ANEXO TÉCNICO
SOSTENIMIENTO APLICATIVO HYDRA

CONTENIDO

1. OBJETO 2
2. DEFINICIONES Y APLICACIÓN 2
3. REQUISITOS....4
4. TOMA DE MUESTRAS Y CRITERIO DE ACEPTACIÓN O RECHAZO: 20
5. MÉTODOS DE ENSAYO 20
6. APÉNDICE 20
7. ANEXOS 21
8. CONTROL DE REVISIONES 21

Elaboró	Revisó	Aprobó
ORIGINAL DEBIDAMENTE FIRMADO ********** Comité Técnico Estructurador		
ORIGINAL DEBIDAMENTE FIRMADO ********** Comité Técnico Estructurador	**ORIGINAL DEBIDAMENTE FIRMADO** ********** **Oficial de Comunicaciones del CAIMI**	**ORIGINAL DEBIDAMENTE FIRMADO** ********** Jefe De Estado Mayor CAIMI

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

1. OBJETO

El presente Anexo Técnico tiene como objeto establecer los requisitos técnicos para el sostenimiento y transición evolutiva que tiene el aplicativo HYDRA hacia una nueva tecnología vanguardista con la implementación de semántica (LLM) siendo para el SICIE un nuevo sistema denominado JANUS. Sin perder la funcionalidad que tiene actualmente HYDRA con la incorporación de una inteligencia artificial (IA).

En los últimos años, la aplicación HYDRA ha experimentado una serie de transiciones tecnológicas, evolucionando hacia la implementación de modelos de aprendizaje automático. Dado que HYDRA opera como un motor de búsqueda, se hizo necesario actualizar su infraestructura para apoyar el desarrollo y la implementación de estos modelos avanzados. Esta actualización tecnológica es clave para que la aplicación pueda seguir siendo eficiente y competitiva en el campo de la inteligencia artificial y el procesamiento de grandes volúmenes de datos.

En 2025, se realizó una importante inversión bajo el contrato 003-CEDE2-2025, cuyo objetivo fue la adquisición de equipos de cómputo de última generación, diseñados específicamente para soportar los requisitos de los nuevos modelos de aprendizaje automático. Esta inversión permitió un cambio fundamental en la infraestructura de la aplicación, sentando las bases para lo que será la nueva fase de su evolución tecnológica. A partir de esta vigencia, HYDRA se renombrará como JANUS, lo que simboliza el inicio de una etapa más avanzada en la integración de Inteligencia Artificial de Nivel 3.

Este cambio no solo refleja la necesidad de adaptarse a las tecnologías emergentes, sino que también tiene como objetivo ofrecer a los funcionarios del SICIE una herramienta más poderosa y precisa para el análisis y la toma de decisiones. La integración de una IA de Nivel 3 permitirá que JANUS maneje tareas más complejas, como el análisis predictivo, la personalización avanzada de resultados de búsqueda, y la mejora en la precisión de los datos procesados.

La optimización de los recursos actuales y el desarrollo adaptativo serán corregidos y tendrán una evolución por medio del sostenimiento, el cual buscan garantizar la continuidad operativa, la disponibilidad, integridad y confidencialidad de la información, alineándose con los estándares de seguridad de la información ISO 27001:2022 que cuenta el SICIE. Además, es fundamental preparar la plataforma para la integración de la Inteligencia Artificial (IA), para optimizar tiempos de análisis y facilitar la toma de decisiones estratégicas y operacionales, que en gran medida apoyan la labor del analista, vital para afrontar los retos en seguridad y defensa en el marco de la Ley Estatutaria 1621 del 2013.

2. DEFINICIONES Y APLICACIÓN

2.1 DEFINICIONES

LINUX: Un sistema operativo de computadora similar a Unix ensamblado bajo el modelo de desarrollo y distribución de software libre y de código abierto. Linux es un sistema

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

operativo líder en servidores, computadoras centrales, supercomputadoras y sistemas integrados como teléfonos móviles, tabletas, enrutadores de red, televisores y consolas de videojuegos. Las principales distribuciones de Linux empresarial son OEL, Ubuntu, RHEL, SLES y Debian.

NODO: Dispositivo conectado a una red de ordenadores. En una red de área local, un nodo es un dispositivo que está conectado a la red y es capaz de comunicarse con otros dispositivos de la misma red.

BIG DATA: Gestión, almacenamiento y análisis de enormes volúmenes de información que no pueden ser tratados de manera convencional. Se habla usualmente en términos de Peta bytes y superiores.

LICENCIA DE CÓDIGO ABIERTO (OPEN SORCEN): Es una licencia de software que permite que tanto el código fuente como los archivos binarios sean modificados y redistribuidos libremente y sin tener que pagar al autor original. Sin embargo, ciertas licencias de código abierto pueden incorporar algunas restricciones, como el requisito de mantener el nombre de los autores y la declaración de derechos de autor en el código, o permitir la modificación del código sólo para usos personales o la redistribución del software para usos no comerciales.

CLÚSTER: Conjuntos o conglomerados de computadoras construidos mediante la utilización de componentes de hardware comunes y que se comportan como si fuesen una única computadora.

KERBEROS: Es un protocolo de autenticación de redes de ordenador creado por el MIT que permite a dos o más entidades en una red insegura demostrar su identidad mutuamente de manera segura.

SOSTENIMIENTO: Se refiere a la acción o efecto de sostener o de sostenerse, un Conjunto de recursos necesarios para manter o mantenerse. Conservación.

CONTENEDOR: Conjunto de procesos aislados del resto del sistema, para los cuales los archivos necesarios para su ejecución son proveídos en una imagen, brindando características de portabilidad y consistencia para ambientes de desarrollo, pruebas y producción.

DOCKER: Software que permite crear, ejecutar y en general gestionar contenedores, a diferentes escalas y de manera segura.

KUBERNETES: Sistema de código abierto para el despliegue, escalamiento y administración de aplicaciones contenerizadas.

DIAGNÓSTICO TÉCNICO: Este proceso debe permitir el aseguramiento de la infraestructura de tecnología adecuada para soportar y facilitar el correcto funcionamiento de los servidores, bases de datos, accesibilidad, seguridad, redundancia y contingencia.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

RECURSO: Dentro del ámbito de sistemas, entiéndase como persona o recurso ofrecido por el contratista, el cual presta el servicio objeto del presente contrato, soportado con las certificaciones solicitadas en la presente ficha, pero no limita a que sea ingeniero de sistemas, puede ser técnico o tecnólogo que tenga las capacidades que se requieren para el cumplimiento del objeto del contrato.

INTELIGENCIA ARTIFICIAL (AI): La inteligencia artificial es un campo de la ciencia relacionado con la creación de computadoras y máquinas que pueden razonar, aprender y actuar de una manera que normalmente requeriría inteligencia humana o que involucra datos cuya escala excede lo que los humanos pueden analizar.

2.2 APLICACIÓN

Consiste en la adquisición de los servicios de sostenimiento del aplicativos, despliegue, afinamiento de servicios, configuración lógica de servidores y gestión de almacenamiento de una Infraestructura Big Data, servicios de integración y componentes bajo tecnologías de contenedores y orquestación de tal manera que sea posible asegurar la información y gestionar grandes volúmenes de datos de inteligencia, que debido a su volumen, variedad y velocidad no pueden ser tratados de manera convencional, permitiendo lo anterior avanzar en el desarrollo de aplicaciones y servicios útiles para toma de decisiones estratégicas y operacionales.

