ANEXO ESPECIFICACIONES TECNICAS DE OBLIGATORIO CUMPLIMIENTO

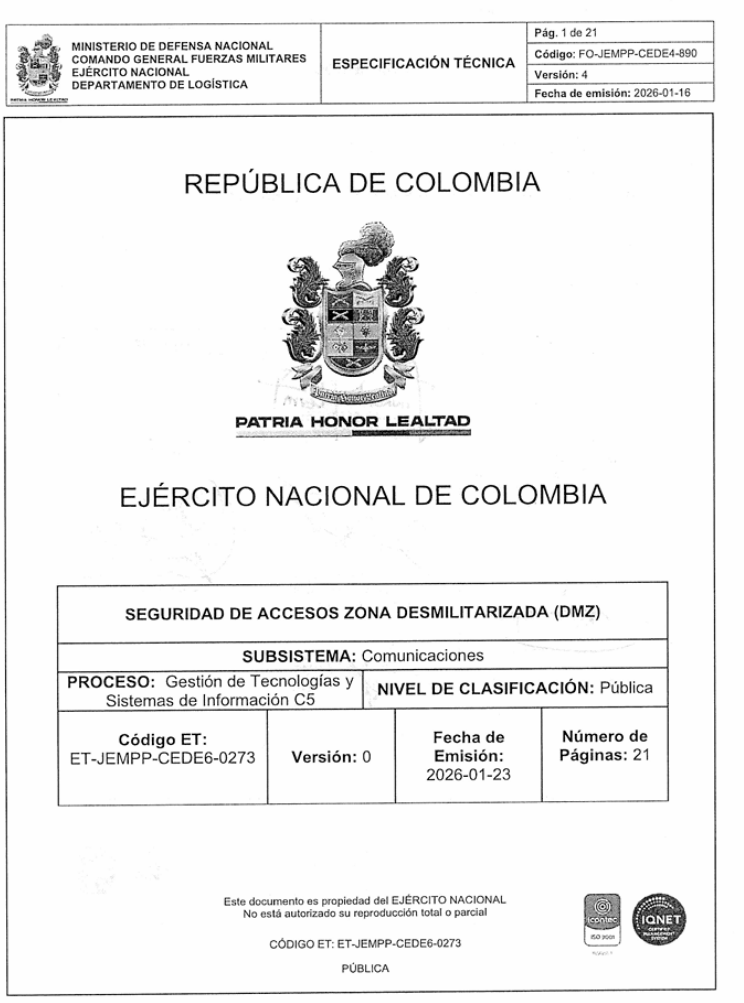
Facatativá XX de XXXXX de 2026

(El apoderado o representante legal), obrando en nombre y representación de conformidad con lo establecido en la Invitación a ofertar, ofertó de forma irrevocable, los siguientes bienes o servicios objeto del presente proceso de contratación, con las siguientes características técnicas:

CUMPLIMIENTO

NORMAS Y/O FICHAS TÉCNICAS Y/O ESPECIFICACIONES TÉCNICAS DE OBLIGATORIO CUMPLIMIENTO

Para efectos de establecer las especificaciones técnicas del presente proceso, se dará aplicación a las especificaciones técnicas del **"SEGURIDAD DE ACCESOS ZONA DESMILITARIZADA (DMZ) No. No. ET-JEMPP-CEDE6-0273** y las **ESPECIFICACIONES TECNICAS ADICIONALES DE OBLIGATORIO CUMPLIMIENTO** No. 2026574010702623/MDN-COGFM-COEJC-SECEJ-JEMOP-CAOCC-BRICC-BAICC-CPCB-29.25, de fecha 16 de marzo de 2026, las cuales contienen los parámetros técnicos que deben cumplir los oferentes en la acreditación del servicio, así mismo, el contenido es el mismo del **ANEXO ESPECIFICACIONES TÉCNICAS**, los cuales se describen a continuación:



MINISTERIO DE DEFENSA NACIONAL COMANDO GENERAL FUERZAS MILITARES EJÉRCITO NACIONAL DEPARTAMENTO DE LOGÍSTICA	ESPECIFICACIÓN TÉCNICA	Pág. 1 de 21 Código: FO-JEMPP-CEDE4-890 Versión: 4 Fecha de emisión: 2026-01-16

REPÚBLICA DE COLOMBIA

PATRIA HONOR LEALTAD

EJÉRCITO NACIONAL DE COLOMBIA

SEGURIDAD DE ACCESOS ZONA DESMILITARIZADA (DMZ)			
SUBSISTEMA: Comunicaciones			
PROCESO: Gestión de Tecnologías y Sistemas de Información C5		**NIVEL DE CLASIFICACIÓN:** Pública	
Código ET: ET-JEMPP-CEDE6-0273	**Versión:** 0	**Fecha de Emisión:** 2026-01-23	**Número de Páginas:** 21

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

CONTENIDO

1. OBJETO 3
2. DEFINICIONES, CLASIFICACIÓN Y APLICACIÓN 3
3. REQUISITOS 10
4. TOMA DE MUESTRAS Y CRITERIO DE ACEPTACIÓN O RECHAZO 16
5. MÉTODOS DE ENSAYO 17
6. APÉNDICE 18
7. ANEXOS 20
8. CONTROL DE REVISIONES 21

Elaboró	Revisó	Aprobó
SV. JOHN FREDDY RUBIO Suboficial analista seguridad Interna Batallón de Ciberdefensa y Ciberseguridad del Ejercito Nacional **PD02 SERGIO ARTURO ALFONSO** PD02 Profesional de Defensa Batallón de Ciberdefensa y Ciberseguridad del Ejercito Nacional	**CT. JINNA MARCELA DEVIA PEREZ** Oficial de Planificación y políticas **MY. FREDY MAURICIO RUIZ GUTIERREZ** Ejecutivo y Segundo Comandante del Batallón de Ciberdefensa y Ciberseguridad del Ejercito Nacional **TC. ROGER JESUS BUELVAS NARVAEZ** Comandante Batallón de Ciberdefensa y Ciberseguridad del Ejercito Nacional	**CR. EDWARD ENRIQUE AREVALO RIOS** Comandante Brigada de Interoperabilidad Computación Comunicaciones y Ciberdefensa

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

1. OBJETO

La presente especificación técnica tiene por objeto fortalecer y modernizar la infraestructura tecnológica del Ejercito Nacional con un sistema de SEGURIDAD DE ACCESOS ZONA DESMILITARIZADA (DMZ) para el Ejército Nacional con la finalidad de contar con un equipo especializado que separe los servicios accesibles desde internet (como servidores web, correo o DNS) de la red interna del Ejército Nacional, asegurando las aplicaciones y optimizando la transferencia de datos frente a las nuevas amenazas de naturaleza cibernética.

2. DEFINICIONES, CLASIFICACIÓN Y APLICACIÓN

2.1 DEFINICIONES

Arquitectura abierta de red:[1] Es el conjunto de características técnicas de las redes de telecomunicaciones que les permite interconectarse entre sí a nivel físico y lógico, de tal manera que exista interoperabilidad entre ellas. (Decreto 2870 de 2007, Artículo 2º).

BGP:[2] El protocolo de puerta de enlace fronteriza (BGP) es un conjunto de reglas que determinan las mejores rutas de red para la transmisión de datos en Internet.

CLI:[3] Una interfaz de la línea de comandos (CLI) es un mecanismo de software que se utiliza para interactuar con el sistema operativo mediante el teclado.

Conectividad: [4] Modelo de cofinanciación en el que participen constructores, beneficiaros VIS, prestadores de servicios de Internet, y el Estado.

Data Center:[5] es una instalación que centraliza las operaciones y el equipo de TI de una organización, así como el lugar donde ésta almacena, administra y difunde sus datos.

---

[1] Ministerio de las Tecnologías de la información (2021) *https://www.mintic.gov.co/portal/inicio/Glosario/*

[2] Amazon AWS (2024) *https://aws.amazon.com/es/what-is/border-gateway-protocol/*

[3] Amazon AWS (2024) *https://aws.amazon.com/es/what-is/cli/*

[4] Ministerio de las Tecnologías de la información (2021) *https://www.mintic.gov.co/portal/inicio/Glosario/*

[5] PowerData (S.F) *https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/data-center-definicion-tipos-y-tendencias*

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

DMZ:[6] Una DMZ o zona desmilitarizada es una red perimetral que protege y agrega una capa adicional de seguridad a la red de área local interna de una organización del tráfico no confiable.

Disponibilidad:[7] Propiedad de que la información y sus recursos relacionados deben estar disponibles y utilizables cuando se los requiera.

FEC:[8] "La corrección de errores de reenvío (FEC) es un proceso de adición de un código de corrección de errores (ECC) a un mensaje («carga útil») para que esto pueda ser recuperado por un receptor incluso cuando se introdujeron múltiples errores". (Texto traducido del inglés - Forward Error Correction).

Fibra óptica:[9] a fibra óptica es un filamento de material dieléctrico, como el vidrio o los polímeros acrílicos, capaz de conducir y transmitir impulsos luminosos de uno a otro de sus extremos. Estos hilos pueden llegar a ser tan finos como un pelo y por ellosse transfiere una señal luminosa desde un extremo del cable hasta el otro. Esta luz puede ser generada mediante un láser o un LED.

Gbps:[10] Significa «Gigabits por segundo». Gbps es una unidad de medida de la velocidad de transferencia de datos. Indica qué tan rápido se pueden transmitir datos en una red. Es comúnmente usada para expresar la velocidad de internet o la capacidad de conexiones de red.

GUI:[11] La GUI es una interfaz entre la persona y la máquina. El objetivo de esta interfaz gráfica es representar el código del backend de un sistema de la forma más clara posible para el usuario para simplificarle las tareas diarias.

Interconexión:[12] Es la vinculación de recursos físicos y soportes lógicos, incluidas las instalaciones esenciales necesarias, para permitir el interfuncionamiento de las redes y la interoperabilidad de servicios de telecomunicaciones.

Interferencia:[13] Es la interconexión que permite a cualquiera de los operadores interconectados, cursar el tráfico de otros operadores a la red del operador

---

[6] *Fortinet (2025) https://www.fortinet.com/lat/resources/cyberglossary/what-is-dmz)*

[7] Ministerio de las Tecnologías de la información (2021) *https://www.mintic.gov.co/portal/inicio/Glosario/*

[8] Nvidia (2023) *https://docs.nvidia.com/networking/display/cablemanagfaq/frequently+asked+questions+(faq)*

[9] Redes&Telecom (2024) *https://www.redestelecom.es/especiales/fibra-optica-que-es-como-funciona-y-mejores-aplicaciones/*

[10] Lenovo (2025) *https://www.lenovo.com/co/es/glosario/gbps*

[11] IONOS Digital (2025) Guide *https://www.ionos.com/es-us/digitalguide/paginas-web/desarrollo-web/que-es-una-gui/*

[12] Ministerio de las Tecnologías de la información (2021) *https://www.mintic.gov.co/portal/inicio/Glosario/*

[13] Ministerio de las Tecnologías de la información (2021) *https://www.mintic.gov.co/portal/inicio/Glosario/*

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

interconectante, siempre que no se contravenga el reglamento para cada servicio. El solo servicio portador entre dos redes no se considera interconexión indirecta [1]

Interoperabilidad: [14] Habilidad de transferir y utilizar información de manera uniforme y eficiente entre varias organizaciones y sistemas de información. (Gobierno de Australia). Habilidad de dos o más sistemas (computadoras, medios de comunicación, redes, software y otros componentes de tecnología de la información) de interactuar y de intercambiar datos de acuerdo con un método definido, con el fin de obtener los resultados esperados. (ISO). El ejercicio de colaboración entre organizaciones para intercambiar información y conocimiento en el marco de sus procesos de negocio, con el propósito de facilitar la entrega de servicios en línea a ciudadanos, empresas y a otras entidades. (Marco de Interoperabilidad para el Gobierno en línea, Versión 2010).

IPv6: [15] El Protocolo de Internet versión 6, es la versión del Protocolo de Internet (IP por sus siglas en inglés) que fue diseñada para suceder al Protocolo versión 4. Ipv6 ha sido desarrollado por la Internet Engineering Task Force (IETF -www.ietf.org), para hacer frente al agotamiento de las direcciones Ipv4, y se describe en el documento estándar de Internet RFC 2460, publicado en diciembre de 1998. Aunque Ipv4 de 32 bits permite una dirección de Protocolo de Internet, y por lo tanto puede soportar 232 direcciones, Ipv6 utiliza direcciones de 128 bits, por lo que el nuevo espacio de direcciones compatible con 2128. Esta expansión permite muchos más dispositivos y usuarios en Internet, así como una mayor flexibilidad en la asignación de direcciones y la eficiencia para el direccionamiento de tráfico.

JSON: [16] JSON es comúnmente utilizado para transmitir datos en aplicaciones web entre el cliente y el servidor. Un uso común de JSON es obtener datos de un servidor web a través de una solicitud HTTP. Este intercambio de datos puede ser entre dos servidores completos o entre un servidor y un cliente.

MAC: [17] Significa Media Access Control (Control de acceso a medios). Es un identificador único para las interfaces de red. Se utiliza como dirección de red para la mayoría de las tecnologías de red IEEE 802. A veces se conoce como la dirección grabada (BIA) o la dirección de hardware Ethernet (EHA). Entre sus aplicaciones se encuentran las redes inalámbricas Ethernet, 802.11 y Bluetooth.

---

[14] Ministerio de las Tecnologías de la información (2021) *https://www.mintic.gov.co/portal/inicio/Glosario/*

[15] Ministerio de las Tecnologías de la información (2021) *https://www.mintic.gov.co/portal/inicio/Glosario/*

[16] Arsys (2025) *https://www.arsys.es/blog/formato-json-que-es-y-para-que-sirve*

[17] Grupo ATICO34 (2025) *https://protecciondatos-lopd.com/empresas/direccion-mac/#Que_es_la_direccion_MAC*

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

MTBF:[18] El MTBF es una medición básica de la fiabilidad de un sistema —cuanto más alto es el MTBF, mayor es la fiabilidad del producto—. El uso del MTBF junto con otras métricas y estrategias de mantenimiento facilita la predicción de los fallos de un activo.

RETIE: [19] Es el Reglamento Técnico de Instalaciones Eléctricas y fue creado mediante la Resolución 18 0398 de 2004, del Ministerio de Minas y Energía, que fija las condiciones técnicas que garanticen la seguridad en los procesos de generación, transmisión, transformación, distribución y utilización de la energía eléctrica.

Servicio:[20] Es el conjunto de acciones o actividades de carácter misional diseñadas para incrementar la satisfacción del usuario, dándole valor agregado a las funciones de la entidad.

Switch:[21] El switch es uno de los componentes fundamentales en el desarrollo de Internet. Funciona como lo hacían los conmutadores telefónicos: recibe paquetes de datos y los direcciona al destinatario correcto.

SSH:[22] SSH son las siglas de Secure Shell y es un protocolo de red destinado principalmente a la conexión con máquinas a las que accedemos por línea de comandos. En otras palabras, con SSH podemos conectarnos con servidores usando la red Internet como vía para las comunicaciones.

Switches core:[23] son un tipo de conmutador de alta capacidad que generalmente se coloca dentro de la red troncal o núcleo físico de una red. Sirven como puerta de acceso a una red de área amplia (WAN) o Internet; proporcionan el punto de acceso final para la red y permiten que varios módulos de agregación trabajen juntos. Debido a la importancia que tiene en las redes, los switches core debe tener una capacidad de poder significativa para manejar eficientemente la carga que se le envía.

TBPS:[24] Unidad de medida utilizada para indicar tasas de transferencia de datos muy altas. Terabits representa 1 billón de bits, y por segundo indica la velocidad a la que se transmiten los datos. Tbps se usa típicamente para describir conexiones

---

[18] PURESTORAGE (2025) *https://www.purestorage.com/es/knowledge/what-is-mtbf.html*

[19] Ministerio de Minias y energías (2004): *Resolución 18 0398 de 2004*

[20] Ministerio de las Tecnologías de la información (2021) *https://www.mintic.gov.co/portal/inicio/Glosario/*

[21] Cisco (S.F) *https://www.cisco.com/c/dam/global/es_mx/solutions/small-business/pdf/glosario-smb.pdf*

[22] Arsys (2025) *https://www.arsys.es/blog/ssh*

[23] Redcomputo (S.F) *https://www.redcomputo.com.co/switches-core*

[24] Martech (2025) *https://es.martech.zone/acronym/tbps/?noamp=mobile*

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

de red de ultra alta velocidad o tasas de transmisión de datos para aplicaciones a gran escala, como centros de datos o redes troncales.

Telecomunicación: [25] Se entiende por telecomunicaciones toda transmisión, emisión o recepción de signos, señales, escritos y sonidos, datos o información de cualquier naturaleza, por hilo, radio, medios visuales u otros sistemas electromagnéticos.

Unidad de rack RU:[26] Una unidad de rack, a menudo abreviada como U o RU, es la unidad de medida de 1,75 pulgadas, que se utiliza comúnmente para medir la altura vertical de bastidores de 19 y 23 pulgadas y los servidores que se montan en ellos.

Yang:[27] YANG es un lenguaje de modelado de datos extensible y basado en estándares que se utiliza para modelar los datos de configuración y estado operativo, llamadas a procedimiento remoto (RPC) y notificaciones de eventos del servidor de los dispositivos de red.

Zona de Cobertura:[28] Zona asociada a una estación transmisora para un servicio dado y una frecuencia específica, en el interior de la cual y en condiciones técnicas determinadas, puede establecerse una radiocomunicación con otra u otras estaciones receptoras.

2.2 CLASIFICACIÓN.

Agrupa los diversos productos que constituyen el objeto de la norma en función de determinados criterios. (opcional)

2.3 APLICACIÓN

Se requiere que el proveedor suministre los equipos y elementos necesarios para la instalación e interconexión de los dispositivos activos y pasivos de comunicaciones, hardware y software necesarios para la instalación, configuración y puesta en funcionamiento del sistema SEGURIDAD DE ACCESOS ZONA DESMILITARIZADA (DMZ), conforme a cada una de los requerimientos relacionados en la presente especificación técnica.

