HOSPITAL UNIVERSITARIO DE SANTANDER
EMPRESA SOCIAL DEL ESTADO

RQ 466 09/04/2026

Fecha	06 / 04 / 2026
Unidad Gestora	SUBGERENCIA ADMINISTRATIVA Y FINANCIERA UNIDAD FUNCIONAL DE APOYO TECNOLOGICO Y DE INFORMACION-SISTEMAS DE INFORMACION
Descripción Necesidad	La ESE Hospital Universitario de Santander, como una institución vital de tercer y cuarto nivel, maneja datos clínicos y personales sensibles de miles de ciudadanos. Ante el panorama actual, donde las amenazas cibernéticas, particularmente el Ransomware, son cada vez más sofisticadas, y dada la creciente dependencia de los servicios asistenciales en la tecnología, se hace imperativo contar con una infraestructura que no solo prevenga ataques, sino que asegure la Ciber-Resiliencia. Esto significa que la institución debe ser capaz de resistir, absorber el impacto y recuperarse rápidamente de cualquier incidente sin interrumpir la prestación esencial de los servicios de salud. Así mismo, es fundamental atender y cerrar de manera urgente la brecha de seguridad identificada en el autodiagnóstico de 2025. Específicamente, se requiere mejorar la visibilidad sobre el tráfico interno de la red, implementar controles de seguridad perimetral avanzados para la gestión del acceso de terceros (proveedores), y reorganizar la arquitectura de red para garantizar la alta disponibilidad y eliminar cualquier punto único de falla. Abordar estos puntos es crucial no solo para proteger la Historia Clínica Electrónica y otros servicios tecnológicos de soporte, sino también para dar estricto cumplimiento al Plan de Seguridad de la Información institucional y asegurar la continuidad operativa en todo momento. La Empresa Social del Estado Hospital Universitario de Santander E.S.E. requiere actualizar, fortalecer y unificar su infraestructura de ciberseguridad perimetral y de usuario final (endpoints). Actualmente, el panorama de amenazas cibernéticas (especialmente ransomware y secuestro de información) dirigido al sector salud exige contar con mecanismos de prevención, detección y respuesta automatizada. Se hace imperiosa la necesidad de adquirir una plataforma de Firewall de Próxima Generación (NGFW) en clúster de Alta Disponibilidad (HA), protección nativa para aplicaciones web (WAF) institucionales y una solución de seguridad avanzada para los dispositivos de los usuarios finales y servidores, garantizando la continuidad en la prestación de los servicios de salud sin disrupciones por incidentes informáticos.
Justificación	**Cumplimiento Legal y Regulatorio:** • **Acatamiento de la Ley 1581 de 2012 (Protección de Datos Personales):** El proyecto es imperativo para garantizar el manejo responsable y seguro de la información sensible de los pacientes (historias clínicas, datos de identificación, diagnósticos, etc.), asegurando el derecho constitucional al Habeas Data y mitigando el riesgo de sanciones por incumplimiento ante la Superintendencia de Industria y Comercio (SIC). • **Adherencia a la Circular 003 de 2018 de la Superintendencia Nacional de Salud (Supersalud):** Se da estricto cumplimiento a las directrices específicas del ente regulador del sector salud sobre la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) maduro, lo cual es vital para mantener la habilitación y la confianza en la gestión hospitalaria. **Continuidad del Negocio:** La salud se clasifica como un servicio público esencial. Por lo tanto, cualquier interrupción operativa (por ejemplo, una caída del sistema debido a un ransomware o un ciberataque de denegación de servicio) tiene consecuencias directas y potencialmente fatales en la vida de los pacientes. La indisponibilidad del sistema implica el retraso inmediato en: o Cirugías y Procedimientos: Al no poder acceder a protocolos o agendamiento.

Con la firma de este documento manifiesto que autorizo el tratamiento de mis datos personales conforme lo establecido en la Ley 1581 de 2012 y el Decreto 1377 de 2013, para los fines aquí establecidos.