Conllevando a nuevas tecnologías e implementando la inteligencia artificial para la optimización de tiempos y así tener un análisis, facilitando para la toma de decisiones y en operaciones de relevancia.

3. REQUISITOS

3.1 REQUISITOS GENERALES

Este servicio tiene como objetivo garantizar el sostenimiento, la optimización y la evolución del aplicativo JANUS, el cual se encuentra integrado al orquestador de servicios para el procesamiento masivo de datos y constituye una plataforma base para el desarrollo e implementación de modelos de analítica avanzada e inteligencia artificial. JANUS integra recursos Open Source dispuestos en el clúster del aplicativo, sobre un entorno basado en tecnologías Kubernetes, permitiendo la escalabilidad, disponibilidad y eficiencia requeridas para cargas de trabajo asociadas a IA y aprendizaje automático.

El soporte aplicativo permitirá asegurar la estabilidad operativa, el rendimiento y la correcta integración de componentes necesarios para el procesamiento, entrenamiento y ejecución de algoritmos de inteligencia artificial, garantizando la entrega de información con eficiencia y rapidez a los funcionarios que realizan búsquedas y análisis en el sistema. Esto fortalecerá las capacidades analíticas, agilizando la consulta, correlación y recolección de información relevante para la producción de inteligencia.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

3.2 REQUISITOS ESPECÍFICOS

ÍTEM	DESCRIPCIÓN
3.2.1	**ADMINISTRACIÓN Y FUNCIONAMIENTO DEL APLICATIVO JANUS**
3.2.1.1	El contratista garantizara el sostenimiento, Mantenimiento, actualización, evolución e implementación de inteligencia artificial en entornos open source – aplicativo janus, que en la actualidad tiene disponible el Subsistema de Inteligencia y Contrainteligencia del Ejército Nacional del (SICIE), garantizando la realización de las siguientes actividades, así: • Implementar capacidades de Inteligencia Artificial (IA) integradas a la infraestructura Open Source del aplicativo JANUS, con el fin de automatizar tareas de monitoreo, diagnóstico, optimización de recursos, gestión de seguridad y soporte predictivo en entornos Kubernetes, fortaleciendo la continuidad operativa del Subsistema de Inteligencia y Contrainteligencia del (SICIE). • Optimizar el sostenimiento del clúster Kubernetes, detectando de forma proactiva fallos, consumos anómalos y brechas de seguridad. • Disminuir tiempos de respuesta para recuperación ante incidentes, parches y ajustes de configuración. • Asegurar la interoperabilidad y escalabilidad de los servicios contenerizados del CAIMI bajo estándares de seguridad y alta disponibilidad. • Integrar tecnologías Open Source y herramientas de IA que faciliten la toma de decisiones estratégicas. • Aplicará a la infraestructura actual del clúster JANUS, abarcando nodos, pods, volúmenes persistentes, conectividad, cifrado de datos y autenticación. • Comprenderá tareas preventivas, correctivas y adaptativas, con despliegues rutinarios y automatización de procesos críticos. • Implementación de módulos IA entrenados para análisis de logs, predicción de fallas, optimización de uso de recursos y monitoreo de seguridad. • Integración directa con Kerberos y RBAC para autenticación robusta de usuarios, servicios y contenedores. • Aislamiento, diagnóstico y corrección de errores en el producto Kubernetes (open source). • Recuperación de fallas y solución de problemas en el producto Kubernetes (open source). • Garantizar la configuración de características de alta disponibilidad sobre el clúster Kubernetes. • Tolerancia a fallos de los pods: Uso de ReplicaSets o DaemonSets para asegurar múltiples réplicas. • Supervisar y mantener la herramienta de monitoreo existente (Grafana) y establecer alertas para detectar problemas en el clúster, como falta de disponibilidad de nodos o agotamiento de recursos. • Realizar una revisión exhaustiva de volúmenes persistentes obsoletos. • Garantizar la configuración de las características de gestión de recursos sobre el clúster Kubernetes. • Gestionar los límites óptimos del consumo de recursos por parte de los contenedores (actualizaciones de valores). • Mejorar el uso de etiquetas para los objetos Kubernetes. • Maximizar el número de solicitudes procesadas por la API en paralelo. • Automatizar procesos de copias de seguridad y restauración (DR) y migrar la información del clúster (volúmenes persistentes). • Reforzar la Integración Continua y Despliegue Continuo (CI/CD) con tecnologías open source. • Garantizar la Interoperabilidad con otras tecnologías y aplicaciones del SICIE. • Actividades relacionadas con procesamiento por lotes distribuido de grandes conjuntos de datos, programación de trabajos, gestión de recursos, coordinación de

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

aplicaciones distribuidas, administración del ecosistema Kubernetes, uso de Kubegres operator, gestión de claves criptográficas, almacén de datos orientado a columnas, y plataforma de búsqueda empresarial.

- Revisar, validar e implementar cambios para la adecuada gestión de roles y privilegios sobre el clúster JANUS open source en Kubernetes (RBAC, Kerberos).
- Validar e implementar mecanismos de cifrado para proteger los datos en reposo y en tránsito, incluyendo rotación de claves.
- Realizar pruebas en un laboratorio controlado, migrando de CentOS 7 a Ubuntu Server, y documentar el proceso, pruebas funcionales y resultados para evaluar riesgos y repercusiones en Janus.

Componentes Técnicos.

Componente	Descripción
Modelo IA	Algoritmos supervisados para clasificación de errores comunes y clustering no supervisado para detección de anomalías en uso de recursos y comportamiento de nodos/pods.
Orquestación	Despliegue de IA contenerizada en Kubernetes, configurada con tolerancia a fallos (ReplicaSets, DaemonSets) y alta disponibilidad.
Seguridad	Integración con Kerberos para autenticación y RBAC para control granular de acceso. Implementación de cifrado de datos en reposo y en tránsito, con rotación de claves.
Monitoreo Predictivo	Módulos que analicen métricas del clúster (CPU, disco, memoria) y generen alertas automáticas y acciones correctivas.
Automatización	Scripts y pipelines CI/CD reforzados para despliegue continuo de parches, rotación de logs, copias de seguridad DR y restauración automatizada.
Interfaz	Dashboard centralizado para visualización de métricas IA, reportes de diagnóstico, estado de seguridad y recomendaciones automatizadas.

Fases del Proyecto.

Fase 1: Diagnóstico y Planeación.

- Levantamiento de requerimientos técnicos específicos para el clúster JANUS.
- Definición de métricas clave de rendimiento, seguridad y disponibilidad.
- Validación de interoperabilidad con el bus de integración y base de datos SICIE.

Fase 2: Evolución y Entrenamiento de la IA.

- Entrenamiento de modelos IA con datos históricos de logs, métricas de consumo y registros de fallos.
- Simulación de escenarios críticos (falla de nodos, sobreconsumo de recursos, errores de configuración).
- Validación de algoritmos de clustering para segmentación de eventos y detección de comportamientos atípicos.

Fase 3: Despliegue Controlado.

