RESERVADO

ANEXO "A"

ESPECIFICACIONES TÉCNICAS

ADQUIRIR, CONFIGURAR E IMPLEMENTAR, DE UN SISTEMA DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD DE NUEVA GENERACIÓN.

ESPECIFICACIONES TÉCNICAS:

	1 REQUERIMIENTOS GENERALES	

	2. RECOLECCIÓN, NORMALIZACIÓN Y ENRIQUECIMIENTO DE LOGS	CUMPLE / NO CUMPLE

	3. CONSULTA DE LOGS, ANÁLISIS FORENSE Y CACERÍA DE AMENAZAS	CUMPLE / NO CUMPLE

	3. PANELES DE CONTROL Y REPORTES	CUMPLE / NO CUMPLE

	5.GESTIÓN DE ENTIDADES	CUMPLE NO CUMPLE

	6. FUNCIONES DE LA ANALÍTICA AVANZADA DE SEGURIDAD (UEBA)	CUMPLE NO CUMPLE

	7. INVESTIGACIÓN DE ALERTAS Y CASOS (INCIDENTES)	CUMPLE NO CUMPLE

	8. RESPUESTA A INCIDENTES (SOAR)	CUMPLE NO CUMPLE

	10. SOPORTE, MANTENIMIENTO Y ACUERDO DE NIVELES DE SERVICIO (SLA)	CUMPLE NO CUMPLE

HARDWARE: MÓDULO DE INFRAESTRUCTURA FÍSICA: COLECTORES ESPECIALIZADOS (SITE COLLECTORS).

SE REQUIERE LA PROVISIÓN DE SIETE (7) UNIDADES DE PROCESAMIENTO ESPECIALIZADO (SITE COLLECTORS) DESTINADOS A LA INGESTA, NORMALIZACIÓN Y REENVÍO DE TELEMETRÍA HACIA LA PLATAFORMA SIEM, GARANTIZANDO UNA ARQUITECTURA DE ALTA DISPONIBILIDAD. EL HARDWARE DEBE ASEGURAR EL CUMPLIMIENTO DE LOS NIVELES DE SERVICIO (SLA) DE INGESTA Y PERSISTENCIA DE DATOS DURANTE LA EJECUCIÓN DEL CONTRATO.

LOS COMPONENTES DE INFRAESTRUCTURA LOCAL DEBERÁN GARANTIZAR EL RENDIMIENTO ÓPTIMO, ESTABILIDAD Y DISPONIBILIDAD REQUERIDOS PARA LA OPERACIÓN CONTINUA DE LAS CAPACIDADES DE SIEM, SOAR Y UEBA, BAJO LOS SIGUIENTES CRITERIOS.

ESPECIFICACIONES TÉCNICAS MÍNIMAS DE LOS COLECTORES ON-PREMISE:

- **SISTEMA OPERATIVO:** DISTRIBUCIÓN LINUX DE GRADO EMPRESARIAL LICENCIADO DEBIDAMENTE ENDURECIDA (HARDENED), CON ACTUALIZACIONES DE SEGURIDAD GESTIONADAS Y SOPORTE TÉCNICO DIRECTO DEL OFERENTE.

- **PROCESAMIENTO (CPU):** PROVISIÓN DE UN MÍNIMO DE 16 NÚCLEOS FÍSICOS (16 CORES) CON UNA FRECUENCIA BASE DE 2.8 GHZ O SUPERIOR. LA ARQUITECTURA DE LA PLACA BASE (MOTHERBOARD) DEBE SER DE DOBLE ZÓCALO (DUAL SOCKET), PERMITIENDO LA EXPANSIÓN FUTURA DE LA CAPACIDAD DE CÓMPUTO MEDIANTE LA INSTALACIÓN DE UN SEGUNDO PROCESADOR DE SIMILARES O SUPERIORES CARACTERÍSTICAS, GARANTIZANDO LA PROTECCIÓN DE LA INVERSIÓN Y LA ESCALABILIDAD DEL PROCESAMIENTO DE LOGS EN SITIO.

- **MEMORIA RAM:** MÍNIMO DE 32 GB DE MEMORIA DE ALTA VELOCIDAD CON TECNOLOGÍA DDR5 (O LA ÚLTIMA GENERACIÓN DISPONIBLE EN EL MERCADO AL MOMENTO DE LA ENTREGA). LA ARQUITECTURA DEL COLECTOR DEBE SER ESCALABLE, PERMITIENDO UNA EXPANSIÓN DE MEMORIA DE HASTA 256 GB MEDIANTE RANURAS DIMM DISPONIBLES, GARANTIZANDO ASÍ LA CAPACIDAD DE RESPUESTA ANTE INCREMENTOS MASIVOS EN EL VOLUMEN DE INGESTA DE DATOS Y PROCESOS DE CORRELACIÓN EN MEMORIA.

- **ALMACENAMIENTO:** MÍNIMO DE 1 TB DE CAPACIDAD EN UNIDADES DE ESTADO SÓLIDO (SSD) DE ALTO RENDIMIENTO O EQUIVALENTE. LA ARQUITECTURA DE ALMACENAMIENTO DEBERÁ ESTAR CONFIGURADA MEDIANTE UN ARREGLO DE DISCOS REDUNDANTE (RAID) QUE GARANTICE LA INTEGRIDAD DE LOS DATOS Y LA TOLERANCIA ANTE FALLAS FÍSICAS DE LAS UNIDADES, ASEGURANDO LA CONTINUIDAD DE LA PERSISTENCIA LOCAL DE LA TELEMETRÍA.