HOSPITAL UNIVERSITARIO DE SANTANDER
EMPRESA SOCIAL DEL ESTADO

	○ Diagnósticos y Resultados de Laboratorio: Lo que impide la toma de decisiones médicas oportunas. ○ Entrega y Dispensación de Medicamentos: Afectando el tratamiento de pacientes ambulatorios y hospitalizados. La implementación del proyecto establece mecanismos de respuesta y recuperación ante desastres (Disaster Recovery Plan - DRP) que garantizan la operación mínima vital en caso de contingencia. **Alineación con la Política de Transformación Digital (Modelo de Arquitectura Empresarial - MAE):** El proyecto se alinea con las directrices y marcos de referencia definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) para impulsar la transformación digital en el sector público. Así mismo, la ejecución del proyecto asegura que la infraestructura de TI que soporta la prestación de servicios tecnológicos no solo sea segura, sino que también cumpla con los estándares de arquitectura empresarial del Estado, facilitando futuras integraciones, interoperabilidad con otras entidades y la adopción de tecnologías emergentes. Adicionalmente, como entidad prestadora de servicios de salud, maneja datos sensibles de pacientes (Historias Clínicas), cuya confidencialidad, integridad y disponibilidad están protegidas por la ley. Una caída en la red o un secuestro de datos afectaría directamente la atención vital de los pacientes. La adquisición de equipos en Alta Disponibilidad (HA) elimina los puntos únicos de falla. Adicionalmente, integrar la protección del perímetro (Firewall) con la protección del dispositivo final (Endpoint) y de los aplicativos expuestos a internet (WAF) bajo una misma estrategia de seguridad sincronizada, permitirá a la Unidad Funcional de Apoyo Tecnológico de la ESE HUS aislar amenazas de forma automatizada, reduciendo los tiempos de respuesta ante incidentes y garantizando un soporte continuo 24x7 por los próximos tres (3) años
Objeto	ADQUISICIÓN, INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO DE UNA SOLUCIÓN INTEGRAL DE CIBERSEGURIDAD COMPUESTA POR DOS (2) FIREWALLS DE PRÓXIMA GENERACIÓN (NGFW) EN ALTA DISPONIBILIDAD, LICENCIAMIENTO DE WEB APPLICATION FIREWALL (WAF) Y UNA SOLUCIÓN DE PROTECCIÓN AVANZADA PARA DISPOSITIVOS FINALES (EPP/EDR), INCLUYENDO EL LICENCIAMIENTO, ACTUALIZACIONES Y GARANTÍA DE HARDWARE PARA LA E.S.E. HOSPITAL UNIVERSITARIO DE SANTANDER.
Especificaciones Técnicas	Se requiere que los elementos y servicios a adquirir cumplan con las siguientes características mínimas: **Plataforma de Firewall de Próxima Generación (NGFW) - Cantidad: Dos (2) Equipos (Hardware)** Cada appliance físico debe cumplir mínimo con las siguientes características: • **Factor de forma:** Montaje en rack de máximo 2 Unidades de Rack (2U). • **Interfaces de Red Base:** Mínimo cuatro (4) puertos Gigabit Ethernet RJ45, cuatro (4) puertos Gigabit Ethernet SFP y ocho (8) puertos 10G SFP+. • **Expansión:** Mínimo cuatro (4) ranuras (slots) disponibles para tarjetas de red (NIC) adicionales. • **Almacenamiento Local:** Sistema de almacenamiento de estado sólido dual (Ej. un disco de al menos 128GB para sistema operativo y otro de al menos 960GB para almacenamiento de logs y reportes). • **Redundancia Eléctrica:** Fuentes de poder de corriente alterna (AC) duales e integradas.

Con la firma de este documento manifiesto que autorizo el tratamiento de mis datos personales conforme lo establecido en la Ley 1581 de 2012 y el Decreto 1377 de 2013, para los fines aquí establecidos.