- Implementación de módulos IA contenerizados dentro del clúster Kubernetes.
- Pruebas funcionales en laboratorio controlado, migración controlada de CentOS 7 a Ubuntu Server y documentación técnica.
- Configuración de integración con Kerberos y RBAC, monitoreo de seguridad y cifrado de datos.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

	Fase 4: Operación y Optimización. • Monitoreo activo de recursos del clúster, generación de alertas automáticas y parches proactivos. • Evaluación continua de volúmenes obsoletos, límites de consumo y uso de etiquetas para gestión eficiente. • Automatización de backups DR y restauración. • Validación de rendimiento, seguridad y escalabilidad. Entregables Clave • Diagnóstico inicial y plan de acción técnico-operativo. • Modelos IA entrenados y documentación técnica. • Dashboards de monitoreo con alertas y reportes automáticos. • Procedimientos operativos estándar actualizados. • Documentación de integración con tecnologías de terceros, Kerberos y RBAC. • Plan de pruebas y resultados de validación de seguridad (penetration test inicial y final). • Plan antidesastres del aplicativo. • Diagnóstico final con hallazgos mitigados y recomendaciones para escalamiento. Seguridad de la Información • Implementación de cifrado de datos en reposo y en tránsito, rotación de claves periódica. • Proceso de autenticación robusto mediante Kerberos. • Control de acceso granular con RBAC. • Supervisión permanente de logs, configuración de alertas y políticas de auditoría conforme a ISO 27001 del 2022. Este proyecto fortalecerá la resiliencia, seguridad y eficiencia operativa del clúster JANUS, asegurando la evolución de sus servicios contenerizados con inteligencia artificial Open Source, cumpliendo estándares de alta disponibilidad, seguridad y automatización.
3.2.2	**DESARROLLO FULL STACK DEL APLICATIVO JANUS**
3.2.2.1	Deberá ser prestado para el sostenimiento del aplicativo JANUS, que en la actualidad tiene disponible el Subsistema de Inteligencia y Contrainteligencia del Ejército (SICIE), para complementar y reforzar las capacidades de Inteligencia Artificial (IA), Big Data, contenerización y seguridad avanzada, certificando la realización de las siguientes actividades, las cuales se debe aplicar la metodología de desarrollo seguro que tenga la entidad (MDAS) regida por Metodología Owasp Testing Guide V4.0, , garantizando la continuidad operativa y la resiliencia del Subsistema de Inteligencia y Contrainteligencia del Ejército (SICIE). A) Se deberá realizar el sostenimiento Adaptativo con Inteligencia Artificial y Big Data. Este tipo de sostenimiento consiste en la modificación del software para ajustarlo a los lineamientos y buenas prácticas del framework Angular, creando una interfaz de usuario escalable e implementable de manera ágil y limpia, contemplando como mínimo las siguientes actividades, así: • Modificación del software para ajustarse a los lineamientos y buenas prácticas del framework Angular, creando una interfaz de usuario escalable, ágil y limpia. • Actualizar versiones de artefactos de desarrollo (ej. Dropwizard 4.0.6, PostgreSQL JDBC 42.7.3, SolrJ 8.11.2, HttpClient 4.5.14, Hadoop 3.3.6, HBase 2.4.17, Kafka Clients 3.7.0, Jackson-databind 2.17.1, etc.). • Optimización del front-end: Corrección de errores, mejoras de capacidades, eliminación de funciones obsoletas e implementación de buenas prácticas. • Despliegue de modelos de IA generativa y predictiva, integrados en contenedores para operación en entornos Kubernetes. • Ejecución de pruebas de penetración (inicial y final), auditorías de código y sanitización de vulnerabilidades.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

- Implementación de IA: Utilizar modelos de inteligencia artificial para predecir y prevenir problemas de rendimiento y seguridad.
- Contenerización de los nuevos desarrollos implementados de IA generativa para integrarlos al clúster JANUS y mantener la contabilidad de la solución con las herramientas existentes en Kubernetes.
- Documentación técnica y operativa actualizada bajo normas ISO 27001.
- Migración del código el cual se encuentra en el repositorio del gitlab
- Sostenimiento, mantenimiento y adaptación a nuevas tecnologías de las aplicaciones del SICIE con la data lake de la entidad.
- Creación o actualización de las Apis existentes o necesarias para el desarrollo de las actividades de integración con las aplicaciones del SICIE.
- Se deberá de hacer implementación del mínimo de un frameworks representativo como ejemplo el de Amazon, Facebook etc.

B) Se deberá realizar el sostenimiento perfectivo. Es el conjunto de actividades para mejorar o añadir nuevas funcionalidades requeridas por el usuario o la administración de la plataforma, contemplando como mínimo las siguientes actividades, así:

- Incorporación de nuevas funcionalidades (ej. evolución de un módulo de **IA generativa** en formato de asistente tipo chat).
- Pruebas de validación al nuevo módulo desarrollado para ingreso a etapa productiva.
- Creación de repositorio privado en Nexus para blindar el módulo.
- Despliegue del módulo desarrollado dentro del clúster de Microk8s de JANUS en producción.
- Actualización tecnológica: Actualizar versiones de artefactos del framework Angular, bibliotecas y dependencias.
- Optimización del front-end: Refactorizar componentes para mejorar rendimiento, usabilidad y seguridad.
- Remediación de vulnerabilidades: Ejecutar revisiones de seguridad en código conforme a OWASP Testing Guide V4.0.
- Integración de IA: evolucionar y desplegar modelos de IA para detección de fallas, anomalías de rendimiento y brechas de seguridad.
- Análisis Big Data: Incorporar herramientas de Big Data para minería de datos, monitoreo de patrones de uso y personalización de experiencia.
- Contenerización: Empaquetar los nuevos módulos IA generativa en contenedores Docker, integrarlos al clúster JANUS y garantizar su orquestación en Kubernetes.

C) Se deberá realizar e implementar la seguridad Cluster Kubernetes, donde se debe realizar dos pruebas de penetración (Inicial- final) en la cual se evidencien las vulnerabilidades encontradas y finalmente la sanitización de las mismas de la siguiente manera:

- Dos pruebas de penetración (inicial y final) al aplicativo JANUS y sus herramientas, identificando vulnerabilidades y presentando un plan de mejora y su mitigación, aplicando las siguientes actividades:

  - Capa aplicación
  - Capa red
  - Roles autorizados/no-autorizados
  - Aplicaciones contenerizadas
  - Identificación de sistemas críticos

- Evaluación de seguridad en capa de aplicación, red, por roles (autorizados/no-autorizados), aplicaciones contenerizadas, e identificación de sistemas críticos.
- Verificación periódica de la arquitectura del sistema e implementación/configuración de un sistema de monitoreo de registros.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

- Realización de actividades de seguridad bajo supervisión del contrato.
- Identificación de problemas o mejoras para la implementación de productos, tecnologías y/o alternativas de seguridad en los productos open source.
- Dos pruebas (inicial y final) automatizadas o manuales al código fuente de la aplicación para determinar posibles vulnerabilidades.
- Plan de Mejora de Seguridad: Anexar al diagnóstico inicial y actualizar tras mitigación de hallazgos.
- Sanitización: Documentar la solución de vulnerabilidades en diagnóstico final, máximo dos meses antes del cierre contractual.
- Suministro y Renovación SSL: Suministrar y Renovar y validar certificados SSL de JANUS y sus microservicios contenerizados, por el periodo del contrato.
- Monitoreo: Configurar sistemas de registro y auditoría permanente, alineados con ISO 27001 del 2022.
- Análisis de código: Ejecutar escaneo automatizado y manual de código fuente (inicial y final) para detectar vulnerabilidades.
- Verificación periódica: Revisar arquitectura, configuraciones y cumplimiento de políticas de acceso (Kerberos, RBAC).

D) Se deberá realizar la respectiva calidad de código y pruebas funcionales, contemplando como mínimo las siguientes actividades, así:

Calidad del Código: Funciona, pero se debe certificar en entornos de alto estrés realizando las respectivas pruebas.

