ANEXO TÉCNICO
SOSTENIMIENTO DE APLICACIONES Y BASES DE DATOS DEL SICIE

CONTENIDO

1. OBJETO 2
2. DEFINICIONES Y APLICACIÓN 2
3. REQUISITOS..... 4
4. TOMA DE MUESTRAS Y CRITERIO DE ACEPTACIÓN O RECHAZO: 24
5. MÉTODOS DE ENSAYO 24
6. APÉNDICE 24
7. ANEXOS 25
8. CONTROL DE REVISIONES 25

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

En la actualidad, el Subsistema de Inteligencia y Contrainteligencia Militar (SICIE) enfrenta la necesidad de mantener y optimizar aplicaciones y bases de datos en plataformas como Oracle y MySQL, en un entorno tecnológico que exige altos estándares de seguridad, eficiencia y resiliencia. La constante evolución de las amenazas cibernéticas, junto con los avances en inteligencia artificial. Oracle sigue siendo una de las soluciones más confiables debido a sus avanzadas capacidades de protección de datos y escalabilidad, lo que permite a las organizaciones gestionar y resguardar la información en tiempo real mediante medidas de ciberseguridad avanzadas, como encriptación y monitoreo constante.

A su vez, las aplicaciones y bases de datos alineadas con la Directiva Permanente No. 0200 del 2017 deben ser constantemente actualizadas para mantenerse a la par con la evolución tecnológica. Facilitando así la toma de decisiones en tiempo real. La agilidad en el acceso a la información se vuelve crucial para la eficiencia operativa, por lo que las herramientas tecnológicas deben ser accesibles e intuitivas. El desafío radica no solo en mantener la infraestructura actual, sino también en adaptarse a un entorno de innovación continua, asegurando que las aplicaciones y sistemas evolucionen conforme a las necesidades cambiantes de la misión.

2. DEFINICIONES Y APLICACIÓN

2.1 DEFINICIONES

- Plan de Mantenimiento: Es un documento que dice cuáles son las prácticas específicas del mantenimiento, los recursos y la secuencia de actividades relevantes para el mantenimiento de un software de modo que el mantenedor es quien prepara este plan.

- Mejora: Es un cambio del software, pero no es una corrección como las definidas antes de iniciar el desarrollo de las historias de usuario así habrá dos tipos de mejoras: adaptativas y perfectivas.

- Informe de Problema: Término usado para identificar y describir problemas detectados en un software.

- MDAS: Metodología de desarrollo ágil y seguro que incluye las fases de conceptualización, diseño, desarrollo, implementación y soporte para el software y los sistemas a fin de validar que los desarrollos se realicen de manera correcta y cumplan con los principios de confidencialidad, disponibilidad e integridad de la información.

- SOSTENIMIENTO: Es una actividad muy amplia que incluye la corrección de errores, mejoras de las capacidades, eliminación de funciones obsoletas y optimización.

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

- ORACLE DATABASE: es un sistema de gestión de base de datos de tipo objeto-relacional (ORDBMS, por el acrónimo en inglés de Object-Relational Data Base Management System), desarrollado por Oracle.

- DATABASE: Una base de datos es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

- SISTEMA OPERATIVO: es un software que administra la forma en que se pueden usar los recursos de una computadora.

- SOLARIS: Es un sistema operativo de tipo Unix el cual funciona en arquitecturas SPARC y x86 administrando las aplicaciones y servicios que sean instalados sobre el mismo. Por ser del fabricante Oracle esté esta optimizado para el manejo de servidores Oracle lo mismo que para las aplicaciones por ellos desarrolladas.

- ORACLE LINUX: Es un entorno operativo seguro y de elevado rendimiento que ofrece herramientas de virtualización, gestión, automatización y computación nativa, ofrece una alternativa 100 % compatible binaria de aplicaciones a Red Hat Enterprise Linux y CentOS Linux, y compatible con entornos tanto híbridos como multinube.

- SOSTENIMIENTO: Es una actividad muy amplia que incluye la corrección de errores, mejoras de las capacidades, eliminación de funciones obsoletas y optimización.

- MYSQL: Es un sistema de gestión de bases de datos relacional (RDBMS) de código abierto, basado en el lenguaje SQL (Structured Query Language). Es uno de los sistemas más populares del mundo para almacenar, organizar y acceder a datos estructurados.

- SQL: (Structured Query Language) es el lenguaje estándar que se utiliza para comunicarse con bases de datos relacionales. Con SQL puedes crear, consultar, modificar y administrar los datos almacenados en una base de datos.

2.2 APLICACIÓN

El contexto de aplicación de las actividades previstas como sostenimiento es necesario ya que los productos de software sufren cambios durante el ciclo de vida, asegurando la información que se procesa a través de los diferentes aplicativos, así como permitir proteger los activos de información que los contienen, propendiendo por la integridad, disponibilidad y confidencialidad de los mismos, además de pretender disminuir la obsolescencia tecnológica a la que se ven expuestos los sistemas de información, por la evolución constante de cada una de las herramientas que se utilizaron inicialmente para su creación.

El servicio sostenimiento está compuesta por bases de datos y aplicaciones existente en el SICIE debe ser continuo en el tiempo y no puede ser suspendido en ningún momento, debido a que la información allí contenida es de vital importancia para el análisis,

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

evaluación y toma de decisiones operacionales de la institución; asimismo la documentación generada en el sistema es almacenada y gestionada en estas bases de datos, por esta razón es indispensable mantener la disponibilidad, seguridad e integridad de la misma y el sostenimiento a dichas aplicaciones, mediante un contrato de mantenimiento preventivo y correctivo, garantizando así el correcto funcionamiento de las mismas y dando cumplimiento de la misión institucional de acuerdo con los lineamientos de la ley 1621 del 2013 referente a la protección de la información y la reserva legal.

3. REQUISITOS

3.1 REQUISITOS GENERALES

El sostenimiento será llevado a cabo por entidades calificadas en cada una de las tecnologías, lenguajes de programación, versionamiento de software y sistemas operativos utilizados por el SICIE. Esto permitirá que el sistema se mantenga a la vanguardia tecnológica y evite la obsolescencia. Estas entidades especializadas cuentan con los recursos, personal calificado, infraestructura y conocimientos necesarios para adaptarse a las nuevas tecnologías. La colaboración con ellas facilitará la ejecución de proyectos más complejos y de mayor envergadura, brindando al SICIE una valiosa base de conocimiento y experiencia, lo que garantizará la funcionalidad de las aplicaciones y su disponibilidad para el desarrollo de la misión institucional.