HOSPITAL UNIVERSITARIO DE SANTANDER
EMPRESA SOCIAL DEL ESTADO

	Licenciamiento de Seguridad Perimetral (NGFW) - Por tres (3) años Para los dos (2) equipos en Alta Disponibilidad, se debe incluir licenciamiento completo que habilite las siguientes funciones: • Prevención de intrusiones (IPS), Control de Aplicaciones, Filtrado de URLs y Gestión de Ancho de Banda. • Inspección de tráfico y protección contra malware impulsada por motores de Inteligencia Artificial, inteligencia de amenazas en la nube, protección contra Botnets y seguridad de correo electrónico (Antispam). • Funcionalidades de ruteo avanzado y Secure SD-WAN. • Módulo de VPN IPsec Site-to-Site y VPN SSL con capacidad para mínimo treinta (30) usuarios concurrentes. • Consola de reportería de seguridad básica y gestión centralizada de alertas. **Licenciamiento de Web Application Firewall (WAF) - Por tres (3) años** Módulo embebido o integrado para ambos equipos que incluya: • Protección basada en firmas, motor de análisis semántico, ocultamiento de aplicaciones y detección de anomalías HTTP,HTTPS. • Escáner pasivo de vulnerabilidades y reportería avanzada de seguridad web. **Transceptores (Ópticas) a suministrar** • Ocho (8) módulos ópticos SFP 1G Multimodo (850NM, alcance hasta 550M). • Dieciséis (16) módulos ópticos SFP+ 10G Multimodo (850NM, alcance hasta 300M). • Patch cord de fibra (48) **Solución de Protección Avanzada de Endpoints (EPP/EDR) - Por tres (3) años** Suscripción para ochocientos veinte (820) agentes de protección finales (Soporte para PC, Workstation, Linux, Mac y Servidores). Debe incluir: • Gestión centralizada desde una consola en la nube (SaaS) con retención de logs de seguridad. • Gestión de vulnerabilidades, inventario de software/hardware, control de dispositivos USB y verificación de cumplimiento. • Protección contra ransomware mejorada (incluyendo doble factor de autenticación para RDP, protección de directorios clave y procesos confiables). • Protección contra amenazas avanzadas, control de aplicaciones y motor antimalware basado en Inteligencia Artificial. • Capacidad de respuesta y aislamiento de red en integración directa con el NGFW adquirido. **Servicios Profesionales y Transferencia de Conocimiento** • Instalación y configuración remota (o en sitio) ejecutada directamente por ingenieros del fabricante.
Requisitos Técnicos Habilitantes	El contratista deberá cumplir estrictamente con los siguientes puntos para la habilitación de su oferta:

Con la firma de este documento manifiesto que autorizo el tratamiento de mis datos personales conforme lo establecido en la Ley 1581 de 2012 y el Decreto 1377 de 2013, con los fines aquí establecidos.