Pruebas Unitarias: No se han implementado pruebas unitarias para validar la lógica de negocio. Jenkins no presenta configuración activa para automatización de pruebas.
Vulnerabilidades de Código:

- Frontend (Angular): 14 vulnerabilidades detectadas en compilación local (2 bajas, 4 moderadas, 8 altas), incluyendo inyección de dependencias y Cross-Site Scripting (XSS).
- Backend (Spring Boot/Java): Vulnerabilidades potenciales incluyen inyección SQL, autenticación/autorización insuficiente, configuración insegura, exposición de información sensible, falta de validación de entrada (XSS, CSRF), dependencias vulnerables, fugas de información por APIs mal configuradas, y problemas de CORS.

VISIÓN DE LA TRANSFORMACIÓN Y PLAN DE MODERNIZACIÓN (TO-BE).

El objetivo general es modernizar JANUS para que entienda, analice y recomiende información como lo haría un analista humano con entrenamiento en inteligencia. Esto transformará a JANUS de un archivador digital a un asistente virtual de inteligencia.

Componente	Situación Actual (AS-IS)	Acción de Modernización (TO-BE)
Angular	Obsoleto (v10/11)	**Actualizar a Angular 17+ (LTS)**
Backend	Monolítico (Java 8/11, Dropwizard)	**Reestructurar a microservicios**, actualizar Java a 17 LTS, Spring Boot 3.x, Dropwizard 4.x
Base de datos	Relacional rígida (PostgreSQL 13.2)	**Rediseño con vistas + vectorización**, PostgreSQL 15+, autenticación SCRAM-SHA-256, SSL/TLS
Servicios IA	IA Basica, sin entrenamiento.	**Crear un AI Gateway**, con conexión directa a modelos LLM y clasificadores
Trazabilidad	Logs simples	**Implementar trazabilidad avanzada** y monitoreo completo (Grafana, Prometheus, ELK)

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

	Seguridad	Autenticación débil, sin WAF/mTLS	**WAF, mTLS**, autenticación fuerte + auditoría, análisis estático de código (SAST)
	Infraestructura	Contenedores sin hardening, sin observabilidad	**Kubernetes seguro**, redes privadas, logs centralizados, AlertManager

ENTREGABLES.

- Diagnóstico inicial (pentesting, plan de mejora de seguridad y cronograma).
- Modelos IA entrenados y contenedorizados.
- Repositorio Nexus privado con módulos blindados.
- Informe Dashboards de monitoreo y reportes automáticos diarios enviando al supervisor del contrato.
- Certificados SSL renovados.
- Plan de pruebas de seguridad inicial y final.
- Diagnóstico final evidenciando hallazgos mitigados.
- Manuales de operación, POEs y documentación de integración Kerberos/RBAC.

3.2.3	**DOCUMENTACIÓN Y REQUERIMIENTOS GENERALES**
3.2.3.1	DIAGNÓSTICO TÉCNICO INTEGRAL DE LA INFRAESTRUCTURA TECNOLÓGICA El contratista deberá realizar un diagnóstico técnico integral de la infraestructura tecnológica, abarcando tanto la arquitectura y estado del hardware como la arquitectura y estado del software. Este diagnóstico deberá llevarse a cabo durante las dos primeras semanas posteriores al inicio de la ejecución del contrato y tendrá como objetivo recopilar información precisa y detallada para garantizar la ejecución efectiva de las actividades contratadas, permitiendo una optimización continua del entorno tecnológico, realizando las siguientes actividades al inicio y al final del contrato. Durante el diagnóstico, se deberá realizar un análisis exhaustivo de cada uno de los servicios, roles y componentes que conforman el Clúster, con los siguientes sostenimientos así: **SOPORTE TÉCNICO** • Identificación y clasificación de posibles fallos que puedan afectar la operatividad de los sistemas críticos. • Evaluación del rendimiento actual de la infraestructura y propuesta de optimización en consumo de recursos. • Identificación de necesidades de mantenimiento preventivo y correctivo para garantizar la estabilidad de los aplicativos. • Validación de niveles de servicio (ANS) y cumplimiento de tiempos de respuesta en incidentes y soporte. • Inspección de la capacidad de procesamiento, memoria y almacenamiento de los servidores. • Verificación de redundancia y escalabilidad para asegurar continuidad operativa y mitigación de fallos. • Análisis del estado físico de los equipos, incluyendo temperatura, ventilación, energía y otros factores ambientales críticos. • Diagnóstico de posibles cuellos de botella en la infraestructura tecnológica. • Identificación y documentación de las versiones de software instaladas y su compatibilidad con los sistemas en operación. • Análisis de estabilidad, tiempos de respuesta y optimización de recursos del software en producción. • Cumplimiento de requisitos funcionales y operativos de los aplicativos dentro del entorno tecnológico. • Identificación de posibles problemas de obsolescencia o incompatibilidad con nuevas tecnologías.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

- Definición de un plan de acción para la actualización de versiones y aplicación de parches de seguridad.
- Evaluación de mejoras en el rendimiento del software y hardware, priorizando soluciones de alta disponibilidad y escalabilidad.
- Análisis de compatibilidad con nuevas tecnologías que optimicen la operación y la seguridad.
- Identificación de herramientas de automatización y monitoreo para mejorar la eficiencia del mantenimiento.
- Se deberá realizar diariamente el monitoreo de las aplicaciones que conforman el aplicativo JANUS, generando un informe diario al supervisor del contrato del estado funcional.
- Se deberá realizar diariamente el monitoreo del gitlab de las aplicaciones del SICIE, generando un informe diario al supervisor del contrato del estado funcional.
- El contratista deberá de suministrar por tres años los certificados SSL del aplicativo JANUS.
- El contratista deberá suministrar mínimo 3 modelos de LLM diferentes para el aplicativo JANUS, de minino 70 billones.
- El contratista deberá contemplar la implementación de técnicas de ajuste fino (*fine-tuning*) y la generación y utilización de *embeddings* en modelos de inteligencia artificial, con el fin de adaptar el comportamiento del sistema a los requerimientos específicos del dominio y mejorar la precisión, relevancia y contextualización de los resultados.

SEGURIDAD INFORMÁTICA

- Análisis de Vulnerabilidades, identificación de posibles brechas de seguridad en la infraestructura tecnológica, aplicativos y configuraciones.
- Evaluación del cumplimiento de estándares de seguridad alineados con normativas internacionales como ISO 27001.
- Diagnóstico del estado de cifrado de datos y protección de información sensible.
- Prueba de Penetración Inicial, simulación de ataques internos y externos para evaluar la capacidad de respuesta de la infraestructura ante amenazas cibernéticas.
- Revisión de políticas de protección contra malware, ransomware y accesos no autorizados.
- Revisión de Políticas de Acceso y Autenticación, evaluación de la gestión de credenciales y aplicación de políticas de contraseñas seguras.
- Implementación y/o mejora de mecanismos de autenticación multifactor.
- Control y auditoría de privilegios de usuarios para minimizar riesgos de acceso no autorizado.
- Análisis de Logs y Monitoreo de Eventos, validación de la existencia y efectividad de los sistemas de auditoría y detección de incidentes.
- Implementación de estrategias de monitoreo proactivo para la identificación temprana de amenazas.
- Definición de procedimientos para la respuesta a incidentes de seguridad.
- Estado y Configuración de Sistemas de Respaldo y Recuperación, evaluación de la integridad y disponibilidad de los sistemas de respaldo de información.
- Validación de tiempos de recuperación ante fallos críticos.
- Pruebas de restauración de datos para garantizar la efectividad de los planes de contingencia.