- **REDUNDANCIA ENERGÉTICA:** EL HARDWARE DEBERÁ CONTAR CON FUENTES DE PODER REDUNDANTES Y EXTRAÍBLES EN CALIENTE (HOT-SWAP) DE ALTA EFICIENCIA. ESTA CONFIGURACIÓN DEBE PERMITIR QUE EL EQUIPO MANTENGA SU OPERACIÓN ININTERRUMPIDA ANTE LA FALLA DE UNO DE LOS MÓDULOS DE POTENCIA, GARANTIZANDO EL CUMPLIMIENTO DE LOS NIVELES DE DISPONIBILIDAD DE INGESTA Y PROCESAMIENTO EXIGIDOS EN EL SLA.

- **CONECTIVIDAD DE RED:** PROVISIÓN DE UN MÍNIMO DE DOS (2) INTERFACES FÍSICAS INDEPENDIENTES GIGABIT ETHERNET (10/100/1000 MBPS) O SUPERIOR. LAS INTERFACES DEBERÁN CONTAR CON SOPORTE NATIVO PARA REDUNDANCIA FÍSICA Y CONFIGURACIONES SEGURAS DE AGREGACIÓN DE ENLACES (BONDING/LACP). ESTA ARQUITECTURA DEBE GARANTIZAR LA CONTINUIDAD DE LA COMUNICACIÓN Y EL BALANCEO DE CARGA DE LA

	TELEMETRÍA, ASEGURANDO QUE LA FALLA DE UN PUERTO O ENLACE NO INTERRUMPA EL FLUJO DE DATOS HACIA LA PLATAFORMA SIEM. **SOPORTE Y GARANTIA**: EL OFERENTE DEBERÁ GARANTIZAR UNA COBERTURA DE SOPORTE TÉCNICO Y GARANTÍA DE HARDWARE POR UN PERIODO MÍNIMO DE 36 MESES, CONTADOS A PARTIR DE LA FIRMA DEL ACTA DE ACEPTACIÓN TÉCNICA A SATISFACCIÓN. LA COBERTURA DEBE INCLUIR EL MANTENIMIENTO PREVENTIVO PROGRAMADO Y CORRECTIVO ILIMITADO, ASEGURANDO LA RESOLUCIÓN DE CUALQUIER FALLA FÍSICA O LÓGICA QUE AFECTE LA OPERACIÓN DE LOS COLECTORES.	
	11.	

	12. CANAL DE COMUNICACIÓN	CUMPLE NO CUMPLE
	11 CERTIFICACIÓN DEL FABRICANTE	CUMPLE NO CUMPLE

	13. TRANSFERENCIA DE CONOCIMIENTO	CUMPLE / NO CUMPLE

HERRAMIENTA PARA LA GESTIÓN Y EL ESCANEO DE VULNERABILIDADES DE UN MINIMO DE 600 ACTIVOS POR TRES (03) AÑOS, CUYOS RESULTADOS SIRVAN COMO INSUMO TÉCNICO PARA OPTIMIZAR LOS PROCESOS DE CORRELACIÓN DEL SIEM, PRIORIZACIÓN Y MEJORA CONTINUA DENTRO DEL ECOSISTEMA INTEGRAL DE CIBERSEGURIDAD INSTITUCIONAL

	14. ESCANER DE VULNERABILIDADES	CUMPLE / NO CUMPLE

CLÁUSULA OFFSET.

De conformidad con el Decreto 1001 de 2025, "Por el cual se reglamenta el Artículo 257 de la Ley 2294 de 2023 - Plan Nacional de Desarrollo 2022-2026, respecto de las compensaciones industriales en materia de Defensa Nacional", cuyo objeto establece "las Compensaciones Industriales en el marco de las compras públicas de naturaleza militar y del Sector Defensa de que trata el artículo 257 de la Ley 2294 de 2023 y establece un modelo de gobernanza para su operación" y en concordancia con la Resolución No. 001767

de 2025 "Por la cual se adopta la Política Sectorial para la implementación de Acuerdos de Cooperación Industrial y Social - OFFSET, relacionados con adquisiciones para. El Sector Defensa y Seguridad en Colombia", el Ministerio de Defensa Nacional exigirá la cooperación industrial y social a los proveedores extranjeros en los contratos cuyo objeto sea la adquisición de bienes para uso militar, equipos y sistemas de armas destinados a la defensa y seguridad nacional, incluyendo aquellos bienes y servicios asociados a su sostenimiento y mantenimiento durante su Ciclo de vida, siempre que el monto supere los USD 3.000.000 (tres millones de dólares) o su equivalente en otras monedas.

El contratista se obliga a suscribir cuando la Armada Nacional lo indique el Convenio Marco de Cooperación Industrial y Social - OFFSET, el cual será mínimo del 100% de compensación sobre el valor total del contrato y sus adicciones.

La entidad cuenta con la potestad de incluir medidas de tipo sancionatorias y/o conminatorias para el cumplimiento de los convenios marcos y derivados, en caso de retrasos o incumplimientos.

Así mismo, el contratista deberá tener en cuenta que la multa por la no suscripción del Convenio Marco, no será inferior al 5%.

Atentamente,

ORIGINAL FIRMADO
Capitán de Navío **LUIS ALONSO RAMÍREZ GUERRERO**
Gerente de Proyecto
RESERVADO

CF GARCÍA RUÍZ JUAN CARLOS CAMILO

TF BONZA SANCHEZ LISSETH PAOLA

TK BENAVIDES MAHECHA LUIS HERNANDO

S1 OCAMPO HERRERA JOAN MANUEL

PD25 PRIETO HERNANDEZ WILSON ARTURO

ESTRUCTURADOR TÉCNICO