	• **Carta de Respaldo del Fabricante:** El proponente debe adjuntar una certificación oficial emitida directamente por el fabricante de la solución, donde se autorice al proponente para comercializar, instalar y dar soporte a los equipos ofrecidos para el Hospital Universitario de Santander. • **Integración Nativa:** El fabricante propuesto debe ser el mismo tanto para el hardware de red (Firewall) como para el software de usuario final (Endpoint), con el fin de garantizar la integración nativa y la respuesta automatizada ante incidentes (EDR) sin depender de APIs de terceros.
Obligaciones	El futuro contratista debe comprometerse a realizar las siguientes actividades: - Entregar la totalidad de los equipos hardware ofertados en perfectas condiciones y en sus empaques originales. - Proveer acceso a los portales de soporte del fabricante para la descarga de actualizaciones de software, firmas de antivirus, IPS y control de aplicaciones. - Garantizar el reemplazo de hardware por avería (Return to Factory o equivalente) durante los tres (3) años del contrato. - Entregar soporte técnico en modalidad 24x7 directamente por el fabricante. - **Entrega de Hardware y Licencias:** Entre tres (3) a cuatro (4) semanas a partir de la firma del acta de inicio. **OBLIGACIONES ESENCIALES** - EL CONTRATISTA deberá garantizar la desinstalación de las soluciones actuales Protección de Endpoints (EDR), y la instalación configuración y correcta operación de la solución de Protección de Endpoints (EDR) en todos los puestos de trabajo y servidores definidos por la ESEHUS, asegurando la protección, detección y respuesta ante amenazas en las estaciones de trabajo y la infraestructura de servidores de la entidad. - El CONTRATISTA deberá presentar la garantía correspondiente a cada equipo, en caso de ser comercializador esta garantía deberá ser certificada por el fabricante o distribuidor exclusivo. - El CONTRATISTA deberá garantizar que el personal utilizado para la ejecución del contrato respetará y acatará las normas internas de la institución y deberá de estar identificado (carnetizado) dentro de las instalaciones de la ESE HUS. - El CONTRATISTA suministrará los repuestos o equipos que sean necesarios para la reparación y dejar en perfecto funcionamiento cualquiera de los elementos ofertados sin costo alguno para el Hospital Universitario de Santander. Este requisito no exceptúa ningún tipo de repuesto durante el tiempo de garantías y de la vigencia del contrato. - El CONTRATISTA se hace responsable por la legitimidad de marca y /o patentes relacionadas con los componentes físicos y lógicos de los equipos y sistemas ofrecidos. - El CONTRATISTA será responsable por toda reclamación que pueda presentarse por concepto de violación a las patentes, licencias o manifiestos de importación, de la calidad de materiales, etc. Y serán por su cuenta todos los gastos que puedan ocasionarse por tal concepto. - El CONTRATISTA se responsabilizará por todos los gastos de transporte, seguros nacionales e Internacionales y gastos de importación si fuese necesario. - El CONTRATISTA deberá certificar que todos los equipos ofertados son nuevos y por ningún motivo se podrán ofertar equipos re-manufacturados, repotenciados o de segunda. - El CONTRATISTA deberá hacer entrega de las tecnologías ofertadas mediante acta con los respectivos seriales al área de almacén para su ingreso al inventario de la institución. - El CONTRATISTA deberá certificar que las tecnologías ofertadas son amigables con el medio ambiente o contener criterios que minimicen el impacto ambiental.

Con la firma de este documento manifiesto que autorizo el tratamiento de mis datos personales conforme lo establecido en la Ley 1581 de 2012 y el Decreto 1377 de 2013, para los fines aquí establecidos.

HOSPITAL UNIVERSITARIO DE SANTANDER
EMPRESA SOCIAL DEL ESTADO

	- El CONTRATISTA debe garantizar y dar cumplimiento al presente anexo de confidencialidad para el manejo de la información de la E.S.E HUS de acuerdo a la normatividad vigente – ver anexo No. 1.		
Plazo	90 días contados a partir de la firma del acta de inicio	**Lugar de Ejecución**	Edificio Principal E.S.E. Hospital Universitario de Santander
Valor Sugerido	MIL TRESCIENTOS NOVENTA Y CUATRO MILLONES DE PESOS M/CTE ($1.394.000.000)		

OBSERVACIONES: *V.S (N/A).*

LEIDER LARIOS ECHAVEZ
Profesional Universitario - UFATI.

NELLY MENDEZ MEZA
Profesional Especializado - UFATI.

FABIO A.ALVARADO RODRIGUEZ.
Contratista Ese Hus.
(Apoyo a la supervisión técnica)

DR. VLADIMIR LOPEZ BARON
Subgerente Administrativo y Financiero

Proyectó: Fabio Alvarado - CPS - Oficina Asesora de Planeación y Desarrollo Institucional

Con la firma del presente documento manifiesto que autorizo el tratamiento de mis datos personales conforme lo establecido en la Ley 1581 de 2012 y el Decreto 1377 de 2013, para los fines aquí establecidos.