DOCUMENTACIÓN DEL DIAGNÓSTICO Y PLAN DE ACCIÓN.

El resultado del diagnóstico técnico integral deberá documentarse en un informe detallado que incluya:

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

	• Hallazgos técnicos identificando deficiencias y oportunidades de mejora en hardware, software y seguridad informática. • Recomendaciones y plan de acción, estableciendo un cronograma de actividades con prioridades y responsables para la implementación de mejoras. • Esquemas y diagramas actualizados de la infraestructura, reflejando la arquitectura tecnológica y los cambios necesarios para optimizar su funcionamiento. • Indicadores de gestión para medir la evolución de la infraestructura tecnológica y validar la implementación efectiva de las recomendaciones. • Este diagnóstico servirá como base para la planificación y ejecución eficiente del mantenimiento, garantizando la estabilidad, seguridad y operatividad continua de los aplicativos y servicios tecnológicos de la entidad. De igual manera, deberán realizar los siguientes documentos entregables mediante el plan de trabajo: **Diagnóstico Técnico Integral Inicial:** Inspección detallada de hardware, software y clúster Kubernetes. Identificación de fallos, cuellos de botella y necesidades de actualización. Evaluación inicial de seguridad: pentest inicial, simulación de ataques y revisión de configuraciones críticas. Emisión de Plan de Acción con hallazgos, diagramas y cronograma validado con Supervisor CAIMI. **Ejecución de actividades de ajuste temprano:** Inicio de corrección de fallos detectados. Implementación de primeras recomendaciones de optimización. Instalación de parches críticos y pruebas de compatibilidad. Configuración de autenticación Kerberos y validación de RBAC inicial. **Desarrollo Adaptativo:** Inicio de actualización de artefactos del framework Angular. Refactorización de componentes front-end críticos. Desarrollo inicial de módulos IA para análisis de logs y predicción de fallos. Integración de scripts de automatización y pipelines CI/CD iniciales. **Pruebas de Módulos IA:** Entrenamiento de modelos IA con datos históricos del clúster. Simulación de escenarios críticos y validación de clustering de anomalías. Integración de Big Data para correlación de eventos y métricas. Avance en contenerización de nuevos módulos. **Sostenimiento Perfectivo:** Desarrollo de módulo de IA Generativa (Asistente Chat). Pruebas funcionales internas del módulo. Configuración de repositorio Nexus privado. Revisión de políticas de acceso y fortalecimiento de autenticación multifactor. **Despliegue Controlado:** Despliegue en laboratorio de los módulos IA contenerizados. Validación de integración con clúster Kubernetes. Renovación inicial de certificados SSL.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

	Configuración de monitoreo de registros y logs centralizados. Pruebas y Ajustes: Pruebas funcionales y de seguridad del módulo IA generativa. Simulación de restauración de datos. Revisión de desempeño de scripts CI/CD. Ajustes a dashboards y reportes automáticos. Despliegue a Producción: Despliegue definitivo del módulo IA generativa en clúster de producción MicroK8s JANUS. Validación de alta disponibilidad y tolerancia a fallos. Revisión de redundancia de nodos y escalabilidad. Pruebas finales de compatibilidad con Kerberos y RBAC. **Monitoreo Activo:** Monitoreo de métricas clave (CPU, memoria, disco). Análisis de logs automatizados por IA. Generación de alertas automáticas. Evaluación de políticas de backup DR. **Validación de Seguridad:** Ejecución de pruebas de restauración de datos. Validación de rotación de claves de cifrado. Auditoría de políticas de acceso. Análisis de cumplimiento ISO 27001. **Pruebas Finales y Pentest Final:** Ejecución de prueba de penetración final (OWASP Testing Guide V4.0). Evaluación de sanitización de vulnerabilidades. Revisión del estado final de cifrado, logs y monitoreo. Diagnóstico Final Técnico Integral. **Cierre y Validación:** Emisión de Diagnóstico Final con hallazgos mitigados. Validación de continuidad operativa, escalabilidad y seguridad. Entrega final de todos los POEs, diagramas, manuales y esquemas. Validación con Supervisor CAIMI. Una vez finalizado el diagnóstico técnico inicial, de acuerdo con la información recopilada y necesidades encontradas, se debe entregar un cronograma en cual se evidencien todas y cada una de las actividades a realizar para el cumplimiento de la totalidad del contrato, este será validado con el supervisor del contrato y ajustado en común acuerdo, durante la primera semana luego del inicio de la ejecución del contrato. El contratista deberá emitir informes mensuales en los cuales se evidencie el avance de las actividades realizadas de acuerdo al cronograma entregado al supervisor del contrato. Una vez realizadas las actividades de sostenimiento y probados cada uno de los servicios y roles de manera satisfactoria, el contratista debe emitir un diagnóstico final de la arquitectura de hardware y software del clúster Open source, en la que además debe resaltar la solución

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

	de cada una de las novedades encontradas en el diagnóstico inicial. Este diagnóstico final será verificado y aprobado por el supervisor del contrato.
3.2.3.2	La ejecución de las actividades de sostenimiento, evolución, implementación de IA y modernización del aplicativo JANUS se regirán por un modelo de planeación y priorización continua y ágil. Este modelo garantizará la atención eficiente de las necesidades operativas y estratégicas del CAIMI, la estabilidad del clúster Kubernetes, la continuidad de los servicios de búsqueda y análisis, y la integración progresiva de capacidades de Inteligencia Artificial, optimizando el uso de la capacidad operativa del contratista. Para tal efecto, las partes adoptarán un road map de ejecución para janus, el cual constituirá el instrumento principal de planeación, seguimiento y control de las actividades técnicas, incluyendo: el sostenimiento del clúster (Kubernetes, contenedores), el desarrollo y despliegue de modelos de IA, las tareas de seguridad (pentesting, hardening), la refactorización de código, y la migración tecnológica (ej. CentOS a Ubuntu). El ROAD MAP será definido, aprobado y actualizado de común acuerdo entre el supervisor y el contratista, con base en la información obtenida durante el levantamiento de los requerimientos. El ROAD MAP deberá contemplar, como mínimo: • La priorización de las actividades a ejecutar. • El alcance funcional y técnico de cada actividad. • La estimación del esfuerzo requerido para su ejecución. • El orden y el cronograma de ejecución, de acuerdo con la capacidad definida. • La duración estimada de cada actividad o conjunto de actividades. La duración del ROAD MAP y sus respectivas actualizaciones, las cuales serán acordadas y expuestas dentro del seguimiento semanal que se realiza a la ejecución del contrato, conforme a la necesidad y al informe elaborado por el contratista durante el levantamiento del requerimiento solicitado (historia de usuario). La inclusión de actividades dentro del alcance del contrato se realizará conforme a la priorización y programación establecidas en el ROAD MAP aprobado durante la reunión de seguimiento. Su ejecución se llevará a cabo de acuerdo con la capacidad disponible y teniendo en cuenta la historia de usuario elaborada para la necesidad priorizada, considerando los recursos asignados y el esfuerzo técnico requerido. Toda actividad que implique adaptación de la funcionalidad, cambios arquitectónicos relevantes, refactorización significativa o requerimientos adicionales no contemplados en el ROAD MAP en ejecución deberá ser objeto de un análisis de impacto técnico y de criticidad, realizado de manera conjunta entre el supervisor y el contratista, previo a su incorporación formal en el ROAD MAP y a su ejecución. El ROAD MAP podrá ser ajustado durante la ejecución del contrato, de común acuerdo entre las partes, con el fin de atender nuevas necesidades institucionales. Dichos ajustes podrán implicar la re-priorización de actividades, la modificación de cronogramas o la redistribución de la capacidad disponible, garantizando en todo momento la continuidad del servicio y el cumplimiento de las obligaciones contractuales.
3.2.4	**PERFILES REQUERIDOS Y EXPERENCIA**
3.2.4.1	EQUIPO DE TRABAJO: El contratista se compromete a garantizar el personal suficiente, idóneo y necesario para la completa ejecución del cumplimiento del contrato, sin que esto genere costo adicional Al momento de la oferta se deberá de anexar en documento independiente una certificación indicando que el oferente cuenta con los perfiles profesionales requeridos y a su vez anexar