El objetivo del sostenimiento es proporcionar asesoría técnica para resolver problemas relacionados con el uso de software, hardware o sistemas informáticos. También incluye la realización de actualizaciones, suministro de parches de seguridad, control rutinario de logs, auditoría y evaluación de servidores y redes, y los servicios de recuperación de datos. La adaptación a nuevas tecnologías y la implementación de políticas de seguridad alineadas con metodologías ágiles y la certificación ISO 270001:2022 son esenciales para garantizar la continuidad de los servicios y la seguridad de la información.

Para el SICIE, es crucial garantizar la continuidad de los servicios de las aplicaciones y bases de datos a todos los funcionarios encargados de la recolección, análisis y difusión de inteligencia. Si no se garantiza la continuidad de estos servicios, el SICIE estaría expuesto a riesgos que podrían afectar la operación normal de las bases de datos y aplicaciones, comprometiendo la seguridad de la información. Por ello, es esencial contar con servicios de sostenimiento para evitar interrupciones, realizar la depuración de logs generados por las bases de datos, adaptarse a nuevas versiones de software enviadas por los fabricantes, y realizar actualizaciones de seguridad para prevenir posibles ciberataques. Además, es necesario monitorear las aplicaciones y bases de datos con herramientas nativas o de terceros para asegurar su correcto funcionamiento.

Es fundamental contar con los servicios de sostenimiento de las aplicaciones y bases de datos del SICIE, ya que la información contenida en ellas es vital para el análisis, evaluación y toma de decisiones operacionales de la institución. Asimismo, la documentación generada y gestionada por las aplicaciones está almacenada en estas bases de datos, lo que hace indispensable mantener su disponibilidad, seguridad e

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

integridad. El sostenimiento de estas aplicaciones es crucial para cumplir con la misión institucional, en cumplimiento de los lineamientos de la Ley 1621 de 2013 sobre la protección de la información y la reserva legal. Cualquier falla en este proceso podría generar la indisponibilidad de los servicios informáticos o la pérdida parcial o total de la información almacenada.

3.2 REQUISITOS ESPECÍFICOS

ÍTEM	DESCRIPCIÓN
3.2.1	**EL SOSTENIMIENTO A LA BASE DE DATOS Y SISTEMAS OPERATIVOS ORACLE LINUX**
3.2.1.1	El sostenimiento deberá ser prestado para todas las bases de datos y sistemas operativos, que en la actualidad tiene disponible el Subsistema de Inteligencia y Contrainteligencia del Ejército (SICIE), garantizando la realización de las siguientes actividades, así: • Se deberá realizar la respectiva depuración de los objetos inválidos de la base de datos, como vistas, dblinks, procedimientos, paquetes, funciones, triggers que no se encuentren en uso y no afectan la integridad y disponibilidad de la información. • Se deberá realizar la actualización y sostenimiento de los servidores de aplicaciones donde están funcionando todas las aplicaciones del SICIE, así mismo se realizará el diagnóstico del funcionamiento y mantenimiento regular que se requiera para su óptimo funcionamiento. • Se deberá garantizar y proporcionar soporte técnico especializado según sea necesario para la actualización, soporte y mantenimiento tanto de la infraestructura de hardware y software como de cada una de las aplicaciones y motores de base de datos que tiene el SICIE. • Se deberá realizar la optimización de código y logs de las aplicaciones del SICIE, reduciendo operaciones excesivas de escritura en disco. • Se deberá realizar y aplicar actualizaciones y parches de seguridad tanto en servidores como en las librerías que sean utilizadas en cada una de las aplicaciones. • Se deberá actualizar los sistemas operativos de las máquinas virtuales donde está instalado el ESB de pruebas y de producción a la versión más reciente. • Se deberá realizar la actualización de la base de datos a la versión 19c del aplicativo de Fuentes y Agencias (F&A) y archivo operacional (ARCHOP), dando el soporte necesario para su puesta en funcionamiento y haciendo los ajustes necesarios. • Se debe llenar el formato de historia de usuario para todos los requerimientos nuevos que requieran las aplicaciones del SICIE • Monitoreo 24/7 del rendimiento, disponibilidad, archivos de log, crecimiento de tablas y espacios críticos. • seguimiento continuo del rendimiento y la estabilidad de las bases de datos. • Garantizar el correcto uso y configuración de ORACLE RAC, asegurando alta disponibilidad (HA) permanente. • Gestión completa de respaldos automáticos, restauraciones parciales y completas, y recuperación ante desastres mediante DataGuard. • Optimización continua de consultas SQL, índices, estructuras físicas y estadísticas para mejorar el rendimiento de la base de datos.

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

	• Administración y endurecimiento de políticas de seguridad de acceso a la base de datos y los sistemas operativos (audit trail, cifrado, RBAC). • Configuración, monitoreo y mantenimiento de consolas Oracle Enterprise Manager, WebLogic y RMAN, incluyendo depuración y alertamiento. • Soporte técnico sobre sistemas operativos Oracle Linux, Solaris, contemplando actualizaciones, hardening, gestión de usuarios y afinamiento del kernel. • Aplicación de parches de seguridad (PSU/CPU), upgrades de versiones y migración progresiva a versiones soportadas para evitar obsolescencia. • Configuración de réplicas de ambientes (desarrollo, pruebas, producción) y su replicación hacia sitio alterno con sincronización validada. • Gestión de espacio en disco, filesystem, uso de memoria, tablespaces y limpieza automatizada de objetos inválidos. • Validación continua de licenciamiento, integridad de los datos, logs de errores críticos y generación de reportes para el supervisor del contrato. • Gestión de alta disponibilidad (HA) utilizando herramientas como MySQL Group Replication, InnoDB Cluster, o soluciones externas como Keepalived y Pacemaker. Administración de respaldos automáticos con herramientas como mysqldump, mysqlpump, Percona XtraBackup o MySQL Enterprise Backup, incluyendo pruebas periódicas de recuperación parcial y total. • Optimización de rendimiento de consultas SQL, índices, configuración de parámetros de MySQL (my.cnf), análisis de planes de ejecución y actualización de estadísticas. • Administración de políticas de seguridad, incluyendo control de accesos (GRANT/REVOKE), cifrado de datos en tránsito y en reposo, uso de roles y revisión de logs de auditoría (general_log, audit_log). • Mantenimiento y monitoreo de herramientas de gestión como MySQL Workbench, phpMyAdmin, Percona Monitoring and Management (PMM) u otras consolas de monitoreo integradas. • Soporte y administración del sistema operativo base (Linux principalmente): actualizaciones, hardening, gestión de usuarios, configuraciones de red y ajustes del kernel para optimizar MySQL. • Aplicación de actualizaciones de seguridad, parches y upgrades de versión de MySQL, planificando migraciones seguras para evitar obsolescencia. • Configuración y sincronización de entornos replicados (replicación Master-Slave, Master-Master, GTID) y gestión de ambientes de desarrollo, pruebas y producción. • Gestión del almacenamiento: limpieza de registros binarios, rotación de logs, uso de tablespaces, mantenimiento del InnoDB Buffer Pool y eliminación de objetos inválidos o huérfanos. • Validación de cumplimiento de licencias (MySQL Enterprise), integridad de los datos, revisión de errores críticos en logs (error.log, slow query log) y generación de reportes ejecutivos y técnicos. • se deberá realizar la revisión de la infraestructura tecnológica donde será evaluada la gestión del equipo y la tecnología necesarios para la operación de bases de datos y de los sistemas operativos. • Se deberá realizar la integración de las bases de datos y de los sistemas operativos realizando una evaluación y aseguramiento de capacidades para su funcionamiento con otras aplicaciones que tiene el SICIE.