---

[25] Ministerio de las Tecnologías de la información (2021) https://www.mintic.gov.co/portal/inicio/Glosario/

[26] Sunbird (S.F) *https://www-sunbirddcim-com.translate.goog/glossary/rack-unit-ru?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc*

[27] HPEJuniper (2024) *https://www.juniper.net/documentation/mx/es/software/junos/interfaces-telemetry/netconf/topics/concept/netconf-yang-overview.html*

[28] Ministerio de las Tecnologías de la información (2021) https://www.mintic.gov.co/portal/inicio/Glosario/

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

La implementación de un sistema de SEGURIDAD DE ACCESOS ZONA DESMILITARIZADA (DMZ) para el Ejército Nacional representa una inversión estratégica en la protección para la separación de servicios internos y externos que permitan un procesamiento de datos optimo en la protección de los activos digitales de una organización. Al interactuar como una zona de contención donde los recursos expuestos al exterior pueden ser accedidos de forma controlada, sin comprometer directamente la red interna en caso de un ataque, se facilita la implementación de medidas de seguridad robustas, análisis de datos, respaldo de información en tiempo real. Además, esta solución permite al equipo técnico de seguridad colaborar de manera más eficiente, segura, e independiente, lo que se traduce en un aumento de la productividad, tiempos de respuesta e innovación.

Más allá de los beneficios en materia de ciberseguridad, la implementación de este sistema ofrece ventajas operativas significativas. Para la infraestructura tecnológica, reduciendo la exposición de los servicios internos a internet e implementado medidas de protección perimetral robustas. La seguridad y protección de la información es un pilar fundamental en cualquier solución de procesamiento, colaboración, detección y prevención de amenazas, como el phishing y el malware, son esenciales para protegerse contra ataques cibernéticos.

Los equipos entregados por el contratista deben ser interoperables o compatibles con la infraestructura o tecnología homologa, con la que cuenta el Ejército Nacional para su correcto funcionamiento.

El contratista deberá realizar una visita técnica previa en coordinación con la supervisión designada en caso de ser necesario para hacer levantamiento de información de hardware y/o software, antes de iniciar cualquier actividad de instalación, configuración, integración y puesta de funcionamiento de las plataformas.

El contratista se obliga a no suministrar ni publicar ninguna información que obtenga o conozca con ocasión de la ejecución del contrato; así como sobre los lugares a los cuales tenga acceso con ocasión de su desarrollo y sea revelada información marcada como confidencial. El contratista deberá diligenciar el formulario Anticorrupción "acuerdo de confidencialidad" el cual debe ser entregado por el supervisor.

El contratista, así como todos los miembros del equipo de trabajo objeto del proceso deberán guardar secreto profesional sobre toda la información, documentos y asuntos, independientemente de su naturaleza (técnica, comercial, financiera, operacional o de otro tipo), a los que tenga acceso o conocimiento durante la

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

vigencia del contrato, independientemente de la forma o soporte (verbal, escrita, grabado o de cualquier otro tipo), por la que haya adquirido la información. En tal virtud, está obligado y se adoptarán todas las medidas necesarias para no hacer público, sustraer, duplicar, alterar, ocultar, ceder o enajenar cuanto dato conozca como consecuencia o con ocasión de la ejecución del contrato. Esta obligación no se limita al tiempo de ejecución del contrato, sino que deberá ser respetada aún después de su finalización.

A tal efecto todos los miembros del equipo prestador del servicio deberán tener un completo conocimiento del deber de secreto de la información durante la ejecución del contrato y en el supuesto de producirse algún cambio en la composición del equipo prestador del servicio, los nuevos integrantes asumirán las obligaciones contenidas en este ítem. Con esta finalidad el contratista se compromete a formar e informar al personal de tales obligaciones asumiendo, en el caso contrario, las responsabilidades que pudieran devenirse por su incumplimiento.

Por lo anterior es indispensable que el contratista y los recursos humanos que formaran parte del grupo de trabajo se comprometa a conocer, aceptar y ajustarse a las políticas de seguridad informática del Comando General de las Fuerzas Militares y del Ejército Nacional y firmar al inicio del contrato una **promesa de reserva o 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 contrato y por tanto en ningún caso podrá divulgarla, copiarla, reproducirla o suministrarla a terceros.

Todos los estudios y documentos elaborados por el contratista como consecuencia de la ejecución del contrato serán de propiedad del Ejército Nacional, quien podrá reproducirlos, publicarlos y divulgarlos, sin que pueda oponerse a ello el adjudicatario autor material de los trabajos, en cumplimiento de los términos establecidos en la Ley 23 de 1982, modificada por la Ley 44 de 1993 y la Ley 1915 de 2018.

En particular, toda aquella documentación generada por intervenciones del personal asignado al servicio en el Ejército Nacional será propiedad de la institución, por tanto, no podrá ser facilitada a otra persona o entidad sin consentimiento expreso del Ejército Nacional.

El contratista renuncia expresamente a cualquier derecho que sobre los trabajos realizados como consecuencia de la ejecución del contrato pudiera corresponderle, y no podrá hacer ningún uso o divulgación de los estudios y documentos utilizados

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

o elaborados en base en el pliego de condiciones o la durante el desarrollo del contrato, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa y por escrito del Ejército Nacional.

Por lo anterior al finalizar la ejecución del proceso toda la información y documentos entregados por el Comando del Ejército, deberán ser retornados y no podrá quedarse con la información que se genere.

El contratista se debe comprometer a conocer, aceptar y ajustarse a las políticas de seguridad de la Directiva de Seguridad Informática del Ministerio de Defensa - Comando General de las Fuerzas Militares Directivas Permanentes de Ciberdefensa y Seguridad de la Información y demás que sean aplicables.

El contratista deberá cumplir con el **ANEXO TÉCNICO DE ESPECIFICACIONES TÉCNICAS ADICIONALES**, en caso de existir. Dicho anexo solo podrá establecer requisitos relacionados con perfiles profesionales, tiempos mínimos de experiencia, certificaciones del fabricante que respalden la calidad de los productos a entregar y actividades de transferencia de conocimiento, cuando así se requiera.

3. REQUISITOS

3.1 REQUISITOS GENERALES

No.	DESCRIPCION
1	Se requiere el suministro, instalación y puesta en funcionamiento del sistema de SEGURIDAD DE ACCESOS ZONA DESMILITARIZADA (DMZ) para el Ejército Nacional de Colombia. Estos dispositivos activos y pasivos de comunicaciones, hardware y software se requieren para brindar servicios de red a los equipos y usuarios que se conecten a sus interfaces, conforme a cada una de los requerimientos relacionados en la presente especificación técnica.
2	Se debe garantizar la disponibilidad y provisión de todos los elementos y recursos necesarios para la implementación y puesta en funcionamiento del Sistema, garantizando que todos los elementos sean totalmente nuevos.
3	Se debe entregar la documentación física y digital de todo lo realizado en el durante la ejecución del contrato, además debe incluir planos o diseños finales, certificaciones en caso de requerirse, manuales de instalación, funcionamiento, administración o mantenimiento, documentos con las garantías de equipos utilizados en la implementación del sistema.

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

	Así mismo, se debe hacer entregar de los manuales físicos y/o digitales del equipo y ejecutables de instalación en DVD y/o USB a fin de que el equipo tenga los soportes respectivos para su correcto funcionamiento en caso de tener una contingencia.
4	Se deben realizar las siguientes actividades para la migración del equipo donde se debe entregar informe de cada uno: **Planificación:** La migración del sistema de seguridad de accesos zona desmilitarizada (DMZ) debe ser cuidadosamente planificada de acuerdo a un proceso estandarizado lo cual permitirá minimizar el tiempo de inactividad de la red. El plan debe incluir un cronograma detallado que describa los pasos y las tareas que se realizarán durante la migración. **Evaluación de riesgos**: La migración del sistema de seguridad de accesos zona desmilitarizada (DMZ) puede ser un proceso complejo que implica ciertos riesgos. Por lo tanto, es importante realizar una evaluación de riesgos para identificar posibles problemas y tomar medidas preventivas, donde se debe entregar un informe de los mismo. **Verificación y pruebas:** Una vez que se ha completado la migración, es esencial verificar y probar el nuevo sistema de seguridad de accesos zona desmilitarizada (DMZ) instalado para asegurarse de que esté funcionando correctamente y cumpla con los requisitos de la red, configuración y las especificaciones técnicas descritos en el presente documento; por tanto, se deberá entregar un informe con registro fotográfico de su funcionamiento que describa todas las actividades desarrolladas.
5	Se deberá entregar un informe detallado de las actividades proyectadas para la migración del equipo, incluyendo: Copia de seguridad de los equipos Configuración del nuevo equipo Pruebas de funcionamiento Transferencia de conocimiento al personal Documentación (Topologías)
6	Se debe realizar la migración de los equipos teniendo en cuenta todas las configuraciones existentes, en los equipos nuevos incluyendo el direccionamiento IPV6.

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

	Se debe realizar la instalación, configuración, puesta en funcionamiento y marquillado de todas las conexiones que tengan los equipos instalados en la actualidad.
7	El equipo deberá incluir todos los cables, conectores y dispositivos necesarios para la correcta instalación y puesta en funcionamiento.

3.2 REQUISITOS ESPECÍFICOS

3.2.1	SISTEMA DMZ CAPA 3
N°	CARACTERISTICAS
1	Suministro e instalación y puesta en funcionamiento de sistema de seguridad de accesos zona desmilitarizada (DMZ), el cual debe cumplir con las características mínimas requeridas en la presente especificación técnica
2	El equipo debe contar con 48 Puertos la cual debe soportar las siguientes conexiones 1/10/25G SFP28 + 12 puertos 40/100G QSFP28
3	El equipo debe soportar arquitecturas BGP de tres niveles, que permiten estructuras de red IPv6 horizontales y sin bloqueos a escala web
4	El equipo debe tener compatibilidad con YANG nativo y el modelo Open Config mediante RESTCONF/NETCONF
5	Debe soportar Protocolo de intercambio de puentes de centros de datos
6	Debe soportar reinicio avanzadas incluyen parches en caliente y en frío.
7	Compatible con API generalizadas para todas las funciones CLI del conmutador (RPC basado en JSON sobre HTTP/HTTP)
8	Debe permitir FC-FEC y RS-FEC habilitados para admitir 25 Gbps
9	El equipo debe admitir hasta 4.8 Tbps de ancho de banda, los cuales deberán están soportado en documento de fábrica.
10	El equipo debe contar con una CPU de mínimo 4 núcleos o superior en caso de requerirse
11	El equipo debe contar con una memoria del sistema mínimo 24Gb o superior
12	El equipo debe tener una unidad de estado sólido de mínimo 128Gb o superior
13	El equipo debe contar con 40Mb de Almacenamiento en búfer del sistema, lo cual se demostrar al momento de la implementación
14	El equipo debe contar con los siguientes puertos de conexión: 1 puerto RJ-45 de gestión + 1 Puerto SFP+, Puerto USB: 1 y Puerto serie RS-232: 1 para realizar configuraciones físicas.
16	El equipo debe tener mínimo 2 o más fuentes de alimentación de mínimo 750W y debe soportar fuentes de alimentación intercambiables en caliente y ventiladores con redundancia N+1 en caso de fallas.

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

17	El equipo debe contar con las siguientes características de potencia, voltaje y frecuencia • Potencia típica (CA): 298W • Potencia máxima (CA): 708W • Voltaje de entrada (CA): 100 a 240V • Voltaje de entrada (CA de alto voltaje [HVAC]): 100 a 277V • Voltaje de entrada (CC) -40 a – 72 V • Voltaje de entrada (CC de alto voltaje [HVDC]) -240 a -380 V • Frecuencia (CA) 50 a 60 Hz
18	El equipo debe incluir mínimo 5 ventiladores o más en caso de ser requeridos al momento de la instalación para su correcto funcionamiento
19	El equipo debe contar con una Acústica 76,4 dBA al 50 % de la velocidad del ventilador 83,3 dBA al 70 % de la velocidad del ventilador 92,1 dBA al 100 % de la velocidad del ventilador
20	El equipo debe contar con un tiempo medio entre fallas (MTBF) de mínimo 345.900 horas
21	Máximo de rutas IPv4 LPM: 896,000
22	El equipo debe permitir hacer los enlaces entre los puertos y los combos de conexión Máximo de entradas de host IPv4: 896,000 Máximo de rutas IPv6 LPM: 498,000 Máximo de entradas de host IPv6: 896,000 Máximo de direcciones MAC: 256,000 Máximo de rutas multicast: 128,000 Máximo de VLANs: 4,096 Máximo de rutas ECMP: 64 Máximo de port channels: 512 Máximo de enlaces por port channel: 32 Sesiones activas de SPAN: 4 Máximo de VLANs en instancias RPVST: 3,967 Máximo de grupos HSRP: 490 Entradas NAT soportadas: 1,023 Número de colas por puerto: 8 Máximo de instancias MST: 64 Debe soportar Priorización Dinámica de Paquetes (DPP) Temperatura de operación: 32 a 104°F (0 a 40°C) Humedad: 5% a 95% (sin condensación) Compatibilidad con IEEE 802.1ae MAC Security
23	El equipo debe soportar protocolos para conjuntos de protocolos de enrutamiento de unidifusión y multidifusión de capa 3 (v4/v6), incluidos

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

	BGP, OSPF (Open Shortest Path First), EIGRP (Enhanced Interior Gateway Routing Protocol), RIPv2 (Routing Information Protocol), PIM-SM (Protocolo de modo disperso de multidifusión independiente del protocolo), SSM (Multicast Specific Multicast Protocol) y MSDP (Multicast Source Discovery Protocol).
24	El equipo deberá contar con las siguientes formas de administración: GUI, CLI, SSH y Debe poseer interfaz por consola/Telnet.
25	El equipo debe soportar IPV6 y debe integrarse de manera nativa con el Switch core de la institución.
26	El equipo debe estar diseñado para ubicarse en dos unidades rack
27	El equipo debe tener instalada la última versión del sistema operativo liberado por el fabricante al momento de la entrega, así como todos los parches liberados para la prevención de vulnerabilidades, lo cual debe ser entregado en documento aparte debidamente firmado; por lo anterior, no se aceptarán sistemas operativos experimentales, en versiones beta o de mantenimiento.
28	El equipo entregado deberá ser totalmente nuevo, estar en perfectas condiciones de uso, y de comprobarse que ha sido reparado o remanufacturado, se deberá sustituir por otro totalmente nuevo, sin que esto genere costo adicional para el Ejército Nacional,
29	El sistema operativo debe entregarse licenciado en forma vitalicia para el Ejército Nacional con características de full capa 3, garantizando la operatividad del mismo, el cual debe llevar integrado el software de administración para su manejo

3.2.2	**MÓDULOS DE CONECTIVIDAD Y CABLES DE STACK**
N°	**CARACTERISTICAS**
1	Módulos de SFP 10G con conector RJ-45 que cumplan como mínimo con las siguientes características: 100/1000/10000 Mbps Tipo de cable soportado: Cat6A/Cat7 o superior Alcance de mínimo 30 metros
2	Módulos de fibra 10G SFP+ SR que cumplan como mínimo con las siguientes características: Tipo de conector LC dúplex Longitud de onda 850 nm Factor de forma SFP + Tipo de fibra: Multimodo Alcance mínimo 300 metros

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

	Deberán ser originales de la misma marca switch ofertado y compatibles con el mismo.
3	Módulos de fibra 25G SFP SR que cumplan como mínimo con las siguientes características: Tipo de conector LC dúplex Longitud de onda 850 nm Factor de forma SFP28 Tipo de fibra: Multimodo Alcance mínimo 70 metros Deberán ser originales de la misma marca del switch ofertado y compatibles con el mismo.
4	Módulos de fibra 40G QSFP SR que cumplan como mínimo con las siguientes características: Tipo de conector MPO-12 Longitud de onda 850 nm Factor de forma QSFP Tipo de fibra: Multimodo Alcance mínimo 100 metros Deberán ser originales de la misma marca switch ofertado y compatibles con el mismo.
5	Cable de stack 100G QSFP que cumplan como mínimo con las siguientes características: ● Tipo de cable óptico activo ● Longitud mínimo 3 Metros ● Conector QSFP en ambos extremos ● Deberán ser originales de la misma marca switch ofertado y compatibles con el mismo.

3.3 REQUISITOS DE EMPAQUE Y ROTULADO

3.3.1 Empaque.

Todos los equipos deberán venir correctamente empacados de acuerdo a la normatividad vigente para equipos tecnológicos.
El elemento debe ser entregado debidamente empacado antes de su instalación, utilizando materiales de protección como bolsas o espumas de polietileno, poliuretano o plástico de burbujas. El empaque deberá garantizar la integridad de cada componente, protegiéndolo contra posibles impactos, vibraciones y otras condiciones adversas que puedan presentarse durante el transporte.

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

Rotulado Todos los elementos suministrados para la solución deben ser etiquetados, de acuerdo a la norma técnica internacional ANSI / TIA-606-C y previa aprobación del supervisor del contrato.

Todos los equipos deberán contar con una placa o etiqueta de fábrica, debidamente grabada mediante impresión permanente y de difícil borrado, así como con un adhesivo resistente al desprendimiento. El rotulado debe ser claro, legible y cumplir con las normas técnicas NTC, las normativas internacionales aplicables, la reglamentación técnica vigente y los boletines SILOG N.° 5A1 y 5A2, relacionados con la identificación y clasificación de productos.

- La etiqueta o placa deberá contener, como mínimo, la siguiente información:
- Nombre del fabricante
- Nombre del proveedor
- Nombre del producto
- Código de especificación (especificación técnica aplicada)
- País de origen
- Fecha y número del contrato
- Modelo

Para verificar los requisitos generales, de empaque y rotulado se deben someter a evaluación todo el Sistema de procesamiento de datos de seguridad que se vaya a suministrar. Evaluando todos sus componentes.

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

Los criterios de aceptación o rechazo de esta especificación técnica se basan en el cumplimiento de los requerimientos establecidos en los numerales 3.1 (Requisitos Generales) y 3.2 (Requisitos Específicos).

4.1.1 Muestreo. No aplica

4.1.2 Criterios de aceptación o rechazo para requisitos generales y requisitos de empaque y rotulado. El criterio para aceptar o rechazar el producto depende del cumplimiento de todos los requisitos técnicos establecidos en el presente documento.

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

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

Los criterios de aceptación o rechazo de esta especificación técnica se basan en el cumplimiento de los requerimientos establecidos en los numerales 3.1 (Requisitos Generales) y 3.2 (Requisitos Específicos).

4.2.1 Muestreo. No Aplica

4.2.2 Criterio de aceptación o rechazo para evaluar requisitos específicos.

No Aplica

5. MÉTODOS DE ENSAYO

5.1. Se realizarán pruebas de encendido y medición necesarias para evaluar el correcto funcionamiento de los, equipos y/o herramientas. Así mismo, se evaluará la transferencia de conocimiento que deberá ser impartida por el contratista, quien deberá garantizar la completa comprensión en el manejo y configuración de cada uno de los equipos instalados y entregados al Ejército Nacional.

5.2. Las pruebas e inspecciones de funcionamiento, estado y cumplimiento, necesarias para la puesta en ejecución del instrumento objeto de la presente especificación, serán efectuadas y aprobadas por el funcionario competente, quien verificará el cumplimiento de los requisitos estipulados en el presente documento.

5.3. El proveedor y la unidad que tengan la necesidad, deberán efectuar las pruebas para cada equipo que a continuación se listan, verificando que se cumplan satisfactoriamente en su totalidad.

No	ACTIVIDAD	SI	NO	OBS
1	Recepcionar el equipo y verificar estado de embalaje.			
2	Identificar rotulado teniendo en cuenta normatividad ISO.			
3	Abrir caja de embalaje.			
4	Supervisar estado físico del equipo			
5	Identificar piezas o elementos pertenecientes al equipo			
6	Revisar manuales de usuario y/o técnicos			
7	Realizar conexión de cable de poder.			

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

8	Se realizará prueba de encendido de cada elemento			
9	Realizar pruebas de rendimiento consistentes en pruebas de velocidad de encendido y respuesta de cambio de funciones si se requiere.			
10	Se verifica el correcto funcionamiento del equipo mediante puesta a prueba de sus principales características			
11	Identificar el paso a paso mediante manuales, el funcionamiento en tiempo real de las funciones del equipo.			
12	Realizar pruebas de esfuerzo como sobrecarga de las aplicaciones al sistema para analizar la capacidad de recuperación si es necesario			
13	Pruebas de estabilidad, eficiencia, robustez en medición de la respuesta del equipo.			
14	Se realiza de forma correcta la transferencia de conocimiento por parte del contratista a los técnicos del Ejército Nacional, comprobando el óptimo funcionamiento de los elementos por parte de los mismos.			
16	Verificar cada uno de los módulos y cables requeridos en la presente especificación técnica que se encuentren en perfecto estado y embalaje.			

6. APÉNDICE

6.1 NORMAS QUE DEBEN CONSULTARSE

- Constitución Política de Colombia.
- Código Civil.
- Código General del Proceso.
- Código de Comercio.
- Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- Ley 80 de 1993 "Por la cual se expide el Estatuto General de Contratación de la Administración Pública" y las demás normas que la modifiquen o aclaren.
- Ley 816 de 2003 "Por medio de la cual se apoya a la industria nacional a través de la contratación pública" y las demás normas que la modifiquen o aclaren.

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

- Ley 1150 de 2007 "Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos" y las demás normas que la modifiquen o aclaren.
- Ley 1341 de 2009 "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones" y las demás normas que la modifiquen o aclaren.
- Ley 1474 de 2011 "Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública" y las demás normas que la modifiquen o aclaren.
- Decreto Ley 19 de 2012 "Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública" y las demás normas que lo modifiquen o aclaren.
- Ley 1712 de 2014 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones" y las demás normas que la modifiquen o aclaren.
- Decreto 1082 de 2015 "por medio del cual se expide el Decreto Único Reglamentario del sector Administrativo de Planeación Nacional" y las demás normas que lo modifiquen o aclaren.
- Decreto 103 del 20 de enero de 2015 "Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones" y las demás normas que lo modifiquen o aclaren.
- Resolución 2710 de 2017 del Ministerio de Tecnologías de la Información y las Comunicaciones "Por la cual se establecen lineamientos para la adopción del protocolo IPv6", modificada por la resolución No. 1126 de 2024 y las demás normas que la modifiquen o aclaren.
- Resolución 4223 de 2022 "Por la cual se delegan unas funciones y competencias relacionadas con la contratación de bienes y servicios con destino al Ministerio de Defensa nacional, unas funciones de carácter administrativo y se dictan otras" y las demás normas que la modifiquen o aclaren.
- Resolución 4130 de 2022 "MANUAL DE CONTRATACIÓN Y DE CONVENIOS" del Ministerio de Defensa Nacional y las demás normas que la modifiquen o aclaren.
- Resolución 7870 de 2022 del Ministerio de Defensa, 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

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

Defensa Nacional, Policía Nacional y entidades adscritas y vinculadas al Sector Defensa y se dictan otras disposiciones.

- Directiva permanente 00201 de 2017 "Lineamiento de Ciberseguridad y Ciberdefensa para el Ejército Nacional" y las demás normas que la modifiquen o aclaren.
- Directiva permanente 00221 de 2017 "Seguridad de la información para el Ejército Nacional" y las demás normas que la modifiquen o aclaren.
- Procedimiento documentos técnicos normativos P-JEMPP-CEDE4-348-V1

6.2 ANTECEDENTES

Omitido

7. ANEXOS

Omitido

8. CONTROL DE REVISIONES

Revisión y/o Actualización	Modificaciones	Fecha
00	Creación de la especificación técnica SWITCH DE SEGURIDAD DE ACCESOS ZONA DESMILITARIZADA (DMZ) No. JEMPP-CEDE6-DIPCO–ET-XXX-COM–00 en cumplimiento a la circular 2023218017093013 del 03 de octubre del 2023 acogiéndose al numeral 20.1 "Citar el documento que motivo la creación o actualización de la Especificación Técnica" por medio del oficio solicito creación de la especificación técnica No. 2025574024803903 de fecha 14 de agosto de 2025 y oficios para reuniones de trabajo No. 2025574024806113 del 14 de agosto del 2025, No. 2025227026400913 del 27 de agosto de 2025 No. 2025227029841003 del 24 de septiembre de 2025, oficio estudio de mercado con No. 2025574029969223 12 de noviembre de 2025.	2026-01-23

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

	El Batallón de Ciberdefensa y Ciberseguridad BACCI, en cumplimiento a la circular 2023218017093013 del 03 de octubre del 2023 acogiéndose al numeral 20.2 "La unidad en este documento técnico garantiza la pluralidad de oferentes" El Batallón de Ciberdefensa y Ciberseguridad BACCI, en cumplimiento a la circular 2023218017093013 del 03 de octubre del 2023 acogiéndose al numeral 20.3 "La unidad garantiza los requisitos generales y específicos, los cuales fueron revisados técnicamente y satisfacen las necesidades del Ejército Nacional" El Batallón de Ciberdefensa y Ciberseguridad BACCI, en cumplimiento a la circular 2023218017093013 del 03 de octubre del 2023 acogiéndose al numeral 20.4" La unidad garantiza que este documento técnico fue elaborado de manera profesional, con la mayor transparencia, siempre buscando enaltecer el nombre del Ejército Nacional.	

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

SISTEMA DE PROCESAMIENTO DE DATOS DE SEGURIDAD PARA EL EJÉRCITO NACIONAL

No. JEMPP-CEDE6-DIPCO-ET-05715-COM-00



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

ITEM	DESCRIPCION
2.2.3	INTERRUPTOR DE TRANSFERENCIA DE RACK HIBRIDO INTELIGENTE
2.2.3.1	Para garantizar la continuidad de la operación, es necesario suministrar un interruptor de transferencia de Rack hibrido inteligente (Switch de transferencia), que permita mantener el suministro de energía hacia los equipos de la solución hiperconvergente en caso de fallos en las fuentes de alimentación (Energia eléctrica o UPS) que cumpla con las siguientes características:
2.2.3.2	Transferencias de carga ultrarrápidas entre 4 y 8 milisegundos, probadas para no interrumpir la carga de energía en condiciones reales.
2.2.3.3	Relés para manejar cargas grandes con alta fiabilidad
2.2.3.4	Evita las transferencias de cortocircuitos de salida, lo que podría llevar a una falla en cascada del segundo suministro de energía.
2.2.3.5	Suministro de energía redundante y arquitectura de controlador inteligente impulsada por firmware
2.2.3.6	Firmware Xerus con scripting
2.2.3.7	Umbrales configurables por el usuario para la calidad de la energía
2.2.3.8	Interfaz configurable basada en la web.
2.2.3.9	Seguridad de red robusta y protocolos de encriptación: AES128, SSH, SNMPv3, Smart TLS, FIPS 140-2.

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

SISTEMA DE PROCESAMIENTO DE DATOS DE SEGURIDAD PARA EL EJERCITO NACIONAL No. JEMPP-CEDE6-DIPCO-ET-05715-COM-00

2.2.3.10	Tecnología híbrida (diseño de relé más SCR) para una mejor eficiencia energética y menos calor (arquitectura sin ventilador).
2.2.3.11	Precisión de medición de energía de grado de facturación (+/-1%).
2.2.3.12	Interruptor de transferencia de rack con medición de energía, monitoreo de calidad de energía y soporte para sensores ambientales opcionales
2.2.3.13	Pantalla local que muestra el estado del interruptor de transferencia y las condiciones de conmutación por falla de un vistazo.
2.2.3.14	Debe estar en la capacidad de operar a temperaturas de hasta 60° C (UL), 50° C (CE) en un entorno con 85% de humedad relativa (RH).
2.2.3.15	Compatible con SecureLock para prevenir desconexiones accidentales.
2.2.3.16	Componentes de estado sólido para transferencias rápidas
2.2.3.17	Elimina los arcos eléctricos que causan fallos en los relés de transferencia.
2.2.3.18	Identifica los cortocircuitos de salida y envía una alarma para que el cortocircuito pueda ser corregido antes de realizar la transferencia de energía manualmente.
2.2.3.19	Proporciona conmutación y medición a nivel de toma de corriente, así como energía confiable para dispositivos de un solo cable.
2.2.3.20	Sistema con diseño sin ventilador
2.2.3.21	Interfaz gráfica de usuario (GUI) intuitiva, SNMP, Modbus, TCP/IP, JSON-RPC para scripting, IPv4 / IPv6.
2.2.3.22	Acceso y control desde tabletas frontales y traseras a través de puertos USB.
2.2.3.23	Alertas por umbral y actualizaciones de estado a través de mensajes de texto GSM, correo electrónico y syslog.
2.2.3.24	Registra los tiempos de transferencia para informes.
2.2.3.25	Soporte para sensores ambientales plug-and-play.
2.2.3.26	Disponible en una unidad de rack
2.2.3.27	Deberá poderse conectar a los switch de transferencia inteligentes y las PDU inteligentes con las que cuenta actualmente el datacenter para gestionar de manera unificada.

ESPECIFICACIONES TÉCNICAS ADICIONALES DE OBLIGATORIO CUMPLIMIENTO

Las especificaciones técnicas de obligatorio cumplimiento y descripción de los mismos se encuentran detalladas en el siguiente anexo como se relación a continuación:



Al contestar, cite este número
Radicado No. 2026574010702623 MDN-COGFM-COEJC-SECEJ-JEMOP-CAOCC-BRICC-BAICC-CPCA-29.25

ESPECIFICACIONES TECNICAS ADICIONALES DE OBLIGATORIO CUMPLIMIENTO PARA LA ADQUISICION DEL SISTEMA DE SEGURIDAD DE ACCESOS ZONA DESMILITARIZADA (DMZ), CUYO FIN ES EL FORTALECIMIENTO DE LOS MEDIOS CIBERNÉTICOS DEL EJÉRCITO NACIONAL, A EJECUTAR EN LA VIGENCIA 2026.

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

ESPECIFICACIONES TECNICAS ADICIONALES DE OBLIGATORIO CUMPLIMIENTO

	ADQUISICION DEL SISTEMA DE SEGURIDAD DE ACCESOS ZONA DESMILITARIZADA (DMZ), CUYO FIN ES EL FORTALECIMIENTO DE LOS MEDIOS CIBERNÉTICOS DEL EJÉRCITO NACIONAL, A EJECUTAR EN LA VIGENCIA 2026.
1	**OBLIGACIONES GENERALES DEL CONTRATISTA:** • **Confidencialidad de la Información** El contratista se obliga a no suministrar ni publicar ninguna información que obtenga o conozca con ocasión de la ejecución del contrato; así como sobre los lugares a los cuales tenga acceso con ocasión de su desarrollo y sea revelada información marcada como confidencial. El contratista deberá diligenciar el formulario Anticorrupción "acuerdo de confidencialidad". La empresa adjudicataria, así como todos los miembros del equipo de trabajo objeto del proceso deberán guardar secreto profesional sobre toda la información, documentos y asuntos, independientemente de su naturaleza (técnica, comercial, financiera, operacional o de otro tipo), a los que tenga acceso o conocimiento durante la vigencia del contrato, independientemente de la forma o soporte (verbal, escrita, grabado o de cualquier otro tipo), por la que haya adquirido la información. En tal virtud, está obligado y se adoptarán todas las medidas necesarias para no hacer público, sustraer, duplicar, alterar, ocultar, ceder o enajenar cuanto dato conozca como consecuencia o con ocasión de la ejecución del contrato. Esta obligación no se limita al tiempo de ejecución del contrato, sino que deberá ser respetada aún después de su finalización. A tal efecto todos los miembros del equipo prestador del servicio deberán tener un completo conocimiento del deber de secreto de la información durante la ejecución del contrato y en el supuesto de producirse algún cambio en la composición del equipo prestador del servicio, los nuevos integrantes asumirán las obligaciones contenidas en este ítem. Con esta finalidad el contratista se compromete a formar e informar al personal de tales obligaciones asumiendo, en el caso contrario, las responsabilidades que pudieran devenirse por su incumplimiento. Por lo anterior es indispensable que el contratista se comprometa a conocer, aceptar y ajustarse a las políticas de seguridad informática del Comando General de las Fuerzas Militares y del Ejército Nacional y firmar al inicio del contrato una promesa de reserva 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 contrato y la de estos pliegos técnicos, y por tanto en ningún caso podrá divulgarla, copiarla, reproducirla o suministrarla a terceros. El contratista y los recursos humanos que formaran parte del grupo de trabajo deberán firmar al inicio de la ejecución del contrato, el 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 contrato y por tanto en ningún caso podrá divulgarla, copiarla, reproducirla o suministrarla a terceros; así mismo, en caso de un ataque cibernético relacionado con las plataformas de seguridad perimetral firewall o presentarse una situación de cualquier naturaleza que llegue a afectar la infraestructura del Ejército Nacional dentro de los términos del contrato y sea necesario el apoyo de personal del equipo prestador de servicios tenga que apoyar en las instalaciones del Batallón de Ciberdefensa y Ciberseguridad del Ejército Nacional, deberá firmar acta de compromiso de confidencialidad.

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

- **Propiedad Intelectual**

Todos los estudios y documentos elaborados por el contratista como consecuencia de la ejecución del contrato serán de propiedad del Ejército Nacional, quien podrá reproducirlos, publicarlos y divulgarlos, sin que pueda oponerse a ello el adjudicatario autor material de los trabajos, en cumplimiento de los términos establecidos en la Ley 23 de 1982, modificada por la Ley 44 de 1993 y la Ley 1915 de 2018.

En particular, toda aquella documentación generada por intervenciones del personal asignado al servicio en el Ejército, será propiedad de la institución, por tanto, no podrá ser facilitada a otra persona o entidad sin consentimiento expreso del Ejército.

El adjudicatario renuncia expresamente a cualquier derecho que sobre los trabajos realizados como consecuencia de la ejecución del contrato pudiera corresponderle, y no podrá hacer ningún uso o divulgación de los estudios y documentos utilizados o elaborados en base a este pliego de condiciones, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa y por escrito del Ejército Nacional.

Por lo anterior al finalizar la ejecución del proceso toda la información y documentos entregados por el Comando del Ejército, deberán ser retornados y no podrá quedarse con la información que se genere.

- **Documentación**

El contratista deberá entregar al Ejército Nacional la documentación necesaria para la Instalación, configuración, implementación y parametrización.

Esta documentación debe incluir el detalle del plan de trabajo completo para efectuar la instalación y configuración de las plataformas adquiridas, además se debe especificar:

- Los recursos necesarios para la instalación.
- Cada uno de los pasos que se deben efectuar.
- Los tiempos de ejecución de cada uno de los pasos.
- Para el desarrollo de la instalación se deberá presentar un cronograma de tareas después de firmada el acta de inicio del contrato.
- Después cada configuración se debe entregar un manual de procedimiento de las configuraciones realizadas en cada una de las soluciones.
- Informe final donde se describa el total de las soluciones, configuraciones y procesos realizados en la ejecución del contrato

Informe de cada visita, documentado los procedimientos realizados.

- **Otros**

El contratista se debe comprometer a conocer, aceptar y ajustarse a las políticas de seguridad de la Directiva de Seguridad Informática del Ministerio de Defensa - Comando General de las Fuerzas Militares Directivas Permanentes de Ciberdefensa y Seguridad de la Información.

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

2	**El contrato debe ser tratado como un proyecto llave en mano.** Para todos los efectos de funcionalidad e interoperabilidad, el contratista debe instalar, configurar, dar soporte y acompañamiento de la solución adquirida y el software y/o firmware instalado, garantizando al Ministerio de Defensa Nacional – Ejército Nacional – Batallón de Ciberdefensa y Ciberseguridad el correcto funcionamiento de acuerdo a las especificaciones técnicas requeridas. ***Nota:*** *"Sera considerado un proyecto llave en mano, aquel que asegure el resultado final de manera satisfactoria, cumpliendo las especificaciones. La optimización de costo, logística, mejores prácticas de implementación serán potestad del contratista, siempre y cuando cumplan con el objetivo final de suministrar una solución que garantice las especificaciones técnicas requeridas; de ser necesario el oferente asumirá costos adicionales de servicios, accesorios, componentes de software, hardware, cableado y elementos adicionales requeridos para la óptima implementación de esta solución e integración con todas las soluciones tecnológicas del Ejercito Nacional."* Se debe suministrar por parte del contratista la logística necesaria para el desarrollo del contrato como: portátiles, desplazamientos, hospedajes, alimentación, discos duros extraíbles, papelería, software y/o firmware para el desarrollo del contrato, sin que esto genere costo adicional para el Ministerio de Defensa Nacional – Ejército Nacional – Batallón de Ciberdefensa y Ciberseguridad; Una vez finalizado el contrato, a estos elementos se les debe realizar un procedimiento de borrado seguro por parte de la Batallón de Ciberdefensa y Ciberseguridad del Ejército Nacional para posteriormente ser retirados de las instalaciones del Ministerio de Defensa Nacional – Ejército Nacional – Batallón de Ciberdefensa y Ciberseguridad.
3	**Cumplimiento de Normatividad Gubernamental en Materia de Tics** Todas las soluciones deben ser compatibles con los protocoles IPV4 e IPV6 **CUMPLIMIENTO DE NORMATIVIDAD GUBERNAMENTAL EN MATERIA DE TICS** Los bienes y servicios TICS contemplados en la presente ficha técnica, deben brindar soporte al protocolo de internet versión seis (IPv6) de conformidad con la Resolución 2710 del 03 de octubre de 2017 de MINTIC, que en su Artículo 5. "Contratación", estipula: "A partir de la entrada en vigencia de la presente resolución, todos los procesos de selección que inicien las entidades públicas deberan, desde los mismos pliegos de condiciones o lo que haga sus veces, exigir soporte IPv6 nativo en coexistencia con IPv4, en la contratación de bienes y servicios relacionados con las TICS." **Cumplimiento Normas Técnicas** El proponente adjudicatario se compromete a cumplir o exceder en las siguientes especificaciones de instalación, documentación, componentes y sistemas de la industria según sea el caso (Si Aplica): • El Reglamento Técnico de Instalaciones Eléctricas – RETIE, para las instalaciones eléctricas del país. • La norma NTC 2050 (Código Eléctrico Colombiano), adoptada y administrada por ICONTEC, la cual establece los lineamientos técnicos para diseño y construcción de instalaciones eléctricas. • Normas ANSI/TIA-568-C (C.0, C.1, C.2 y C.3) y la norma ISO/IEC 11801 constituyen estándares internacionales ampliamente reconocidos para el diseño e implementación de sistemas de cableado estructurado en cobre y fibra óptica. • Norma ANSI/TIA-942 (Redundancia eléctrica y de telecomunicaciones, clasificación por niveles (Tier) y diseño de rutas de cableado y separación de trayectorias.

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

<table>
<tr><td></td><td>

- Las disposiciones de puesta a tierra para telecomunicaciones (ANSI-J-STD-607) y la norma IEC 61000-5-2.

</td></tr>
<tr><td>4</td><td>

- El oferente deberá incluir en la oferta, un cuadro de marcas y referencias de los equipos a ofertar con su respectivo catalogo o ficha técnica y el detalle técnico. La entidad proporciona el siguiente modelo, el cual podrá usar el oferente de manera opcional.

Cuadro De Marcas Y Referencias

<table>
<tr><th>ITEM</th><th>DESCRIPCIÓN</th><th>MARCA</th><th>REFERENCIA</th></tr>
<tr><td>1</td><td>Suministro de equipos activos switch en alta disponibilidad para DMZ SEGÚN ESPECIFICACION TECNICA No. JEMPP-CEDE6-0273 Ítem 3.2.1</td><td></td><td></td></tr>
<tr><td>7</td><td>Interruptor de transferencia de rack híbrido SEGÚN ESPECIFICACION TECNICA No. JEMPP-CEDE6-DIPCO-ET-05715-COM-00 Ítem 2.2.3</td><td></td><td></td></tr>
</table>

</td></tr>
<tr><td>5</td><td>

- Los equipos deben tener un sticker adhesivo con el nombre de la empresa que suministra los equipos, el número del contrato, número telefónico y correo electrónico donde brindan soporte técnico.

- Todos los equipos deberán estar embalados en las cajas de la fábrica y deben ser totalmente nuevos. La instalación de las licencias ya debe venir incluida en cada maquina que a partir de la firma del contrato serán Propiedad del Ejército Nacional, así mismo es responsabilidad del contratista garantizar mediante certificado escrito y avalado por el fabricante y/o distribuidor autorizado que los equipos no cuentan con ningún tipo de licenciamiento adicional al que esta descrito en esta ficha, de no ser así será responsabilidad del contratista el costo del licenciamiento adicional lo que no generara costo alguno para el Ejército Nacional.

- De igual modo los equipos deben ser nuevos y no remanufacturados.

- Cada uno de los equipos será entregado con sus respectivas cajas individuales y manuales técnicos, manuales de operación, cargador, interfaces de conexión, software y/o firmware de configuración (drivers) en medios digitales originales, para cada uno de los componentes del equipo que garanticen su pleno funcionamiento. Los manuales deben contener idioma inglés y/o español.

- El contratista deberá adjuntar en archivo digital e impreso en Excel el listado de los seriales, referencias, periodo de garantía, licenciamiento, de todos los equipos a entregar con el fin de verificar de una forma rapida el material.

</td></tr>
</table>

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

6	El contratista debe garantizar que toda representación gráfica debe cumplir normas fijas y preestablecidas para poder describir de forma exacta y clara; equipos, asignación de recursos físicos y licencias, al igual que dimensiones y características que permitan identificar la plataforma adquirida y habilitar la construcción del nuevo diseño elaborado. Al finalizar la implementación el contratista debe entregar un diagrama técnico detallado donde sea representado gráficamente cada uno de los componentes de Hardware y/o Software y/o firmware con sus correspondientes conexiones de red (datos y de potencia), con el propósito de proporcionar información suficiente para facilitar su análisis, mantenimiento e integración con las demás herramientas con las que cuenta el Ejército Nacional.
7	El contratista debe garantizar que los dispositivos de hardware ofertados como appliance deben tener las características y elementos para montaje en rack estándar, e incluir sus cables de alimentación eléctrica, cables para datos tipo RJ45, conversores RJ45 a RJ .5 y cables de fibra óptica necesarios para su correcta operación y funcionalidad de acuerdo con el diseño lógico y físico ofrecido. Así mismo deben ser instalados y configurados todos los elementos de la solución, lo cual no incurrirá en costos adicionales para el Ejército Nacional.
8	El contratista debe garantizar que los equipos a implementar deben ser compatibles con las plataformas actuales del Ejército Nacional y cumplir con el protocolo IPv4 e IPV6.
9	Para la implementación y conexión eléctrica no se podrán realizar apagados del centro de datos, por lo cual toda la actividad de implementación se debe realizar en producción sin afectar los servicios del centro de cómputo previa coordinación con el supervisor del contrato. De ser necesario un apagado programado, este debe ser coordinado con el supervisor del contrato, en donde el contratista deberá generar un plan de trabajo donde especifique actividades a desarrollar y el tiempo para cada una de ellas (minutograma).
10	El Contratista deberá disponer de personal técnico especializado, debidamente capacitado y certificado para realizar actividades de instalación, configuración, soporte, diagnóstico y solución de fallas de los equipos descritos en la Especificación Técnica No. **ET-JEMPP-CEDE6-0273**.
11	**Soporte Fabricante** Según las especificaciones proporcionadas, el horario de cobertura de soporte por parte del fabricante debe ser 24x7x365, lo que significa que debe estar disponible los 365 días del año, las 24 horas del día, incluyendo días festivos. Esto garantiza que el Ministerio de Defensa Nacional - Ejército Nacional - Batallón de Ciberdefensa y Ciberseguridad pueda recibir asistencia técnica y soporte en cualquier momento, incluso fuera del horario laboral regular. En cuanto a las actualizaciones de software y/o firmware, el fabricante debe proporcionarlas sin costo adicional durante el periodo de vigencia del contrato. Esto garantiza que el software y/o firmware utilizado en la solución se mantenga actualizado y cuente con las últimas mejoras y correcciones de seguridad sin incurrir en costos adicionales. Es importante tener en cuenta que estos aspectos relacionados con el soporte, la cobertura horaria y las actualizaciones de software y/o firmware deben ser detallados y especificados tanto en el contrato como en los términos de garantía, para asegurar que ambas partes, el Ministerio de Defensa Nacional - Ejército Nacional - Batallón de Ciberdefensa y Ciberdefensa el contratista, estén de acuerdo y cumplan con estas condiciones durante la ejecución del contrato. El Fabricante atreves del contratista debe incluir los servicios de revisión y validación del estado de salud de la plataforma generando informes para optimización y verificación de casos específicos solicitados por el supervisor del contrato.