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

	los respectivos soportes donde se evidencie las CERTIFICACIONES Y FORMACIÓN REQUERIDA. **DESARROLLO FULL STACK** Se requiere (1) Ingeniero en Sistemas, Electrónica o carreras afines, con experiencia mínima certificada de tres (3) años en desarrollo y soporte técnico, con conocimientos y experiencia comprobada de aplicaciones bajo el framework Angular y Python aplicando buenas prácticas de arquitectura y escalabilidad; actualización y gestión de dependencias y artefactos tales como Dropwizard 4.0.6, PostgreSQL JDBC 42.7.3, Apache SolrJ 8.11.2, Apache HttpClient 4.5.14, Apache Hadoop 3.3.6, Apache HBase 2.4.17, Apache Kafka Clients 3.7.0 y Jackson-databind 2.17.1; optimización de front-end mediante corrección de errores, refactorización y mejora de rendimiento; despliegue e integración de modelos de inteligencia artificial generativa y predictiva contenerizados para su operación en entornos Kubernetes; ejecución de pruebas de penetración, auditorías de código y remediación de vulnerabilidades; migración y gestión de código fuente en repositorios GitLab; creación y actualización de APIs RESTful para integración de sistemas; sostenimiento y evolución tecnológica de aplicaciones integradas con arquitecturas Data Lake; e implementación de frameworks y arquitecturas empresariales basadas en microservicios y patrones escalables de alta disponibilidad, en el ítem 3.2.2 se encuentra la información con las actividades a desarrollar las cuales están enfocadas al sostenimiento de componentes tecnológicos de inteligencia artificial (IA). En consecuencia, el contratista deberá garantizar la disponibilidad de los profesionales necesarios que aseguren la adecuada atención de cada una de las tecnologías involucradas, dando cumplimiento a los niveles de servicio y a las actividades definidas en el anexo técnico. **GESTION Y ANALISIS DE REQUERIMIENTOS** Profesional en Ingeniería de Sistemas o carreras afines, con título debidamente acreditado y experiencia mínima certificada de tres (3) años en proyectos de Tecnologías de la Información, de los cuales al menos dos (2) años deberán corresponder específicamente a actividades de levantamiento, análisis, documentación, validación y gestión de requerimientos funcionales y no funcionales; con experiencia comprobada en la elaboración de historias de usuario, casos de uso, especificaciones técnicas (SRS), modelado de procesos AS-IS y TO-BE, construcción de diagramas bajo estándares UML y/o BPMN, definición de criterios de aceptación, gestión de trazabilidad y control de cambios, priorización y refinamiento de backlog, y articulación efectiva entre equipos técnicos y áreas funcionales; con conocimientos en metodologías ágiles y tradicionales de gestión de proyectos, herramientas especializadas para administración de requerimientos y seguimiento, y capacidad demostrada para estructurar documentación técnica integral, verificable y alineada con los objetivos estratégicos y alcance del proyecto; adicionalmente, deberá contar con conocimientos y aplicación práctica de los lineamientos establecidos en la norma ISO/IEC 27001:2022, incluyendo gestión de riesgos de seguridad de la información, identificación y tratamiento de activos, definición de controles del Anexo A (versión 2022), principios de confidencialidad, integridad y disponibilidad, gestión de incidentes de seguridad, control de accesos, seguridad en el desarrollo de software y aseguramiento del cumplimiento normativo dentro del Sistema de Gestión de Seguridad de la Información (SGSI). En consecuencia, el contratista deberá garantizar la disponibilidad de los profesionales necesarios que aseguren la adecuada atención de cada una de las tecnologías involucradas, dando cumplimiento a los niveles de servicio y a las actividades definidas en el anexo técnico. **GESTION Y ANALISIS DE INTELIGENCIA ARTIFICIAL** Profesional en Ingeniería de Sistemas o carreras afines, con título debidamente acreditado y experiencia mínima certificada de tres (3) años en proyectos de Tecnologías de la Información, de los cuales al menos dos (2) años deberán corresponder específicamente al diseño, desarrollo e implementación de soluciones basadas en Inteligencia Artificial, Machine Learning o Analítica de Datos; con certificación en lenguaje de programación Python, que respalde

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

competencias prácticas en programación orientada a objetos, manipulación de datos y desarrollo de scripts para soluciones de IA, y con certificación de Explorador en Ingeniería de Inteligencia Artificial, que demuestre comprensión integral del ciclo de vida de soluciones de IA, diseño de modelos, implementación de algoritmos y principios éticos asociados a su uso, incluyendo gestión de datos, control de calidad de modelos, y consideración de seguridad y privacidad de la información

En consecuencia, el contratista deberá garantizar la disponibilidad de los profesionales necesarios que aseguren la adecuada atención de cada una de las tecnologías involucradas, dando cumplimiento a los niveles de servicio y a las actividades definidas en el anexo técnico.

GESTION Y ANALISIS DE ARQUITECTURA DE SOLUCIÓN NATIVA / KUBERNETES

Profesional en Ingeniería de Sistemas, Computación o carreras afines, con título debidamente acreditado, con experiencia mínima certificada de tres (3) años, de los cuales al menos dos (2) años deberán corresponder específicamente a la gestión y análisis de arquitecturas de soluciones nativas sobre Kubernetes, especializado en sostenimiento de aplicativos con integración de inteligencia artificial para monitoreo, optimización y recuperación ante fallas. Experto en administración de clústeres, configuración de pods, volúmenes persistentes, alta disponibilidad, seguridad (RBAC, Kerberos, cifrado de datos) y automatización de procesos críticos mediante CI/CD, garantizando interoperabilidad, escalabilidad y continuidad operativa de sistemas estratégicos.

En consecuencia, el contratista deberá garantizar la disponibilidad de los profesionales necesarios que aseguren la adecuada atención de cada una de las tecnologías involucradas, dando cumplimiento a los niveles de servicio y a las actividades definidas en el anexo técnico.

El contratista deberá de hacer entrega en el momento de la firma del acta de inicio las hojas de vida al supervisor; así mismo, los perfiles solicitados dentro de las actividades contempladas en la realización del SOSTENIMIENTO APLICATIVO HYDRA, las cuales se llevarán a cabo de manera presencialmente en un horario de (3x8) es decir tres días a la semana 8 horas diarias en las instalaciones del CAIMI, y (2x8) dos días de forma virtual 8 horas diarias garantizando un entorno seguro para la protección de los activos informáticos y la confidencialidad de la información. Cuyas instalaciones estarán disponibles para su ejecución de lunes a viernes en el horario de 07:00 a.m. a 05:00 p.m

El contratista acepta que el supervisor evalúe, verifique y califique el desempeño profesional de la(s) persona(s) asignada(s) al proyecto durante la ejecución del contrato, y estará en facultad de solicitar su reemplazo por otra en caso de que dicho personal no cumpla con las expectativas de la Dirección de Arquitectura de Software.
Solo en el caso que dicho personal, no cumplan con las expectativas de acuerdo al desempeño, con base a requerimientos asignados y al cumplimiento de tareas relacionadas, el Supervisor o quien haga sus veces podrá solicitar cambio del mismo, por lo cual el contratista deberá asignar un nuevo profesional que cumpla con el perfil y los requisitos exigidos para cada caso, en un tiempo máximo diez (10) días calendario y presentarlo formalmente por escrito.