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

	• Se deberá realizar la gestión del almacenamiento y del flujo de Información del SICIE. • Se deberá realizar todas las actividades necesarias para garantizar la seguridad de la Información, implementación y supervisión de medidas para proteger la integridad y confidencialidad de los datos. • Se deberá tener la documentación detallada técnicamente sobre los procedimientos de sostenimiento, configuraciones realizadas y cualquier cambio realizado en las bases de datos y de los sistemas operativos. • Se deberá garantizar que las bases de datos de desarrollo, pruebas y producción existentes o nuevas estén en perfecto funcionamiento. • Se deberá garantizar que las instancias se encuentren en modo pasivas y/o activas según se requiera. • Se deberá garantizar que las tareas de mantenimiento programadas sean ejecutadas y acordes a la necesidad del SICIE. • Se deberá garantizar la verificación de espacio disponible en las bases de datos y sistemas operativos sean las óptimas para su pleno funcionamiento. • Se debe garantizar que los permisos que tiene los usuarios de desarrollo en las bases datos y de los sistemas operativos Linux, sean los necesarios por el SICIE de acuerdo con la necesidad que se requiera, así mismo, se debe instalar esta política de seguridad para evitar fuga de información de los datos almacenados en las bases de datos. • Se deberá dejar instalada, actualizada la base de datos y el software requerido para los sistemas operativos Linux a la última versión existente en el mercado, para estar acorde a la tecnología que se encuentra en el mercado y evitar vulnerabilidades o en su defecto instalación de parches o actualizaciones. • Se deberá tener siempre la disponibilidad de los servicios prestados por la herramienta HERCULES, la cual esta instala en la institución, realizando actividades necesarias para su perfecto funcionamiento. • Se deberá actualizar los sistemas operativos de las máquinas virtuales donde está instalado el ESB de pruebas y de producción a la versión más reciente.
3.2.2	**SOSTENIMIENTO, MANTENIMIENTO Y SOPORTE CORRECTIVO, PREVENTIVO DE LA CAPA MEDIA Y APLICATIVOS DE INTELIGENCIA DEL SICIE**
3.2.2.1	Deberá ser prestado para todas las aplicaciones, que en la actualidad tiene disponible el Subsistema de Inteligencia y Contrainteligencia del Ejército (SICIE), garantizando la realización de las siguientes actividades, así: • Se deberá realizar la implementación de contenedores por dominio funcional con orquestación automatizada mediante Kubernetes (o MicroK8s), permitiendo escalabilidad, tolerancia a fallos y despliegue independiente de componentes críticos. • Se deberá realizar el rediseño del control de acceso basado en roles (RBAC) a nivel de aplicación, integrando autenticación centralizada y políticas de permisos granulares por tipo de usuario, con trazabilidad y logging activo. • Se deberá realizar la automatización de ambientes de desarrollo, pruebas y producción mediante pipelines CI/CD con herramientas como GitLab CI y Jenkins, asegurando validación previa, pruebas automatizadas y rollback controlado. • Se deberá realizar la actualización y modernización de frameworks obsoletos en frontend y backend (ej.: migración de AngularJS a Angular 16+ o Spring MVC a Spring Boot 3), incluyendo refactorización de servicios, interfaces y lógica de negocio, y todas las librerías que sean necesarias.

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

	• Se deberá realizar el diseño e implementación de APIs estandarizadas y documentación técnica (OpenAPI/Swagger), permitiendo integración segura con otras aplicaciones del SICIE. • Se deberá realizar la optimización del rendimiento mediante análisis de logs, profiling de memoria y control de hilos, minimizando cuellos de botella y mejorando la experiencia de usuario. • Se deberá realizar la gestión de versiones con GitHub para todos los artefactos desplegables, asegurando trazabilidad de cambios y control de dependencias en cada módulo. • Se deberá garantizar y proporcionar soporte técnico especializado según sea necesario. • Se deberá realizar y aplicar actualizaciones y parches de seguridad tanto en servidores, como en las librerías que sean utilizadas en cada una de las aplicaciones. • Se deberá realizar un monitoreo contaste al número de usuarios concurrentes de las aplicaciones del SICIE. • Se deberá realizar una evaluación periódica de vulnerabilidades, pruebas de penetración (pentesting) inicial y final con herramientas especializadas. • Se deberá realizar la configuración de controles RBAC, monitoreo de accesos, trazabilidad y protección de datos en tránsito y reposo. • Se deberá realizar la aplicación de estándares SGSI, implementación de mejores prácticas OWASP y monitoreo activo de integridad. • Se deberá realizar el levantamiento de arquitectura, documentación de código fuente, APIs y diagramas de interacción con otros sistemas. • Se deberá realizar y hacer entrega de manuales técnicos, bitácoras, repositorios y cronograma con actividades detalladas por fase, esta entrega se deberá de realizar con una versión inicial a los 15 días posterior al acta de inicio y la versión final se deberá de hacer entrega en el informe final de cierre del contrato. • Se deberá garantizar y realizar las diferentes actividades en la intranet disponible en el SICIE. • Se deberá realizar un plan de contingencia de la base de datos y los aplicativos el cual deberá de ser entregado con el informe inicial al supervisor con un plazo máximo de 15 días calendario contados a la firma del acta de inicio del contrato.
3.2.2.2	• Se deberá realizar la refactorización profunda del código heredado para desacoplar capas de presentación, lógica de negocio y acceso a datos, progresivamente del aplicativo SIGAR y de las aplicaciones del SICIE. • Se deberá garantizar la correcta refactorización de las aplicaciones del SICIE, priorizando el desarrollo tecnológico del Sistema Integrado de Información (SI3) basado en nuevas tecnologías y con un plan de trabajo acordado entre el contratista y SI3. • Se deberá realizar el rediseño del control de acceso basado en roles (RBAC) a nivel de aplicación, integrando autenticación centralizada y políticas de permisos granulares por tipo de usuario, con trazabilidad y logging activo. • Se deberá realizar la automatización de ambientes de desarrollo, pruebas y producción mediante pipelines CI/CD con herramientas como GitLab CI y Jenkins, asegurando validación previa, pruebas automatizadas y rollback controlado. • Se deberá realizar la actualización y modernización de frameworks obsoletos en frontend y backend, incluyendo refactorización de servicios, interfaces y lógica de negocio, y todas las librerías que sean necesarias.