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

12	**Garantía** El Contratista durante los primeros 15 días posteriores a la reunión de inicio deberá indicar el procedimiento que se deberá seguir para solicitar el servicio de garantía, tanto del hardware como de software y/o firmware de los servicios implementados. El contratista debe ofrecer el servicio de soporte técnico de la garantía para los sistemas y/o productos descritos en las Especificaciones Técnicas, durante la ejecución del contrato, es decir por un periodo de 02 años que es el término de la garantía. El horario de soporte por parte del contratista debe ser 24x7x365 remoto o presencial según lo solicite la entidad a partir de la firma del contrato, en caso de requerir cambios de equipos o partes por el fabricante, el contratista debe asumir todos los costos por desplazamiento, instalaciones, configuraciones y demás que sean necesarios en sitio sin que genere costo adicional para el Ejército Nacional. El término de la garantía técnica por parte fabricante será de mínimo dos (02) años para cada elemento del sistema de Seguridad DMZ. El término de la garantía técnica por parte del contratista será de mínimo dos (02) años para cada elemento del sistema de Seguridad DMZ desde la firma del acta de recibo a satisfacción. **Tiempos de respuesta:** El servicio de soporte debe ser atendido de manera inmediata de acuerdo a lo solicitado por el Batallón de Ciberdefensa y Ciberseguridad del Ejército Nacional durante la duración del periodo de garantía. Tiempo máximo de respuesta dos (02) horas después de haber reportado el incidente. De ser necesario el contratista deberá enviar personal técnico especializado a sitio en un tiempo máximo de cuatro (04) horas. El tiempo máximo permitido para restablecer el servicio es de 4 horas. **NOTA:** El Oferente deberá incluir con la oferta el procedimiento que se deberá seguir para solicitar el servicio de garantía de los servicios implementados.
13	**Certificación de Fabricante** El oferente deberá adjuntar, en documento independiente dentro de la oferta, certificado de fábrica que acredite que es canal certificado y que está autorizado para distribuir y brindar soporte a los productos requeridos para el cubrimiento de la necesidad, de conformidad con el anexo "Proyecto Pliego de Condiciones del Proceso" y el "Estudio Previo". Asimismo, deberá adjuntar certificados que acrediten que cuenta con ingenieros en redes, ciberseguridad y datacenter a nivel profesional.
14	**SERVICIO DE MIGRACIÓN E IMPLEMENTACIÓN:**
14.1	**Implementación del Proyecto** El contratista junto con el supervisor debe realizar un plan de trabajo de la propuesta de implementación del proyecto garantizando la integración de cada una de las capacidades y herramientas que se deben integrar con el sistema adquirido.

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

	El Contratista debe contar con personal técnico especializado, capacitado y certificado en cada una de las herramientas relacionadas en la presente especificación técnica para atender y solucionar los incidentes reportados durante la ejecución del contrato y el tiempo de soporte de todo el sistema. Antes de realizar una implementación el contratista debe garantizar compatibilidad con la infraestructura y arquitectura tecnológica actual e indicar que el presente proceso es para fortalecer e integrar la seguridad con la que cuenta actualmente el Ejército Nacional. El contratista asumirá los costos que genere las integraciones con las tecnologías que posee el Ejército Nacional que sean necesarias para el óptimo funcionamiento del sistema a implementar. El contratista debe entregar un diagrama técnico detallado donde sea representado gráficamente cada uno de los componentes de Hardware & Software y/o firmware con sus correspondientes conexiones de red (datos y de potencia), con el propósito de proporcionar información suficiente para facilitar su análisis, mantenimiento e integración con las demás herramientas con las que cuenta el Ejército Nacional. El contratista debe garantizar que los dispositivos de hardware ofertados como appliance deben tener las características y elementos para montaje en rack estándar, e incluir sus cables de alimentación eléctrica, cables para datos tipo RJ45, conversores RJ45 a RJ .5 y cables de fibra óptica necesarios para su correcta operación y funcionalidad de acuerdo al diseño lógico y físico ofrecido. Así mismo deben ser instalados y configurados todos los elementos de las soluciones, lo cual no incurrirá en costos adicionales para el Ejército Nacional. El sistema a implementar debe ser compatible con las plataformas actuales del Ejército Nacional y cumplir con el protocolo IPv4 e IPV6. Para la implementación y conexión eléctrica no se podrán realizar apagados del centro de datos, por lo cual toda la actividad de implementación se debe realizar en producción sin afectar los servicios del centro de cómputo previa coordinación con el supervisor del contrato. De ser necesario un apagado programado, este debe ser coordinado con el supervisor del contrato, para lo cual se deberá socializar un plan de trabajo por parte del contratista incluyendo tiempos y actividades a realizar (minutograma).

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

14.2	**Caso de Fallas** Los daños ocasionados por la implementación, desarrollo y puesta en marcha del contrato a cualquier elemento o sistema existente en la entidad serán asumidos por el contratista sin costo alguno para la entidad. El Contratista en caso de que al momento de las pruebas o instalación de las soluciones si algún equipo sale defectuoso el contratista está en la obligación de reemplazar los equipos por uno de las mismas características y/o superiores en un plazo no mayor a 30 días. El equipo no puede ser remanufacturado o reparado debe ser totalmente nuevo y deberá enviar los números de seriales para realizar los cambios pertinentes administrativos en el Ejército Nacional. En caso de presentarse fallas en cualquiera de los elementos que componen el sistema, se deberán efectuar los soportes todas las veces que se requiera; estos soportes deben incluir como mínimo: • Cambio de equipos en caso de fallas. • Remplazo de equipos por otros de iguales o superiores características. • Instalación de software y/o firmware. Configuraciones, puesta en producción y funcionamiento En caso de falla de alguno de los equipos, el fabricante deberá proporcionar los materiales y/o piezas para su reparación o reemplazo de características iguales o superiores.
14.3	**Migración:** El contratista deberá realizar una reunión inicial para el levantamiento de información y planificación para la implementación de la solución. El contratista deberá entregar un plan de trabajo y cronograma de trabajo donde se evidencien los recursos, tiempos, requisitos, factores críticos de éxito y responsables del proceso de implementación El contratista aplicara las mejoras prácticas de seguridad y ajustarlas a las políticas de seguridad informática de seguridad informática del Ejército Nacional. El contratista deberá integrar los equipos a la red y configurará el enrutamiento y la dirección IP. El contratista deberá contemplar dentro de su oferta todo el costo asociado al cableado estructurado, patch cord de cobre, fibra ópticas y demás elementos que se requiera para la implementación y puesta en funcionamiento del sistema de seguridad de accesos zona desmilitarizada del Ejército Nacional. **Integración:** Realizar una correcta instalación: Es importante realizar una correcta instalación de la solución, siguiendo las instrucciones proporcionadas por el fabricante y verificando que se cumplan los requisitos de hardware, software y/o firmware. Configuración adecuada: La configuración de la solución debe realizarse de manera adecuada, considerando las políticas de

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

	seguridad existentes en la organización y las necesidades de la red. Pruebas de integración: El contratista en conjunto con el supervisor del contrato debe realizar pruebas de integración para comprobar la eficacia de la solución en la infraestructura existente y asegurarse de que la solución esté proporcionando el servicio esperado.
15	**TRANSFERENCIA DE CONOCIMIENTO**
15.1	El Contratista debe realizar transferencia de conocimiento para 04 personas, del Batallón de Ciberdefensa y Ciberseguridad del Ejercito Nacional, dictado en instalaciones adecuadas por mínimo 40 horas, además debe expedir certificado de participación.
16	**RECURSOS HUMANOS**
15.1	La implementación deberá ser ejecutada directamente por el contratista, quien deberá disponer del personal mínimo requerido para garantizar la correcta planeación, ejecución, puesta en operación y estabilización de la solución. El oferente deberá presentar junto con la oferta la documentación que acredite el cumplimiento de los perfiles profesionales y certificaciones exigidas a continuación. **Líder del Proyecto** Profesional con título ingeniería de sistemas o electrónica o telecomunicaciones o eléctrica o informática o redes o software o carreras afines con formación de posgrado en gerencia de proyectos, mínimo tres (03) años de experiencia en soluciones de seguridad y/o arquitecturas DMZ. Será responsable de la coordinación, seguimiento y control del proyecto durante todas sus fases. Deberá contar con certificación vigente Project Management Professional (PMP) y CompTIA Security+. **Implementación:** Dos (02) Profesional con título en ingeniería de sistemas o telecomunicaciones con experiencia profesional mínima de dos (02) años en implementación de soluciones DMZ, con especialización en seguridad informática o seguridad de redes o ciberseguridad. Deberá acreditar las certificaciones vigentes: • Certificación nivel profesional en seguridad de redes • Certificación CompTIA Security+ o CISM o CISSP **DOCUMENTACIÓN DEL PERSONAL:** Para acreditar la **"Formación Académica"** se debe adjuntar con la oferta copia de los diplomas de los estudios realizados a nivel de pregrado, posgrado y/o de las certificaciones requeridas. Las certificaciones que contemplen tiempo de expiración deberán estar vigentes durante la evaluación del proceso y la ejecución del contrato. Para acreditar **"Experiencia Específica"**, debe anexar con la oferta copia de certificaciones laborales o contractuales, que indiquen por lo menos: (i) fecha de inicio, (ii) fecha de terminación, (iii) actividades

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

	ejecutadas, (iv) firma, nombre, dirección y teléfono de quien la expide. Se debe adjuntar con la oferta Hoja de vida, de la matricula y/o tarjeta profesional vigente, según aplique, expedida por el Consejo Profesional correspondiente para los profesionales que aplique y de la cédula de ciudadanía.

Teniente Coronel ROGER JESUS BUELVAS NARVÁEZ
Comandante Batallón de Ciberdefensa y Ciberseguridad

SV. [illegible] RUBIO
Comité Técnico Estructurador

PD02. SERGIO [illegible] ALFONSO GÓMEZ
Comité Técnico Estructurador

El OFERENTE

_____

REPRESENTANTE LEGAL O APODERADO
Nombre
Identificación Razón social
C.C. / NIT XXXXXXX