Para el cumplimiento de la ejecución, el contratista deberá poner a disposición el personal con su respectivo equipo de cómputo, **so pena de hacerse efectiva las garantías que la entidad estatal exige para la ejecución del contrato en caso que no se cumpliere con el perfil propuesto.**

El personal reemplazado deberá cumplir con lo establecido en el Acuerdo de Confidencialidad y estudios de seguridad correspondientes.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

3.2.5	**EXPERIENCIA Y PERFIL DEL PROPONENTE**
3.2.5.1	Con el fin de garantizar que el proponente cuente con experiencia en el desarrollo de proyectos relacionados con el presente objeto contractual, deberá incluir en su oferta mínimo una (1) una certificación donde demuestre lo siguiente: Certificación expedida por entidades en las cuales hayan participado en proyectos iguales o similares, así: ✓ Certificación expedida por entidades en las cuales hayan participado en proyectos de desarrollo y/o sostenimiento de software similar o igual al objeto del presente proceso. Para efectos de verificar la certificación(es) de la empresa, emitidas por las entidades donde ha laborado o desarrollado proyectos con relación del objeto contractual, las cuales contendrán como mínimo los siguientes aspectos: ✓ Nombre o razón social del contratante. ✓ Nombre o razón social del contratista. ✓ Descripción del ítem contratado. ✓ Fecha del contrato. ✓ Fecha de inicio y fin del contrato. ✓ Valor del contrato. ✓ Firmada por el respectivo funcionario. ✓ La suma de dichas certificaciones deberá sumar el 100% del valor del presupuesto oficial. Nota: No se aceptan auto certificaciones. Nota: se aclara que en el RUP se verificará los contratos ejecutados del oferente, sin embargo, se solicita allegar soporte del contrato relacionado como experiencia con el fin de corroborar el objeto y de esta manera verificar de manera eficiente que el oferente cuenta con la experiencia requerida para el proceso.
3.2.6	**ACUERDOS DE CONFIDENCIALIDAD**
3.2.6.1	El contratista y todo el personal vinculado al proyecto deberán firmar, antes del inicio de actividades, un Acuerdo de Confidencialidad y Protección de Información Clasificada, mediante el cual se obligan expresamente a preservar la reserva, integridad, custodia y confidencialidad de toda información institucional, operativa, estratégica o de inteligencia, a la que tengan acceso directo o indirecto, o que generen como producto del cumplimiento del presente contrato, incluyendo aquella clasificada conforme a los niveles de reserva establecidos en la Ley 1621 de 2013 y el decreto reglamentario correspondiente. En virtud de lo anterior, queda prohibida la divulgación, reproducción, copia, almacenamiento, extracción, transmisión, procesamiento, análisis o uso para fines distintos al objeto contractual de cualquier información clasificada de inteligencia o contrainteligencia, ya sea por medios físicos, digitales, orales o de cualquier otra índole, sin la autorización previa, formal y expresa del Comando de Apoyo de Inteligencia Militar – CAIMI. Lo anterior, en cumplimiento de lo establecido en los artículos 1, 2, 4, 5, 6, 7 y 13 de la Ley 1621 de 2013, que regulan el uso, acceso, tratamiento, clasificación, reserva legal, y los límites del uso de la información obtenida o generada en actividades de inteligencia, y en concordancia con su decreto reglamentario. Como condición indispensable, el contratista deberá: • Comprometerse formalmente a conocer, acatar y cumplir integralmente las disposiciones de la Ley 1621 de 2013, su reglamentación, y las políticas de seguridad

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

	de la información del Ministerio de Defensa Nacional, el Comando General de las Fuerzas Militares, el Ejército Nacional y el CAIMI, especialmente aquellas relativas al manejo, almacenamiento, clasificación y destrucción de información de inteligencia y contrainteligencia. • Autorizar y facilitar la práctica de estudios de seguridad al personal vinculado por parte de la IMI-CAIMI, de acuerdo con los procedimientos institucionales, con el fin de validar su idoneidad, confiabilidad y nivel de acceso a información clasificada. • Implementar todas las medidas técnicas, administrativas, organizacionales, físicas y digitales necesarias para impedir la fuga, filtración, alteración, uso indebido, interceptación o cualquier otra acción que comprometa la información clasificada, conforme a los principios de seguridad de la información y de necesidad de conocer. • Evitar el almacenamiento o tratamiento de información clasificada en entornos, plataformas o dispositivos no autorizados por la IMI-CAIMI, así como el acceso por personal que no cuente con el nivel de acreditación o autorización correspondiente. • Abstenerse de compartir o replicar cualquier tipo de material clasificado en redes sociales, plataformas colaborativas, aplicaciones de mensajería, o cualquier otro canal no institucional, so pena de incurrir en responsabilidad penal, disciplinaria o contractual. Al finalizar la ejecución del contrato, toda la información, soportes, modelos, respaldos, copias, documentos físicos y digitales generados o suministrados por el CAIMI deberán ser entregados en su totalidad y de manera formal, mediante acta de entrega-recepción, sin conservar duplicados ni registros en ningún tipo de soporte, de acuerdo con los principios de necesidad, proporcionalidad y legalidad establecidos en la Ley 1621. Cualquier incumplimiento a lo aquí estipulado será considerado una falta grave y podrá acarrear sanciones legales de orden penal, disciplinario y/o administrativo, según lo contemplado en el régimen jurídico vigente para el manejo indebido de información clasificada de inteligencia, y conforme a lo previsto en el Código Penal Colombiano y en la Ley 1621 de 2013.
3.2.7	**GARANTIA TECNICA**
3.2.7.1	El oferente al momento de la oferta deberá anexar documento independiente indicando que cumple de forma expresa y dando cumplimiento de los términos y condiciones establecidos para la garantía técnica del servicio, por un periodo de 6 meses posterior al término de la ejecución del contrato en el marco del presente contrato, comprometiéndose a prestar soporte técnico especializado, conforme a los siguientes lineamientos: El contratista dispondrá de personal técnico certificado, competente en la plataforma y funcionalidades del sistema JANUS, quien deberá prestar soporte presencial en las instalaciones del CAIMI cuando así se requiera por parte de la Entidad. • Responder por la garantía técnica durante toda la vigencia del contrato. • Asumir la disponibilidad inmediata del personal técnico. • Cumplir con los niveles de servicio (SLA) y tiempos de respuesta establecidos por el CAIMI. • Garantizar la confidencialidad y seguridad en la atención de incidentes, fallas o requerimientos técnicos. El contratista será responsable del correcto funcionamiento de todas las aplicaciones y componentes del sistema JANUS, durante la vigencia del contrato, incluyendo: • Asistencia técnica en sitio ante fallas, errores o degradación del rendimiento del sistema.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