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

	• Se deberá realizar la gestión de versiones con GitHub para todos los artefactos desplegables, asegurando trazabilidad de cambios y control de dependencias en cada módulo. • Se deberá realizar un análisis profundo del sistema actual y diseño detallado de la nueva arquitectura de microservicios y APIs. • Se deberá realizar el despliegue iterativo necesarios y construcción del nuevo frontend desacoplado de las aplicaciones del SICIE. • Se deberá entregar funcionalmente los ciclos completos de pruebas de integración, rendimiento, usabilidad y seguridad para garantizar la calidad. • Se deberán realizar los respectivos despliegues progresivos de la refactorización, monitorización y soporte de los bugs presentados. • Migración y actualización de la intranet del SICIE con nuevas tecnologías • Se deberá realizar desarrollo adaptativo de todas las aplicaciones del SICIE, los cuales deberán de permitir la escalabilidad a nuevas tecnologías y las diferentes directivas emitidas por el comando superior .
3.2.3	**GENERALIDADES DEL SERVICIO**
3.2.3.1	El contratista deberá realizar el sostenimiento de todas las aplicaciones que tiene el SICIE disponibles para todos los funcionarios siendo estas la intranet, SICDI, SICAI, SICOOI, ARCHOP, FYA, BUS DE INTEGRACION, DATA LAKE, SIGAR, KAIROS, SIGOP, SIMAI. El contratista garantizará un soporte adicional al 5x8 bajo esquema 7x24x365 con un tiempo de respuesta de atención inicial máximo de 2 horas. El contratista presentará el plan de trabajo y el equipo de trabajo, el cual contendrá el cronograma que indique las siguientes fases diagnóstico, planeación, ejecución de cada una de las aplicaciones, base de datos que tiene el SICIE. El contratista entregará los respectivos informes mensuales los cuales deberán de contener los siguientes criterios arquitectura de software, arquitectura de la plataforma funcional del CAIMI (servidores, instancias de bases de datos, conectividad, direccionamiento IP), manual técnico con guía de administración y plan de contingencia y recuperación de desastres. El contratista deberá configurar los servidores de respaldo los cuales deberán de contener los siguientes criterios arquitectura de software, arquitectura de la plataforma funcional del CAIMI (servidores, instancias de bases de datos, conectividad, direccionamiento IP), manual técnico con guía de administración acorde al plan de contingencia y recuperación de desastres de todas las aplicaciones del SICIE. El contratista garantizará que las actividades de sostenimiento de las aplicaciones del SICIE a intervenir se llevarán a cabo de manera presencialmente en las instalaciones del CAIMI, garantizando un entorno seguro para la protección de los activos informáticos y la confidencialidad de la información. El contratista garantizará la operatividad, estabilidad y evolución continua de todas las aplicaciones esto incluye la actualización y mejora del software (update y upgrade), la depuración y análisis de logs para optimizar el rendimiento y la

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

	seguridad, así como el mantenimiento adaptativo para garantizar la compatibilidad con nuevas tecnologías y cambios en el entorno operativo. El contratista realizará el diseño y desarrollo de nuevos servicios, junto con el levantamiento, actualización y optimización de diagramas de flujo y arquitectura de las aplicaciones, asegurando una representación clara y precisa de los procesos y su interacción con otros sistemas. El contratista deberá hacer el levantamiento, modernización y la refactorización del código el cual permitirá mejorar la eficiencia, mantenibilidad y escalabilidad del software, mientras que el modelamiento entidad-relación de bases de datos garantizará una estructura óptima para la gestión de la información. El contratista entregará al supervisor del contrato la documentación detallada del código fuente y la arquitectura de las aplicaciones, facilitando su comprensión y futuras intervenciones. El contratista deberá realizar e implementar pruebas técnicas y funcionales para validar el correcto funcionamiento y desempeño del software antes de su puesta en producción. Así mismo, se realizará la configuración y optimización de servidores de aplicación y almacenamiento. El contratista deberá ajustarse a realizar las actividades de mejoramiento, refactorización, actualización, desarrollo de nuevos módulos y perfeccionamiento a todas las aplicaciones, base de datos y sistemas operativos Linux, donde se ejecutarán bajo metodologías ágiles y seguras de desarrollo de software, permitiendo una gestión flexible y eficiente de los cambios. Además, se garantizará el cumplimiento de los lineamientos y mejores prácticas establecidos en la certificación ISO 27001 del 2022 de la entidad, asegurando la confidencialidad, integridad y disponibilidad de la información en cada etapa del proceso. El contratista se compromete a entregar en ambiente de producción de las aplicaciones y base de datos de todas las actividades completadas y operativas. El contratista garantizará que el sostenimiento, mantenimiento preventivo y correctivo de todas las aplicaciones y desarrollos adaptativos, en base de datos y ESB, debe mantener siempre compatibilidad con los navegadores Chrome, Firefox Mozilla, Safari y Microsoft Edge, IOS y android y demás disponibles en el mercado en sus versiones recientes y mantener un comportamiento responsive según los diferentes tipos de dispositivos móviles. El contratista deberá realizar y hacer entrega en un documento los manuales correspondientes al despliegue, reinicio, apagado de la infraestructura tecnológica en la que se encuentran instaladas las aplicaciones del SICIE con el propósito de garantizar la disponibilidad de los servicios frente a una situación de contingencia. El contratista deberá realizar y garantizar todas las actividades necesarias para garantizar la seguridad de la Información, implementación y supervisión de medidas para proteger la integridad y confidencialidad y disponibilidad de todas las aplicaciones.

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

	El contratista debe garantizar la idoneidad y experiencia del personal dispuesto para prestar los servicios de desarrollo, mantenimiento, actualización, refactorización y sostenimiento de las aplicaciones, al igual que su disponibilidad, cuando se evidencie ausencia de idoneidad en alguno de los miembros del equipo, el supervisor del contrato solicitara el reemplazo de dicho profesional, trasladando la responsabilidad al contratista por los tiempos en los que se pueda incurrir para su reemplazo y en la aplicación de las garantías que soportan el proceso contractual. El contratista debe asumir todos los costos asociados con desplazamientos de su personal, transporte de equipos a los sitios, suministro de los equipos de cómputo para que los ingenieros o técnicos usen para desarrollar los diferentes trabajos en el CAIMI. En el evento de requerirse elementos adicionales no contemplados en la oferta y los cuales se requieren para el desarrollo del proyecto y cubra el alcance de este, el contratista debe proveerlos sin que estos generen costos adicionales para la entidad contratante. El contratista garantizará que los recursos profesionales designado al contrato se encuentre en las instalaciones del CAIMI, deberán enfocarse exclusivamente en el sostenimiento, refactorización, innovación, creación, migración, desarrollo adaptativo y mejora de las aplicaciones del SICIE. En ninguna circunstancia podrán desempeñar funciones o trabajar en proyectos ajenos. El contratista instalará el software y los servicios de instalación, configuración y puesta en funcionamiento requerido para la configuración de las pruebas y entregará en completa operación, todos los componentes necesarios de software que garanticen la correcta ejecución del sostenimiento de la plataforma Oracle, sql server y de aplicaciones del SICIE. El contratista deberá garantizar que las aplicaciones del SICIE, se encentren de modo seguro en el entorno tecnológico al momento de hacer el uso por parte del funcionario y así dar el cumplimiento a la norma ISO 27001 En caso de ser necesario apagar el datacenter el contratista será el responsable de, apagar y encender todos los servidores de bases de datos y las aplicaciones esto garantizando el servicio de todas las aplicaciones del SICIE, las 24 horas del día durante la vigencia del contrato. El contratista deberá realizar todos los backups con una retención de 5 días para garantizar el funcionamiento de todas las aplicaciones en caso de presentarse alguna caída y monitorear el software de backups e instalar nuevas políticas para la realización de copias de seguridad a las bases de datos Oracle y de las aplicaciones del SICIE, igualmente, prestará asistencia técnica en la definición e implementación de las políticas de copias de seguridad garantizando su recuperación a cualquier punto en el tiempo. Igualmente, lo anterior se realizará hacia el sitio alterno (CAIMI) configurando los periodos de tiempo para la sincronización. El contratista realizará pruebas para verificar el correcto funcionamiento de los componentes de la integridad de la información de estos, validando este último aspecto con los funcionarios de las aplicaciones y base de datos garantizando que, en todos los procedimientos necesarios para el cumplimiento del objeto contractual,

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

	se apliquen las normas técnicas referentes a la seguridad de la información ISO 27001 del 2022. El contratista debe realizar un esquema de red, con su respetivo direccionamiento, de todos los servidores de bases de datos y aplicaciones y debe documentar los puertos por donde se están conectado las aplicaciones y documentar toda la operación de estos. El contratista realizará la instalación de los servidores de base de datos y de todas las aplicaciones con los distintos sistemas operativos, para la creación del sitio alterno para que este entre a funcionar en caso de caída haciendo las pruebas necesarias para demostrar que este se puede acceder desde este sitio alterno, esto se debe desarrollar dentro de los tres primeros meses del presente contrato. El contratista realizará las configuraciones necesarias para garantizar la conectividad de los componentes necesarios para el óptimo funcionamiento de las bases de datos y de los aplicativos del SICIE. Todas las comunicaciones deben ser enviadas de manera oficial por el correo de la entidad, y se debe tener la trazabilidad de todos los procesos que se desarrollan en el presente contrato. El contratista debe garantizar la continuidad del personal inicialmente ofertado en la ejecución del objeto contractual suscrito, de ser necesario el cambio, deberá de realizar una comunicación oficial vía correo u oficio, en el momento de realizar cualquier cambio en la plantilla del personal ofertado, con mínimo cinco (5) días hábiles de anterioridad al retiro efectivo del mismo, en el cual anexará la hoja de vida del profesional que sea postulado para reemplazar al saliente, quien deberá cumplir con los mismas o mejores requisitos de experiencia y educación que se establecen para cada cargo al interior de esta especificación técnica y por la cual fue adjudicado. Una vez recibida la anterior información, el supervisor del contrato, contará con dos (2) días hábiles para aprobar la hoja de vida del nuevo profesional propuesto por el contratista, autorizando el ingreso y salida del personal de conformidad con la solicitud recibida. Mientras el contratista no cuente con la autorización anterior, no podrá disponer el retiro o la salida de ningún profesional que intervenga en la ejecución del objeto del respetivo contrato. El contratista entregará la documentación, usuarios, contraseñas usadas de administración siempre cuando haga cambio de esta. El contratista dispondrá de los computadores necesarios para el desarrollo de las actividades de sostenimiento de las bases de datos y de las aplicaciones del SICIE durante la duración de todo el plazo de ejecución del contrato a suscribir y en los sitios de ejecución del objeto de este; estos computadores serán incluido dentro de la red institucional y con las políticas de seguridad establecidas, una vez finalizado el contrato, el contratista deberá retirar este equipo. El contratista es el responsable de la gestión inmediata del fichero de identificación personal provisto por la entidad una vez se realiza la adjudicación del proceso, esto con la finalidad de que el acceso a las instalaciones no le represente demoras al profesional.

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

	El contratista junto con los recursos asignados deberá de firmar la sesión de los derechos de autor del sostenimiento realizado a las aplicaciones del SICIE. El contratista junto con los recursos asignados deberá de realizar la planificación y elaboración de un plan contingencia frente a la recuperación de desastres el cual debe ser entregado al terminal el primer mes del contrato. El contratista deberá de realizar las respectivas actividades de seguridad en las bases de datos, de conforme a los parámetros de la norma ISO 27001 del 2022 y las de owasp, aplicaciones y sistemas operativos para identificar vulnerabilidades y así darles las respectivas soluciones. El contratista deberá brindar una solución y de ser el caso la reinstalación de software, de las aplicaciones y bases de datos del SICIE, esta actividad se deberá instalar de ceros para que las bases datos estén en perfecto funcionamiento y sus componentes con una disponibilidad del 99 %, brindando soporte en la instalación, ajustes, balanceo, configuración de los parámetros de funcionamiento para las licencias, servidores y aplicaciones de WEBLOGIC, ORACLE DATABASE, REAL APLICATION CLUSTERS, DATAGUARD, ORACLE BUSSINESS INTELLIGENCE, ULTRASEARCH en el servidor o servidores con que cuenta el CAIMI en Alta Disponibilidad y Sitio Alterno generando este cambio de manera automatizada, incluyendo parches y/o actualizaciones. El contratista deberá suministrar y configurar un centro de monitoreo de las aplicaciones, base de datos, almacenamiento de las aplicaciones tales como dashboards de monitoreo y reportes automáticos diarios enviando este informe por correo electrónico al supervisor del contrato y al administrador de la plataforma designado por el supervisor. El contratista deberá garantizar y realizar las respectivas actualizaciones al SICDI en relación a la normativa de gestión documental y directivas emitidas por el comando superior.
3.2.3.2	Las actividades contempladas en el sostenimiento, mantenimiento y desarrollos evolutivos a realizar en las aplicaciones del SICIE por parte del contratista se ejecutarán bajo un modelo de planeación y priorización continúo denominado ROAD MAP, el cual permitirá garantizar la adecuada atención de las necesidades institucionales y, en consecuencia, la continuidad de los servicios. Este ROAD MAP constituirá el instrumento principal de planeación, seguimiento y control de las actividades de sostenimiento, mantenimiento y desarrollos evolutivos. 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.

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

	• 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 los respectivos soportes donde se evidencie las CERTIFICACIONES Y FORMACIÓN REQUERIDA. **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

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

	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). **ADMINISTRACION Y GESTION DE BASES DE DATOS ORACLE** Tecnólogo o 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 a la administración, soporte, optimización y aseguramiento de plataformas de bases de datos empresariales y sistemas operativos asociados. Este perfil deberá ser cubierto como máximo por dos (2) profesionales designados por el contratista, en consideración a que dentro del alcance técnico se contempla la gestión de dos (2) tipos de bases de datos distintas, que requieren conocimientos y competencias específicas. Los profesionales deberán contar con experiencia en la gestión de Oracle Database 19c en entornos RAC, ASM y Grid Infrastructure sobre Oracle Enterprise Edition, garantizando alta disponibilidad (HA), continuidad operativa e integridad de la información, El oferente deberá presentar las certificaciones expedidas por ORACLE, como Oracle Database 19c: RAC, ASM, and Grid Infrastructure Administrator Oracle Certified Professional y Oracle Database Administration 2019 Certified Professional y Oracle Certified Associate (OCA) – MySQL. Adicionalmente, deberán demostrar competencias en la depuración de objetos inválidos, monitoreo continuo (24/7) del rendimiento, administración de respaldos y recuperación ante desastres mediante RMAN y DataGuard, aplicación de parches PSU/CPU y ejecución de actualizaciones de versión, optimización de consultas SQL e índices, gestión de tablespaces y almacenamiento, implementación y fortalecimiento de políticas de seguridad (auditoría, cifrado y control de accesos), administración de Oracle Enterprise Manager y WebLogic, soporte especializado en sistemas operativos Oracle Linux y Solaris (incluyendo actualizaciones, hardening y afinamiento del kernel), actualización de sistemas operativos en entornos virtualizados, gestión de ambientes de desarrollo, pruebas y producción, implementación de controles de seguridad de la información, elaboración de documentación técnica de configuraciones y cambios, soporte a servidores de aplicaciones, optimización de código y análisis de logs, verificación de espacio y recursos críticos, ejecución de mantenimientos programados, integración de bases de datos con otros sistemas institucionales y garantía de la disponibilidad permanente de los servicios tecnológicos asociados. 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. **ARQUITECTURA DE SOFTWARE**

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

	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 diseño, desarrollo e implementación de arquitecturas de software en entornos empresariales, con conocimientos y experiencia en Arquitectura de Software y Middleware Empresarial, orquestación de contenedores mediante Kubernetes, implementación de soluciones basadas en microservicios, Event Mesh y Service Mesh, refactorización de aplicaciones monolíticas, integración de mecanismos de mensajería como Apache Kafka, RabbitMQ y ActiveMQ, desarrollo Back End en Java (6, 7, 8, 11, 17, 21), desarrollo en ORACLE APEX , Kotlin, Node.js, Go o Python, y Front End con JavaScript o TypeScript utilizando frameworks modernos; experiencia en el uso de frameworks como Spring Boot, Spring Framework, JPA e Hibernate; gestión de bases de datos relacionales (Oracle, SQL Server, PostgreSQL) y NoSQL (Redis, Firebase Realtime Database); construcción e implementación de servicios web SOAP y REST bajo especificación OpenAPI 3.0; adopción de prácticas DevOps y CI/CD con herramientas como Jenkins, GitLab, SonarQube y Docker; conocimientos en observabilidad con Grafana y Datadog; así como implementación de esquemas de seguridad y autenticación basados en OAuth 2.0 y herramientas como Keycloak, trabajando bajo metodologías ágiles como Scrum 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. **DESARROLLO BACKEND** Profesional en Ingeniería de Sistemas o carreras afines, con título debidamente acreditado y experiencia mínima certificada de dos (2) años en proyectos de Tecnologías de la Información, de los cuales al menos un (1) año deberán corresponder específicamente a actividades de desarrollo backend, implementación de soluciones basadas en microservicios y automatización de despliegues; con conocimientos en desarrollo backend y manejo de herramientas de automatización; certificado como Java Certified Foundations Associate por Oracle y Oracle Certified Associate, Java SE 8 Programmer; con experiencia en desarrollo de aplicaciones backend usando Java y Spring Boot, participación en entornos de contenerización con Docker y orquestación local, automatización de despliegues (CI/CD), dominio de lenguajes de programación como Java, Python, PHP y Node.js, manejo de bases de datos SQL (MySQL, PostgreSQL), conocimientos en arquitecturas de microservicios y desarrollo de API REST, administración de servidores web Apache y Nginx, fundamentos de redes, buenas prácticas de seguridad informática y protección de datos, así como uso de Git para control de versiones y frameworks como Spring. **DESARROLLO DE SOFTWARE** Profesional en Ingeniería de Sistemas o carreras afines, con título debidamente acreditado y experiencia mínima certificada de dos (2) años en proyectos de Tecnologías de la Información, de los cuales al menos un (1) año corresponden específicamente a actividades de análisis, diseño, desarrollo, pruebas e implementación de soluciones de software y modernización tecnológica. Certificado como Oracle Certified Professional: Java SE 11 Developer, con sólidos conocimientos

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

	en desarrollo backend en Java, frameworks como Spring Boot y JPA, pruebas unitarias con JUnit, manejo de control de versiones (Git, GitHub, Apache Subversion), participación en proyectos bajo metodologías ágiles como Scrum y Kanban, dominio de lenguajes como Java, JavaScript, Python o C# desarrollo en ORACLE APEX, conocimiento en bases de datos relacionales y NoSQL, comprensión de desarrollo web frontend (HTML, CSS, JavaScript) y backend, experiencia con frameworks y bibliotecas modernas como React, Angular, Vue.js y Node.js, así como manejo de sistemas operativos Windows y Linux y buenas prácticas de integración continua en entornos colaborativos. 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. **DESARROLLO FULL STACK** 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 corresponden específicamente a actividades de desarrollo backend y frontend. Que posea certificaciones técnicas en Java Foundations Associate (Oracle), Angular 11 y en calidad de desarrollo de software. Tiene sólidos conocimientos en desarrollo de aplicaciones web full stack usando Java, Spring Boot y Angular, buenas prácticas de desarrollo, control de versiones con Git/GitHub, pruebas funcionales, estructuración de documentación técnica y trabajo en equipos multidisciplinarios bajo metodologías ágiles. En el ámbito Front-End, domina HTML, CSS y JavaScript, así como frameworks y bibliotecas como Angular, React o Vue.js; en Back-End, maneja lenguajes como Java, Node.js, Python, frameworks como Spring Boot, Express.js, Rails, bases de datos relacionales y no relacionales, servidores y redes, seguridad web y APIs RESTful, con habilidades en comunicación, colaboración, resolución de problemas y gestión de proyectos. 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. **ADMINISTRACION Y GESTION MIDDLEWARE** Profesional en Ingeniería de Sistemas, Ingeniería Electrónica, Ingeniería Telemática, Ingeniería en Telecomunicaciones o Ingeniería Informática, en Arquitectura o Construcción de Software u otras áreas 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 corresponden a actividades específicas en administración y despliegue de Oracle WebLogic Server, datalike y middleware empresarial. Este perfil deberá ser cubierto como mínimo por dos (2) profesionales designados por el contratista, en consideración a que dentro del alcance técnico se contempla la gestión de dos (2) tipos de entornos de capa media distintas (WebLogic Server y datalike), que requieren conocimientos y competencias específicas. Los profesionales deberán contar con experiencia en la gestión de Cuenta con las certificaciones Oracle WebLogic Server 12c Certified Implementation Specialist, Oracle Certified Professional (OCP) – Oracle WebLogic Server 12c, Oracle

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

	Data Integrator 12c Certified Implementation Specialist, y experiencia técnica en administración de dominios, clústeres, nodemanagers, seguridad (SSL, LDAP), tuning de rendimiento y despliegue continuo (CI/CD) de aplicaciones Java EE sobre WebLogic, así como conocimientos complementarios en Apache Tomcat. Además, tiene experiencia en Oracle Business Intelligence (OBIEE): instalación, configuración y soporte de servicios (BI Server), parametrización de catálogos, dashboards y seguridad por capas, integración con WebLogic y bases de datos Oracle, y en la implementación de buenas prácticas de seguridad, alta disponibilidad, balanceo de carga, tolerancia a fallos e integración de logs con soluciones de monitoreo. 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 DE APLICACIONES Y BASES DE DATOS DEL SICIE, 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.
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 directamente relacionados con el presente objeto contractual, deberá incluir en su oferta máximo 3 certificaciones, donde demuestre lo siguiente: Certificación expedida por entidades en las cuales hayan participado en proyectos iguales o similares, así:

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

	• Certificaciones expedidas por entidades en las cuales hayan participado en contratos de servicios de mantenimiento y soporte de capa media y aplicativos. • Certificaciones expedidas por entidades en las cuales hayan participado en contratos Soporte, sostenimiento, mantenimiento y actualización de aplicativos y bases de datos Oracle. Para efectos de verificar la certificación(es) de la empresa, emitidas por las entidades donde ha laborado o desarrollado proyectos con relación directa 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. Resaltando que los servicios que se prestaran durante el contrato y todos los relacionado con el anexo técnico, son de alta criticidad y con el fin de garantizar la calidad del servicio a contratar y evitar incumplimientos en la ejecución del contrato, se exige de forma adicional y obligatoria acreditar experiencia en mantenimiento, soporte de Bases de Datos Oracle mínimo de 18c o superior, en entornos de ALTA DISPONIBLIDAD, Oracle RAC y Oracle Dataguard. 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.

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

	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 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 la garantía técnica corresponderá a un documento escrito e independiente, establecidos para la garantía técnica del servicio, por un periodo de 6 meses posterior al término de la ejecución del contrato en el que se expresa explícitamente la aceptación y la obligatoriedad que se dará a

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

	la misma, teniendo en cuenta el comprometimiento con el cumplimiento de los siguientes aspectos: • Toda actividad de sostenimiento, mantenimiento, mejoras continuas en los aplicativos y base de datos del SICIE, asegurando su optimización y adaptación realizada sobre las aplicaciones y base de datos deben de ser implementadas bajo la metodología de desarrollo seguro con que cuenta el CAIMI. • Se debe ofrecer el servicio modernización y atención ilimitada de casos reportados ante cualquier evento relacionado con el funcionamiento lógico del hardware, Software, así como los servicios integrales de la solución durante la vigencia de la garantía. Para el personal que la entidad haya destinado para este proyecto, para ello el contratista deberá contar con un medio de recepción de reportes e incidentes y solicitudes de asistencia técnica, el cual debe ser informado a la entidad, al inicio de la ejecución del contrato. • Deberá responder por cualquier daño producido a los aplicativos, objeto de intervención, como los daños generados a bienes puestos a su disposición para la ejecución del respectivo contrato. • Ante la falta de estipulación legal que establezca el tiempo de garantía del sostenimiento a las bases de datos, aplicaciones y sistemas operativos de Oracle existentes en el CAIMI durante la duración del contrato, sin costo alguno para el Ejército Nacional. La garantía incluye el funcionamiento correcto de estos mantenimientos preventivos y correctivos a las bases de datos y sistemas operativos de Oracle existente, de tal forma que se garantice que operan adecuadamente sin afectar el sistema integrado de información.
3.2.8	**TERMINO DE RESPUESTA**
3.2.8.1	El contratista teniendo en cuenta el comprometimiento con el cumplimiento de los siguientes aspectos: • Se garantizará que el tiempo de respuesta para el sostenimiento de los aplicativos, base de datos del SICDI, deberá ser como máximo de dos (2) horas, garantizando la continuidad operativa del sistema. • Se deberá atender de inmediato los casos reportados por el personal administrador a través del Centro de Atención de Llamadas (CAL) y proporcionar soporte local bajo un Acuerdo de Nivel de Servicio (ANS) 7x24. La solución deberá restablecer el correcto funcionamiento del sistema, abordando incidentes o eventos que afecten cualquier componente de los aplicativos de inteligencia mencionados anteriormente. • Se pondrá a disposición del CAIMI, de manera permanente, los siguientes medios para el reporte de incidentes durante la ejecución del contrato y el término de la garantía de este, mesa de servicio o autoservicio con acceso vía web, Número telefónico, Correo electrónico, Número móvil celular de un contacto directo. • Se garantizará soporte técnico presencialmente, como primer nivel de atención.

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

	• El grupo de soporte garantizará que el ticket del problema tenga un seguimiento adecuado, se maneje rápida y eficientemente, y se lleve a los niveles adecuados hasta su cierre. Además, se informará constantemente por escrito al supervisor del contrato o quien éste delegue, los progresos en la búsqueda de la solución. • Durante el periodo de garantía, en un plazo de 24 horas evaluará la solución a las fallas presentadas entorno al funcionamiento y conexión que presente alguna falla de los sistemas operativos, aplicaciones y el motor de las bases de datos Oracle, que conforman el sistema integrado de información y los dejará en perfecto estado de funcionamiento en el menor tiempo posible • Durante el tiempo de la garantía se prestará todo el acompañamiento necesario para realizar correcciones sobre el servicio prestado. Brindar planes de acompañamiento y soporte técnico durante la ejecución del contrato y la garantía de este, en el cual se verifique el funcionamiento del soporte y mantenimiento. • Al momento de realizarse el uso de la garantía, se debe hacer entrega de un informe técnico al finalizar la actividad que los motivo donde se indique, Actividades realizadas, Actualizaciones aplicadas, Procedimientos preventivos y/o correctivos aplicados y Recomendaciones. • Se garantizará la corrección de fallas, bugs e imprevistos producto del mismo servicio, que surjan durante la ejecución y vigencia del contrato, de lo cual la entidad solicitará a través del supervisor del contrato, previa comunicación escrita o verbal al contratista cuantas veces sea necesario durante el tiempo de la garantía. El tiempo de respuesta de la garantía anterior, no será superior a cuatro (04) horas contadas a partir del requerimiento del respectivo servicio por parte de la Entidad. • Se garantizará un soporte adicional al 5x8 bajo esquema 7x24, con un tiempo de respuesta de atención inicial máximo de 2 horas.
3.2.9	**POLÍTICAS SEGURIDAD**
3.2.9.1	• Todo el personal que disponga el contratista para la prestación del servicio dentro de las instalaciones de la entidad contratante, deben realizar los trámites de estudio de seguridad personal, así como la asignación del respectivo fichero de identificación personal, por tal motivo el contratista debe cancelar el valor del fichero del personal asignado para prestar el servicio, al igual que estos funcionarios están obligados a portarlo en todo momento dentro de las instalaciones, ahora bien el contratante no está obligado a aceptar personal que no cumpla los parámetros de seguridad establecidos por la Institución, esto como medida de seguridad por tratarse del manejo de información clasificada. • El SICIE no incurrirá en gastos de transporte, alimentación, papelería, fotocopias, teléfonos o equipos de sistemas que el proveedor utilice para el debido cumplimiento del servicio, por lo cual se considera que todos los gastos adicionales estarán incluidos dentro de la propuesta final. • El contratista deberá firmar al inicio del proyecto una promesa de reserva donde garantiza la confidencialidad de la información institucional a la cual tenga acceso directamente o por intermedio de terceros, así como la que genere, como producto de la ejecución del presente proceso, contrato, y por

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

	tanto en ningún caso podrá divulgarla, copiarla, reproducirla o suministrarla a terceros. • El contratista se comprometa a conocer, aceptar y ajustarse a las políticas de seguridad informática del Ejército Nacional. En tal virtud, adoptará todas las medidas necesarias para impedir la duplicación, sustracción, divulgación, alteración, ocultamiento o utilización indebida de información. En ninguna circunstancia dicha información y/o documentación podrá ser utilizada por el contratista para fines distintos al desarrollo del contrato respectivo. Al finalizar la ejecución del proyecto toda la información y documentos entregados por el Ejército Nacional y producidos por el contratista, deberán ser retornados. • Una vez finalizado el contrato los equipos que sean utilizados tales como: portátiles, discos duros extraíbles, se les realizará un borrado seguro que garantice que no haya fuga de información. • Se prohíbe el ingreso y uso de computadoras personales, dispositivos de almacenamiento externo (USB, discos duros) y conexiones remotas o VPN sin autorización expresa.
3.2.10	**TRANSFERENCIA DE CONOCIMIENTO**
3.2.10.1	El contratista deberá realizar una transferencia de conocimiento para los funcionarios mensual de conocimiento al personal del CAIMI (mínimo 4 horas/semanales). Con relación al SOSTENIMIENTO DE APLICACIONES Y BASES DE DATOS DEL SICIE.
3.2.11	**PROPIEDAD INTELECTUAL Y RESTRICCIÓN DE DIFUSIÓN DE INFORMACIÓN**
3.2.11.1	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.

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

	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.

3.3 REQUISITOS DE EMPAQUE Y ROTULADO

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

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

- 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)
- 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 DE APLICACIONES Y BASES DE DATOS DEL SICIE	26/02/2025
01	Se realiza ajustes al Anexo Técnico SOSTENIMIENTO DE APLICACIONES Y BASES DE DATOS DEL SICIE, con relación a observaciones allegadas en el proceso de contratación No. 064-CENACINTELIGENCIA-2025.	27/07/2025
02	Se realiza ajustes al Anexo Técnico SOSTENIMIENTO DE APLICACIONES Y BASES DE DATOS DEL SICIE, con relación a mejora del documento técnico al ser revisado por el comité técnico estructurador.	21/08/2025

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

	Luego de realizar la revisión al anexo técnico el comité técnico estructurador realiza ajustes a los numerales.	
03	Se realiza ajustes al Anexo Técnico SOSTENIMIENTO DE APLICACIONES Y BASES DE DATOS DEL SICIE, 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
04	Se realiza ajustes al Anexo Técnico SOSTENIMIENTO DE APLICACIONES Y BASES DE DATOS DEL SICIE, 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.	03/02/2026
05	Se realiza ajustes al Anexo Técnico SOSTENIMIENTO DE APLICACIONES Y BASES DE DATOS DEL SICIE, con relación a mejora del documento técnico al ser revisado por la dupla del comité estructurador, donde se da claridad a los perfiles requeridos y experiencia numeral 3.2.5	13/02/2026
06	Se realiza ajustes al Anexo Técnico SOSTENIMIENTO DE APLICACIONES Y BASES DE DATOS DEL SICIE, con relación a mejora del documento técnico por observaciones allegadas en el proceso de evento de cotización, donde se da claridad perfiles requeridos y experiencia el numeral 3.2.4	23/02/2026
07	Se realiza ajustes al Anexo Técnico SOSTENIMIENTO DE APLICACIONES Y BASES DE DATOS DEL SICIE, con relación a mejora del documento técnico por observaciones allegadas en el proceso de pliegos de condiciones, donde se da anexa un perfil requeridos y experiencia el numeral 3.2.4	06/04/2026

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