en las instalaciones del Hospital, dentro de los 8 días siguientes al inicio de la ejecución del contrato.	Las licencias fueron entregadas y activadas electrónicamente desde fábrica.	Certificado de licenciamiento
4.Dar garantía de un año por conecto de fallas o actualizaciones presentadas por las licencias entregadas al hospital.	Se realizara soporte durante el tiempo de licenciamiento, desde STAC Tecnología, hasta casa matriz de ESET.	N/A
5.Cumplir con los tiempos establecidos del contrato.	Se cumplió con los tiempos establecidos en el contrato	N/A
6.Atender las solicitudes de los supervisores	Las solicitudes han sido atendidas y resueltas.	N/A
7.El contratista deberá acatar el SGA del Hospital, conocer su política y los objetivos ambientales; adquirir el compromiso de gestionar los aspectos ambientales asociados a las actividades derivadas de la ejecución del contrato y garantizar el cumplimiento de la totalidad de las obligaciones como proveedor del servicio, según la normatividad ambiental aplicable vigente, así como también garantizar la adherencia al mejoramiento continuo de la certificación ISO 14001:2015 de la cual la institución es acreedora.	Se acata el SGA y se tiene pleno conocimiento de las políticas y objetivos ambientales.	N/A

DOCUMENTOS ANEXOS	No. FOLIOS, CD'S, DVD'S

✓ FACTURA N° FE1237 ✓ CERTIFICACIÓN DE PAGO SS Y PARAFISCALES PLANILLA N° 9477402072 ✓ CERTIFICADO DE LICENCIAMIENTO	✓ 1 FOLIO ✓ 1 FOLIO ✓ 1 FOLIO
Dado en la ciudad de Popayán, el 20 de noviembre de 2024	
 **FIRMA CONTRATISTA**	**JULIAN CAMILO DELGADO BURBANO** **CC 1.061.728.957** **Representante Legal** **NIT 900.593.363-7**