	• Respuesta calificada a consultas técnicas, operativas o de administración solicitadas por el CAIMI. • Actualización y mantenimiento correctivo o preventivo de la aplicación. La ejecución de la garantía técnica será monitoreada por el equipo de supervisión del contrato en CAIMI, y cualquier incumplimiento será causal de aplicación de medidas contractuales y/o sanciones, conforme al régimen legal vigente y las cláusulas contractuales pactadas.
3.2.8	**TERMINO DE RESPUESTA**
3.2.8.1	Los soportes técnicos deben ser atendidos presencialmente de forma inmediata, si en el lapso de dos (02) horas después de haber reportado el incidente no se ha dado una solución definitiva al incidente, se deberá enviar personal técnico especializado a sitio en un tiempo máximo de dos (02) horas. El tiempo máximo permitido para restablecer el servicio luego de realizada la llamada que solicita el soporte técnico es de veinticuatro (24) horas.
3.2.9	**PROPIEDAD INTELECTUAL Y RESTRICCIÓN DE DIFUSIÓN DE INFORMACIÓN**
3.2.9.1	En cumplimiento de la Ley 23 de 1982 sobre Derechos de Autor, la Ley 1915 de 2018, y demás normas concordantes en materia de propiedad intelectual aplicables en Colombia, se establece que todos los desarrollos, avances tecnológicos, resultados técnicos, líneas de código, algoritmos, arquitecturas, modelos de datos, productos de software, documentación, informes, modelos de inteligencia artificial, mejoras, personalizaciones y cualquier otro resultado tangible o intangible generado dentro del marco del presente contrato, serán de propiedad exclusiva del Ejército Nacional de Colombia, en cabeza del Comando de Apoyo de Inteligencia Militar (CAIMI). El contratista reconoce expresamente que no adquiere, en ningún caso, derechos de propiedad, uso, explotación comercial o divulgación pública sobre dichos desarrollos o productos, y que su participación en el proyecto no le confiere titularidad sobre ninguno de los derechos patrimoniales o morales de autor asociados a los resultados obtenidos. Toda creación realizada en el marco del contrato se entiende como obra por encargo a favor del Estado colombiano. Asimismo, el contratista se obliga a no divulgar, reproducir, transferir, licenciar, publicar, almacenar o comunicar de ninguna forma información relacionada con los desarrollos del proyecto, el contenido del contrato, los procesos técnicos, estratégicos o metodológicos del CAIMI, ni antes, durante ni después de la ejecución contractual, salvo autorización previa, expresa y por escrito por parte del Ejército Nacional – CAIMI. Esta restricción de uso y difusión incluye, pero no se limita a: La publicación de contenidos en redes sociales, blogs, repositorios de código (como GitHub, GitLab, Bitbucket), medios académicos, comerciales o conferencias técnicas. La reutilización parcial o total de fragmentos de código, arquitecturas o metodologías fuera del entorno autorizado. La utilización de información contractual o técnica en proyectos externos, propios o de terceros. Cualquier incumplimiento a lo estipulado en la presente cláusula dará lugar a la aplicación de sanciones legales, contractuales y penales, según lo previsto en el régimen de propiedad intelectual del Estado, el Código Penal Colombiano, y el régimen de responsabilidad por divulgación no autorizada de información clasificada o reservada.
3.2.10	**TRANSFERENCIA DE CONOCIMIENTO**
3.2.10.1	El contratista deberá realizar una transferencia de conocimiento para los funcionarios de conocimiento al personal del CAIMI (mínimo 40 horas). sobre la utilización de prompt.

3.3 REQUISITOS DE EMPAQUE Y ROTULADO

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

3.3.1 Empaque.

Omitido

3.3.2 Rotulado.

Omitido

4. TOMA DE MUESTRAS Y CRITERIO DE ACEPTACIÓN O RECHAZO:

4.1 TOMA DE MUESTRAS Y CRITERIO DE ACEPTACIÓN O RECHAZO PARA EVALUAR LOS REQUISITOS GENERALES Y REQUISITOS DE EMPAQUE Y ROTULADO

Omitido

4.1.1 Muestreo. Omitido

4.1.2 Criterios de aceptación o rechazo para requisitos generales y requisitos de empaque y rotulado. Omitido

4.2 TOMA DE MUESTRAS Y CRITERIOS DE ACEPTACIÓN O RECHAZO PARA EVALUAR REQUISITOS ESPECÍFICOS.

Omitido

4.2.1 Muestreo. Omitido

4.2.2 Criterio de aceptación o rechazo para evaluar requisitos específicos.

Omitido.

5. MÉTODOS DE ENSAYO

Omitido.

6. APÉNDICE

6.1 NORMAS QUE DEBEN CONSULTARSE

- Constitución Política de Colombia
- Código Civil
- Código General del Proceso
- Código de Comercio
- Código de Procedimiento Administrativo y de lo Contencioso Administrativo
- Ley 80 de 1993 (Estatuto General de Contratación de la Administración Pública)

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

- Ley 1150 de 2007 (Modifica la Ley 80 de 1993 sobre contratación pública)
- Ley 816 de 2003 (En el caso de no limitarse a MIPYMES nacionales)
- Ley 1952 de 2019 (Estatuto Anticorrupción)
- Ley 1978 de 2019 (Norma que reglamenta las Tecnologías de la Información y las Comunicaciones – TIC)
- Decreto-Ley 019 de 2012 (Medidas para la simplificación de trámites)
- Decreto 1082 de 2015 (Por el cual se expide el Decreto Único Reglamentario del Sector Administrativo de la Función Pública)
- Decreto 1263 de 2022 (Lineamientos para la transformación digital de la Administración Pública)
- Resolución de Delegación 1549 del 6 de marzo de 2015
- Directiva Permanente 09 de 2014 emitida por el Ministerio de Defensa Nacional
- Resolución No. 6302 del 31 de julio de 2014 (Manual de Contratación del Ministerio de Defensa Nacional)
- Cartilla de Formatos de Contratación, Tomo I (Jefatura de Logística – Dirección de Contratación, en lo que aplique)
- Manuales y Circulares de Colombia Compra Eficiente y sus respectivas actualizaciones
- Ley Estatutaria 1621 de 2013 (Ley de Inteligencia y Contrainteligencia)
- Manuales y circulares de Colombia Compra Eficiente y sus respectivas actualizaciones Y demás normas concordantes y pertinentes.

6.2 ANTECEDENTES

Omitido.

7. ANEXOS

Omitido.

8. CONTROL DE REVISIONES

Revisión y/o Actualización	Modificaciones	Fecha
00	Creación del Anexo Técnico SOSTENIMIENTO INFRAESTRUCTURA HYDRA	30/07/2025
01	Se realiza ajustes al Anexo Técnico SOSTENIMIENTO INFRAESTRUCTURA HYDRA, con relación a mejora del documento técnico al ser revisado por el comité técnico estructurador, donde se realizó los ajustes a numerales y cambio en los años de experiencia de pasar de 5 años a 2 años con la finalidad de dar mayor pluralidad.	09/01/2026
02	Se realiza ajustes al Anexo Técnico SOSTENIMIENTO INFRAESTRUCTURA HYDRA, con relación a mejora del documento técnico al ser revisado por la dupla del comité estructurador, donde se da claridad a las actividades de sostenimiento, mantenimiento y desarrollo adaptativo creando el numeral 3.2.3.2 en el numeral 3.2.	13/02/2026
03	Se realiza ajustes al Anexo Técnico SOSTENIMIENTO INFRAESTRUCTURA HYDRA, con relación a mejora del documento técnico por observaciones allegadas en el proceso de	06/04/2026

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

	evento de cotización, donde se da claridad perfiles requeridos y experiencia el numeral 3.2.4	

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial