ANEXO TÉCNICO
SOPORTE Y MANTENIMIENTO INFRAESTRUCTURA MICROSOFT, VMWARE, LINUX Y SOLUCIONES INFORMATICAS

CONTENIDO

1. OBJETO 2
2. DEFINICIONES Y APLICACIÓN 2
3. REQUISITOS.....4
4. TOMA DE MUESTRAS Y CRITERIO DE ACEPTACIÓN O RECHAZO: 14
5. MÉTODOS DE ENSAYO 15
6. APÉNDICE 15
7. ANEXOS 15
8. CONTROL DE REVISIONES 15

Elaboró	Revisó	Aprobó

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

1. OBJETO

El Subsistema de Inteligencia y Contrainteligencia del Ejército (SICIE), requiere el mantenimiento a la infraestructura Microsoft, VMware y soluciones informáticas con el fin de contribuir y garantizar el funcionamiento de sus distintas aplicaciones. Esta plataforma permite el flujo de información y los medios necesarios para soportar la producción de inteligencia al nivel nacional. La actualización y la revisión periódica de la plataforma permiten mitigar riesgos de ataque cibernéticos y problemas de disponibilidad integridad y confidencialidad de la información.

La plataforma Microsoft la conforman equipos y software que prestan el servicio tecnológico para el almacenamiento, procesamiento y flujo de información digital en el proceso de inteligencia. El incremento en la utilización de los servicios informáticos y cambios tecnológicos requieren que esta plataforma este actualizada y monitoreada por personal especializado para garantizar la disponibilidad del servicio del sistema de inteligencia.

2. DEFINICIONES Y APLICACIÓN

2.1 DEFINICIONES

SISTEMA OPERATIVO: En el mundo de la informática se denomina sistema operativo al programa, o conjunto de ellos, que gestiona los recursos físicos de un sistema informático (memoria, capacidad de procesamiento, espacio en disco duro, acceso a la red, etc.) y provee servicios a los programas de aplicación para que éstos funcionen correctamente. Todas las interacciones con el equipo físico son gestionadas por el sistema operativo por lo que son casi transparentes para el equipo que desarrolla la aplicación funcional que utiliza el usuario.

VMWARE: Es un sistema de virtualización por software VMware Inc., (VM de Virtual Machine) es una filial de EMC Corporation que proporciona software de virtualización disponible para ordenadores compatibles X86. Entre este software se incluyen VMware Server

HYPER-V: Es un programa de virtualización de Microsoft basado en un hypervisor para los sistemas de 64 bits, con los procesadores basados en Tecnología de virtualización.

CONTROLADORES DE DOMINIO: Un controlador de dominio es una entidad administrativa, no es un ordenador en concreto, sino un conjunto de ordenadores agrupados que se ciñen a unas reglas de seguridad y autenticación comunes. Para regular un dominio, se precisa al menos de un equipo que sea el controlador principal, la fuente primera donde se almacenan las reglas del dominio, y donde serán consultadas esas reglas en última instancia. Un controlador primario de dominio (PDC) puede implementarse tanto bajo Windows como bajo Linux. En este artículo vamos a contrastar ambas implementaciones.

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

FIRMWARE: El firmware o soporte lógico inalterable es un programa informático que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo. Está fuertemente integrado con la electrónica del dispositivo, es el software que tiene directa interacción con el hardware, siendo así el encargado de controlarlo para ejecutar correctamente las instrucciones externas. De hecho, el firmware es uno de los tres principales pilares del diseño electrónico. En resumen, un firmware es un software que maneja físicamente al hardware.

El programa BIOS de una computadora es un firmware cuyo propósito es activar una máquina desde su encendido y preparar el entorno para cargar un sistema operativo en la memoria RAM y disco duro.

MANTENIMIENTO PREVENTIVO: Es el proceso por el cual se mejora y optimiza el software que se ha instalado, este mantenimiento se realiza para la prevención de posibles problemas que puedan llegar a surgir a medida que se utiliza el equipo.

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.

NOTA: Entiéndase infraestructura informática, o sea, las plataformas y soluciones de Microsoft, VMware y demás soluciones informáticas instaladas y configuras en el CAIMI.

2.2 APLICACIÓN

Es de vital importancia que el servicio de mantenimiento de la infraestructura Microsoft, VMware y soluciones informáticas sea prestado para la vigencia 2026, sin ninguna interrupción, debido a que se requiere tener actualizado y soportado todos los equipos que componen los servicios informáticos del subsistema de inteligencia y contrainteligencia militar (SICIE), por ser un servicio prestado 7x24x365 debe de estar operativamente y disponible a los usuarios, por otra parte es necesario hacer el continuo monitoreo de la infraestructura para garantizar el perfecto funcionamiento de las aplicaciones que cuenta el SICIE, las cuales fueron desarrolladas por la sección de comunicaciones C6 CAIMI y otras son nativas desplegadas en la infraestructura tecnológica, por lo que se requiere contar con servicios de mantenimientos necesarios.

Para el comando de apoyo de combate de inteligencia militar, es indispensable garantizar disponibilidad de los servicios que conforman la infraestructura Microsoft, VMware y soluciones informáticas, cuya infraestructura soporta la actividad de inteligencia que realiza cada una de las unidades como es la recolección, análisis y difusión de productos de inteligencia para la toma de decisiones. Actualmente el CAIMI cuenta con un contrato con el No. 066-CENACINTELIGENCIA-2025 en ejecución el cual se desarrolla hasta el 30 de noviembre de 2025, por lo que se requiere dar continuidad al servicio de mantenimiento a la infraestructura Microsoft, VMware y soluciones informáticas del SICIE, por lo expuesto

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

anteriormente de no continuar con estos servicios se generaría un riesgo en la continuidad del servicio prestados al SICIE, siendo una vulnerabilidad ante cualquier tipo eventualidad que afecte su normal funcionamiento.

En relación a lo anterior es de suma importancia darle continuidad a los servicios mantenimiento preventivos a la infraestructura Microsoft, VMware y soluciones informáticas, manteniendo la alta disponibilidad de estos recursos informáticos, para el análisis, evaluación y toma de decisiones operacionales del SICIE; por esta razón es indispensable mantener la disponibilidad, seguridad e integridad de la misma, el sostenimiento a dichas herramientas y aplicaciones de la infraestructura Microsoft, VMware y soluciones informáticas, 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 cualquier falla presentada en la aplicación puede generar la indisponibilidad de los servicios informáticos mencionados o la pérdida parcial o total de la información del SICIE.

3. REQUISITOS

3.1 REQUISITOS GENERALES

Adquisición de servicio de mantenimiento de la infraestructura Microsoft, VMWARE y soluciones informáticas, contemplando actividades de soporte técnico y mantenimiento preventivo en sitio y/o remoto de las unidades a nivel nacional, de las plataformas que tiene la entidad y que se encuentran instaladas y configuradas en el CAIMI, durante la ejecución del contrato.

3.2 REQUISITOS ESPECÍFICOS

ÍTEM	DESCRIPCIÓN
3.2.1	**MANTENIMIENTO DE LA INFRAESTRUCTURA MICROSOFT, VMWARE Y SOLUCIONES INFORMATICAS**
3.2.1.1	Se deberá llevar a cabo la coadministración, creación y el correcto funcionamiento de la infraestructura Microsoft Windows, VMware, Hyper-V, Exchange, almacenamientos y soluciones informáticas con las cuales cuenta el Subsistema de Inteligencia y Contrainteligencia del Ejército (SICIE). **A)** Microsoft Active Directory • Administración de réplica Sysvol • Administración de relación de confianza a nivel de bosque • Administración e Información de supervisión de desviación horaria • Detalles sobre el estado y el rendimiento de la réplica en la red • Administración del Servicio de réplica de archivos (FRS) • Administración de la réplica de archivos distribuidos (DFS-R) • Estado de red de Active Directory • Administración de DNS relevantes para Active Directory • Administración de Objetos políticas de seguridad • Administración de objetos del directorio activo

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

	B) Microsoft CA (Certification Authority) • Creación de certificados digitales • Creación de plantillas de certificados digitales • Revocación de plantillas • Administración de nombres de servicio de directorio activo • Administración de subordinadas de CA **C)** Microsoft Exchange Server. • Configuración y mantenimiento de DAG y Mailbox • Migración de todos los servidores de Exchange Server a última versión • Creación de bases de datos Exchange • Manteamiento de bases de datos Exchange • Manteamiento sistema de archivos Exchange • Creación de políticas de Exchange • Instalación de certificados SSL Exchange • Administración de objetos Exchange server • Manteamiento a los servidores CAS • Manteamiento los servidores MAILBOX • Creación y configuración de NLB Round Robin **D)** Plataforma WSUS • Despliegue de 14 servidores Downstream • Sincronización de OU con WSUS • Autorización de actualizaciones y despliegues de parches • Sincronización de Downstream con el Upstream • Creación de contenedores en el WSUS **E)** Políticas de seguridad (Microsoft Security Compliance y Microsoft Advanced Threat Analytics) • Administración de base de datos ATA • Centro de administración de ATA • Generación de informes de ATA • Administración grupos y roles ATA • Etiquetar cuentas confidenciales **F)** Proxy Reverso Enrutamiento de Solicitudes de aplicación • Creación de sitios web. • Aprovisionamiento y administración de IIS. • Configuración de seguridad. • Administración de la configuración del rendimiento • Administración de las opciones de configuración **G)** HYPER-V • Supervisar los recursos y el rendimiento del host de Hyper-V • Ver el inventario de máquinas virtuales • Creación de una máquina virtual • Cambiar la configuración de la máquina virtual

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

- Migrar en vivo una máquina virtual a otro nodo de clúster
- Administración avanzada y solución de problemas de las máquinas virtuales
- Administrar una máquina virtual a través del host de Hyper-V (VMConnect)
- Cambiar la configuración del host de Hyper-V
- Ver registros de eventos de Hyper-V

H) Funcionamiento plataforma VMWare.(servidores)

- Implementar máquinas virtuales
- Administración maquinas virtuales
- Implementación de plantillas OVF
- Configuraciones de opciones máquinas virtuales
- Supervisión de Vcenter y ESXI
- Inventario del Vcenter
- Supervisión de ESXI

1.Sostenimiento de Servidores de almacenamiento NAS Y SAN

- Implementar todos los recursos compartidos
- Administración de servidores SAN Y NAS
- Migración de servidores SAN y NAS
- Implementación de Políticas SAN y NAS
- Configuraciones recursos compartidas y Backups

Se deberá de realizar las siguientes actividades a todos los componentes y herramientas anteriormente descritos como lo son la actualización (Upgrade, Update, criticas de Seguridad), revisión y solución de errores, realización y programación de copias de seguridad, revisión logs, revisión y mejoramiento de espacio de disco, utilización de CPU – RAM y desinstalación de funcionalidades inoperativas.

Se debe suministrar el certificado digital SSL del dominio IMI por un año. Es un certificado digital que autentica la identidad de un sitio web y permite una conexión segura entre el navegador del usuario y el servidor web, utilizando el protocolo HTTPS. Estos certificados son emitidos por autoridades de certificación (CA) y contienen información sobre el sitio web, como el nombre de dominio, la clave pública y la firma digital de la CA. La instalación de certificados digitales SSL, que garantizan la seguridad de las comunicaciones cifradas, se relaciona principalmente con el control A.8.24 "Uso de Criptografía" de la norma ISO 27001:2022. Este control se enfoca en asegurar la confidencialidad, integridad, autenticidad y disponibilidad de la información mediante el uso de técnicas criptográficas, incluyendo certificados SSL.

Se debe suministrar el certificado digital SSL para Microsoft Exchange por un año. El cual se utiliza para cifrar y proteger la comunicación entre el servidor Exchange y los clientes (como Outlook, Exchange ActiveSync, etc.). Estos certificados garantizan la identidad del servidor y la seguridad de la información transmitida, evitando que terceros puedan interceptar o manipular los datos. La instalación de certificados digitales SSL, que garantizan la seguridad de las comunicaciones cifradas, se relaciona principalmente con el control A.8.24 "Uso de Criptografía" de la norma ISO 27001:2022. Este control se enfoca en asegurar la confidencialidad, integridad, autenticidad y disponibilidad de la información mediante el uso de técnicas criptográficas, incluyendo certificados SSL.

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

	En caso de que el oferente adquiera una licencia más actualizada para Exchange y se requiera migrar el servicio de correspondencia a última versión, el contratista deberá preparar, ejecutar y garantizar dicha migración, si por el contrario el oferente no adquiere últimas versiones, deberá sostener, optimizar y asegurar el funcionamiento del sistema actual. Se deberá migrar el correo Exchange a última versión si la entidad cuenta con el licenciamiento requerido para esta ejecución. Se deberá migrar el directorio activo de Windows server a última versión si la entidad cuenta con el licenciamiento requerido para esta ejecución. Se debe presentar un plan de contingencia y un plan de restauración para recuperación y restauración de backups por plataforma, además un reporte de corrección de vulnerabilidades.
	HERRAMIENTA DE AUDITORIA
3.2.1.2	Teniendo en cuenta la pluralidad de las diferentes herramientas para el monitoreo y control de cambios, el contratista deberá suministrar e implementar sin generar ningún costo adicional al oferente unas soluciones que permita auditar en Active Directory (AD), Microsoft Exchange y sistemas de almacenamiento SAN y NAS a nivel empresarial, estas soluciones con el fin de garantizar la integridad, disponibilidad y confidencialidad de la información del SICIE. Estas herramientas deben ser versiones pagas, con licencia comercial y soporte oficial del fabricante; no se aceptarán soluciones de prueba, freeware o software de código abierto sin soporte oficial. **NOTA:** Es de aclarar que el oferente cuenta con catorce (14) controladores de dominio, cuatro (04) SAN, cuatro (04) NAS y un (01) clúster de file server con cobertura de cinco mil (5.000) buzones de correo.
3.2.2	**GENERALIDADES DEL SERVICIO**
3.2.2.1	El contratista deberá de hacer un informe diagnóstico a más tardar 15 días calendario contados a partir de la firma del acta de inicio, donde como resultado de este diagnóstico informará el esquema de cómo se encuentran conformadas de manera física y de manera virtual incluyendo servidores, direcciones IP, Racks y un informe del estado actual de la infraestructura Microsoft Windows, VMware, Hyper-V, Exchange, almacenamientos y soluciones informáticas, con recomendaciones y plan de trabajo para implementar los ajustes a que haya lugar (reinstalación, reconfiguración, actualizaciones de Services Packs a las últimas versiones disponibles, entre otros). El contratista deberá ejecutar Microsoft Advanced Threat Analytics y se deberán implementar las políticas de seguridad recomendadas por Microsoft en el Security Compliance Manager previa aprobación por parte del CAIMI. El contratista debe garantizar la continuidad y permanencia del recurso inicialmente asignado; Cualquier cambio de personal por parte del contratista deberá ser aprobado por el supervisor designado y el Administrador de las Plataformas de la inteligencia, previa solicitud por escrito con cinco (05) días hábiles de anticipación.

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

	El contratista dará en su informe al supervisor del contrato, un asesoramiento a la implementación de nuevas funcionalidades en pro de la mejora de infraestructura Microsoft Windows, VMware, Hyper-V, Exchange, almacenamientos y soluciones informáticas con las cuales cuenta la institución para mejoras en los servicios actuales o para la introducción de nuevas tecnologías, que permitan mejorar el desempeño tecnológico. El contratista de ser necesario garantizará el servicio de soporte técnico a través de herramientas WEB online cuando las circunstancias así lo requieran (24x7) y en sitio (8x5) en el edificio del CAIMI ubicado en la ciudad de Bogotá D.C., para las unidades fuera de la ciudad de Bogotá D.C., el soporte y mantenimiento podrá ser prestado remotamente desde el CAIMI. El contratista debe brindar atención ilimitada a casos reportados por el CAIMI, referentes a cualquier evento relacionado con el funcionamiento, administración, incidentes o eventos de seguridad de los sistemas, o plataformas, hasta dejar en completo funcionamiento la misma de acuerdo a los tiempos de respuesta relacionados en a continuación. El contratista garantizará el perfecto funcionamiento y la continuidad de los procesos y servicios prestados de la infraestructura Microsoft Windows, VMware, Hyper-V, Exchange, almacenamientos y soluciones informáticas del SICIE. Por lo anterior, los costos relacionados a los daños causados por el personal o recursos asignados por el contratista, para el cumplimiento del objeto del contrato, serán asumidos por el contratista, donde la novedad presentada será verificada y avalada por el supervisor del mismo. Se debe efectuar como mínimo un (01) mantenimiento preventivo mensual del software, de la infraestructura Microsoft Windows, VMware, Hyper-V, Exchange, almacenamientos y soluciones informáticas durante la ejecución del contrato según cronograma acordado con el supervisor del contrato, el cual quedará establecido en el acta de inicio. El contratista debe, a nivel preventivo soportar, operar, monitorear y coadministrar resolución de incidentes (soporte y solución de fallas de TI) nivel uno, dos y tres en todos los sistemas de servidores Windows en sus versiones 2012 R2, 2016, 2019, 2022 o superiores ofrecidas en el mercado por el fabricante e instaladas en la institución. El contratista debe, a nivel preventivo soportar, operar, monitorear y coadministrar resolución de incidentes (soporte y solución de fallas de TI) nivel uno, dos y tres en todos los sistemas de correo de la organización Exchange 2013, con sus roles CAS, MAILBOX Y PROXY REVERSO. El contratista debe, a nivel preventivo soportar, operar, monitorear y coadministrar resolución de incidentes (soporte y solución de fallas de TI) nivel uno, dos y tres en todos los sistemas que estén compuestos por un VCENTER de VMWARE y ESXI, que se encuentran en VMOTION, los cuales están en alta disponibilidad en versión 6.0 o superior que son con los que cuenta la organización. El contratista debe, a nivel preventivo soportar, operar, monitorear y coadministrar resolución de incidentes (soporte y solución de fallas de TI) nivel uno, dos y tres en todos los sistemas de auditoria proporcionados.

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

	El contratista debe, a nivel preventivo soportar, operar, monitorear, y gestionar todos los sistemas de Directorio Activo, SYSVOL, NTDS y roles FSMO al igual que su replicación constante y efectiva. El contratista debe, a nivel preventivo soportar, operar, monitorear, y gestionar todos los sistemas de virtualización basados en Hyper-V donde estarán incluidos los nodos y máquinas virtuales en estos sistemas. El contratista debe, a nivel preventivo soportar, operar, monitorear, y gestionar todos los roles del sistema de certificados digitales que se encuentran configurados en la entidad certificadora de la organización. El contratista debe, a nivel preventivo soportar, operar, monitorear, y gestionar todos los sistemas de WSUS con todos sus Downtream y Upstream. El contratista dispondrá de los computadores y demás recursos tecnológicos necesarios para el desarrollo de las actividades del recurso en sitio (8x5) y remoto (24x7), este computador y/o demás recursos serán incluidos dentro de la red y se ajustarán a las condiciones establecidas por la entidad y los protocolos de seguridad de la información del SICIE, una vez finalizado el contrato, se retirarán cumpliendo con los protocolos y los requisitos de seguridad establecidos por la entidad.
3.2.3	**PERFILES Y DOCUMENTACION REQUERIDA**
3.2.3.1	El contratista. debe anexar dentro de su oferta, documentación requerida para garantizar que cuenta con personal capacitado para el presente proceso, como mínimo uno (01) o máximo cuatro (04) recursos y que, en la sumatoria cuenten y cumplan con las siguientes certificaciones. • **Microsoft Windows Server Hybrid Administrator Associate:** valida las habilidades de un profesional de TI para gestionar y administrar tecnologías Windows Server en entornos híbridos, que combinan infraestructura local con servicios en la nube, especialmente en Azure. Esta certificación se enfoca en la implementación, administración y seguridad de cargas de trabajo de Windows Server en entornos híbridos y en la nube, así como en la integración de servicios de Azure con entornos locales para soluciones híbridas • **Exchange Server Subscription Edition (SE):** se refiere a la última versión del servidor de correo y calendario de Microsoft, que se ofrece a través de un modelo de suscripción. Esta certificación valida que un profesional tiene los conocimientos y habilidades necesarios para implementar, administrar y mantener Exchange Server SE en entornos locales, en la nube o híbridos. • **VMware Certified Professional 6 o superior - Data Center Virtualization" (VCP-DCV):** valida las habilidades y conocimientos de un profesional en la implementación y administración de soluciones VMware vSphere, incluyendo máquinas virtuales, redes y almacenamiento. • **Azure Virtual Desktop Specialty:** valida las habilidades de un profesional en la planificación, implementación, administración y seguridad de escritorios virtuales en Azure. Se centra en la experiencia del usuario, escalabilidad, rendimiento y administración de identidades en entornos de escritorios virtuales basados en la nube.

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

	• **IPv6 Certified Network Associate (IPv6-CNA):** valida los conocimientos y habilidades de un profesional en redes en el ámbito de IPv6, el protocolo de internet más reciente. Esta certificación, a menudo ofrecida por organizaciones como APNIC, se centra en los fundamentos de IPv6, incluyendo configuración, direccionamiento, enrutamiento y seguridad. El objetivo principal es asegurar que los profesionales estén preparados para implementar y gestionar redes que utilicen IPv6, un protocolo crucial para el futuro de internet debido a la escasez de direcciones IPv4. Para su verificación de las certificaciones del personal designado el contratista deberá anexar copia del transcript emitido por Microsoft o por el fabricante o casas oficiales de certificación requerido con usuario y contraseña, para ser verificado a través de la página: www.microsft.com/learning/mcp/transcript, o la que corresponda, esto garantiza capacidad, conocimiento idóneo, profesionalismo, experiencia en este tipo de soluciones y que la entidad pueda confirmar y avalar los recursos propuestos. Lo anteriormente exigido es de vital importancia para el soporte, mantenimiento, monitoria, sostenimiento, actualización y migración de la infraestructura Microsoft Windows, VMware, Hyper-V, Exchange, almacenamientos y soluciones informáticas, a fin de cubrir todos los requerimientos técnicos solicitados y en los que deben de realizar asistencia técnica, afinamiento de la plataforma, soporte técnico de primer, segundo y tercer nivel descritos y mantenimiento en sitio de todos los productos y/o servicios que conforman los equipos de comunicaciones y computación para las aplicaciones y plataformas descritas anteriormente.
3.2.4	**EXPERIENCIA Y PERFIL DEL PROPONENTE**
3.2.4.1	Se deberá de anexar en la propuesta un documento emitido por Microsoft donde se evidencie que se encuentra inscrito en el programa “Microsoft Partner Network”, acreditar por Microsoft que es “Partner de Microsoft”. Se deberá anexar copia de certificaciones de experiencia y/o contratos terminados donde se pueda certificar que cuenta con la experiencia en las herramientas aquí relacionadas. Es decir, al menos (2) Certificaciones de experiencia especifica en la participación de proyectos de implementación y/o servicios objeto del contrato. Lo anterior con el fin de garantizar capacidad, conocimiento idóneo, profesionalismo y experiencia en este tipo de soluciones. El Ministerio de Defensa Nacional - Ejercito Nacional- CAIMI, se reserva el derecho a comprobar la autenticidad de los certificados y/o contratos si así fuese necesario. Los cuales deben tener como mínimo la siguiente información: **1.**Fecha de inicio y terminación **2.**Objeto del contrato **3.**Tiempo y valor del servicio contratado **4.**Firma de la persona encargada **5.**Recibo a satisfacción en caso de aplicar.
3.2.5	**POLÍTICAS SEGURIDAD**
3.2.5.1	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

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

	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. La entidad contratante 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 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, y se restringe el uso de equipos móviles exclusivamente para funciones laborales aprobadas, garantizando la seguridad y confidencialidad de la información.
3.2.6	**ACUERDOS DE CONFIDENCIALIDAD**
3.2.6.1	El contratista y el personal que formará parte del grupo de trabajo deberán firmar al inicio del proyecto un acuerdo de confidencialidad donde garantizan la confidencialidad de la información Institucional a la cual tengan acceso directamente o por intermedio de terceros, así como la que genere, como producto de la ejecución del presente contrato, y por tanto en ningún caso podrá divulgarla, copiarla, reproducirla o suministrarla a terceros. Por lo anterior es indispensable que el oferente se comprometa a conocer, aceptar y ajustarse a las políticas de seguridad de la información del MDN- CGFM-Ejército Nacional-IMI, así como aceptar y permitir que la IMI efectúe los estudios de seguridad al personal de la empresa contratista que considere necesario, para garantizar la seguridad de su infraestructura computacional e información. En tal virtud, adoptará todas las medidas necesarias para impedir la duplicación, sustracción, divulgación, alteración, ocultamiento o utilización indebida de información. Bajo ninguna circunstancia dicha información y/o documentación podrá ser utilizada por el personal de la empresa contratista para fines distintos al desarrollo del contrato respectivo. Al finalizar la ejecución del proyecto toda la información y documentos entregados por la IMI, deberán ser retornados.

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

3.2.7	**GARANTIA TECNICA**
3.2.7.1	El oferente al momento de la oferta deberá de anexar la garantía técnica corresponderá a un documento escrito e independiente, en el que se expresa explícitamente la aceptación y la obligatoriedad que se dará a la misma, teniendo en cuenta el comprometimiento con el cumplimiento de los siguientes aspectos: **A.** 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. **B.** Se debe ofrecer el servicio de soporte técnico 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. **C.** El contratista debe ofrecer asistencia técnica, respuesta calificada a consultas, aclaración de dudas, sobre el conjunto de hardware, software y servicios integrales de la solución, 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. **D.** El contratista debe 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. **E.** Durante el tiempo de la garantía el contratista 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. **F.** El contratista cuando se realice 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. **G.** El contratista se obliga a que el tiempo de respuesta de la garantía anterior, no será superior a cuatro (02) horas contadas a partir del requerimiento del respectivo servicio por parte de la Entidad. El contratista 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.
3.2.8	**TERMINO DE RESPUESTA**
3.2.8.1	**Soporte de Primer Nivel:** Los casos de atención de primer nivel serán asumidos por el recurso asignado en sitio dentro del horario estipulado.

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

	Soporte de Segundo Nivel: En este nivel comprenden los incidentes escalados al contratista por parte del recurso asignado en sitio, que requieren mayor capacidad profesional para ser solucionados, se hace claridad que el recurso asignado también podrá atender estos casos. **Soporte de Tercer Nivel:** Será prestado por el Centro de soporte regional de Microsoft a través del contratista, sin extinguir la responsabilidad de este en la solución del incidente. Mantenimiento en sitio de todos los productos y/o servicios que conforman de la infraestructura Microsoft Windows, VMware, Hyper-V, Exchange, almacenamientos y soluciones informáticas, quien se dedicará a la gestión, administración y servicio profesional en sitio (CAIMI), en horario de ocho (08) horas diarias cinco días a la semana, durante la ejecución del contrato.
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. La entidad contratante 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 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, y se restringe el uso de equipos móviles exclusivamente para

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

	funciones laborales aprobadas, garantizando la seguridad y confidencialidad de la información.
3.2.10	**MANUALES TECNICOS**
3.2.10.1	El contratista deberá entregar manuales técnicos y/o de administración actualizados en su última versión referentes a la infraestructura Microsoft Windows, VMware, Hyper-V, Exchange, almacenamientos y soluciones informáticas de cada una de las plataformas y/o infraestructura con la que cuenta la plataforma tecnológica del Subsistema de Inteligencia y Contrainteligencia del Ejercito (SICIE). **NOTA:** En el caso de presentarse una actualización de versión o incidente no contemplado en alguna de las plataformas anteriormente descritas, el contratista debe actualizar y/o entregar un nuevo manual técnico con dicha versión.

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.

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

Omitido.

5. MÉTODOS DE ENSAYO

Omitido.

6. APÉNDICE

6.1 NORMAS QUE DEBEN CONSULTARSE

- Directiva Permanente No.00200 de 2017 "COMPUTACION"
- Plan No. 00005514 DEL 02 DE MARZO DE 2020 "LINEAMIENTOS PARA EL CUMPLIMIENTO DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y USO SEGURO DE EQUIPOS DE CÓMPUTO Y DISPOSITIVOS ELECTRÓNICOS PARA EL AÑO 2020.
- Directiva Permanente No. Radicado 0123000354502 /MDN-COGFM- JEMCO-SEMPE-CGDJ6-DIPCO-ARFOE del 28 de agosto de 2023 "Lineamientos para la implementación de la metodología para la gestión de los proyectos de Tecnologías de la Información y las Comunicaciones (TIC) para las Fuerzas Militares y el Comando General de las Fuerzas Militares.
- Decreto 199 del 20 de febrero de 2024, "Por el cual se establece el Plan de Austeridad del Gasto 2024 para los órganos que hacen parte del Presupuesto General de la Nación".
- RESOLUCIÓN No.7870 del 26 de diciembre de 2022 Por la cual se emite y adopta la Política General de Seguridad y Privacidad de la información, Seguridad Digital, Ciberseguridad y Continuidad de los Servicios Tecnológicos en las Unidades Ejecutoras o Dependencias del Ministerio de Defensa Nacional, Policía Nacional y entidades adscritas y vinculadas al Sector Defensa, y se dictan otras disposiciones.
- Plan Estratégico de Tecnologías de la Información PETI 2022-2026.
- 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

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

Revisión y/o Actualización	Modificaciones	Fecha
00	Creación del Anexo Técnico SOPORTE Y MANTENIMIENTO INFRAESTRUCTURA MICROSOFT, VMWARE, LINUX Y SOLUCIONES INFORMATICAS	26/02/2025
01	Se realiza ajustes al Anexo Técnico SOPORTE Y MANTENIMIENTO INFRAESTRUCTURA MICROSOFT, VMWARE, LINUX Y SOLUCIONES INFORMATICAS	01/08/2025

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