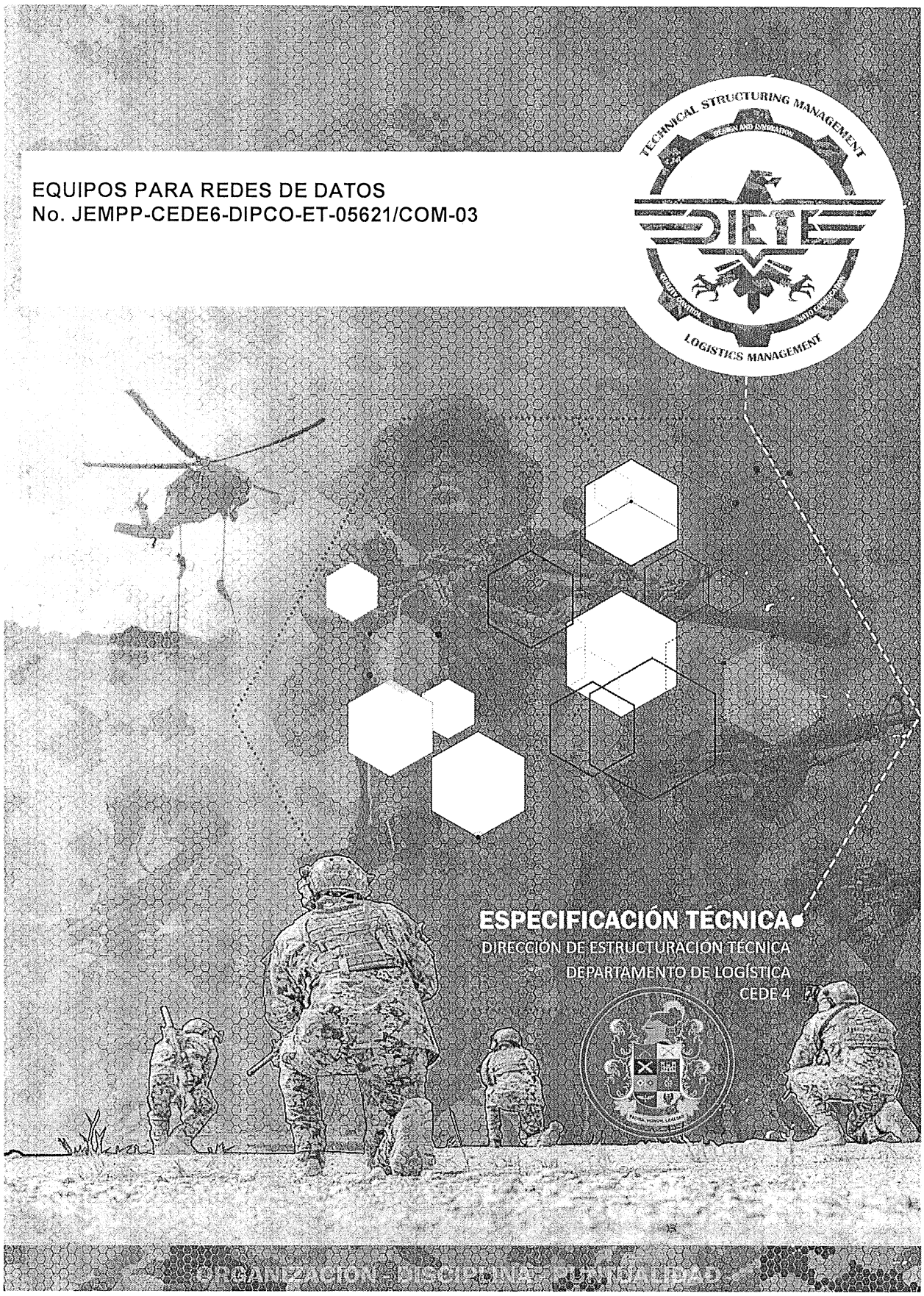
EQUIPOS PARA REDES DE DATOS
No. JEMPP-CEDE6-DIPCO-ET-05621/COM-03



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

CONTENIDO

1. OBJETO 3
2. DEFINICIONES Y APLICACIÓN 3
3. REQUISITOS 7
4. TOMA DE MUESTRAS Y CRITERIO DE ACEPTACIÓN O RECHAZO 25
5. MÉTODOS DE ENSAYO 26
6. APÉNDICE 26
7. ANEXOS 27
8. CONTROL DE REVISIONES 27

Elaboró	Revisó	Aprobó
TE HUMBERTO MARTINEZ PORTELA Técnico Estructurador	MY. DIEGO BENITEZ Ejecutivo y Segundo Comandante BAICC	TC. JHON WALTER QUIROGA LONDOÑO Comandante BAICC

No está autorizado su reproducción total o parcial

1. OBJETO

La presente especificación técnica tiene por objeto establecer los requisitos técnicos que se debe cumplir para la adquisición de un sistema de Switch Core en alta disponibilidad para fortalecer las plataformas tecnológicas, continuar con el desarrollo y sostenimiento de la capacidad de comando, control, comunicaciones, computación, ciberdefensa (C5), mediante proyectos, métodos, técnicas, servicios, aprendizaje, prospectiva e innovación, propendiendo por el desarrollo de los objetivos estratégicos de la fuerza.

2. DEFINICIONES 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 2°).

Cobertura:[2] Área geográfica en la que un operador de telecomunicaciones presta determinado tipo de servicio.

Conectividad:[3] Modelo de cofinanciación en el que participen constructores, beneficiaros VIS, prestadores de servicios de Internet, y el Estado.

Data Center:[4] Es el cerebro de la infraestructura tecnológica, agrupa todos los equipos y servidores esenciales para su buen funcionamiento.

Disponibilidad:[5] Propiedad de que la información y sus recursos relacionados deben estar disponibles y utilizables cuando se los requiera.

Firewall:[6] Un firewall es una aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico

---

[1] https://www.mintic.gov.co/portal/inicio/Glosario/

[2] https://www.mintic.gov.co/portal/inicio/Glosario/

[3] https://www.mintic.gov.co/portal/inicio/Glosario/

[4] https://www.cisco.com/c/dam/global/es_mx/solutions/small-business/pdf/glosario-smb.pdf

[5] https://www.mintic.gov.co/portal/inicio/Glosario/

[6] https://www.mintic.gov.co/portal/inicio/Glosario/

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

es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.

Fibra óptica: [7]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; permite la transmisión de comunicaciones telefónicas, de televisión, etc., a gran velocidad y distancia, sin necesidad de utilizar señales eléctricas.

Gbps:[8] Significa «Gigabits por segundo». 1Gbps es igual a 1,000 Megabits por segundo (Mbps) o 1,000,000,000 los bits por segundo. GBps se usa comúnmente para medir velocidades de transferencia de datos entre hardware dispositivos.

Interconexión: [9]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: [10]Es la interconexión que permite a cualquiera de los operadores interconectados, cursar el tráfico de otros operadores a la red del operador 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:[11] 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:[12] 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

---

[7] https://www.redcomputo.com.co/switches-core

[8] https://abrirarchivos.info/tema/definicion-de-gbps-gigabits-por-segundo

[9] https://www.mintic.gov.co/portal/inicio/Glosario/

[10] https://www.mintic.gov.co/portal/inicio/Glosario/

[11] https://www.mintic.gov.co/portal/inicio/Glosario/

[12] https://www.mintic.gov.co/portal/inicio/Glosario/

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

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.

MAC:[13] 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.

RETIE: [14] 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.

Router:[15] Los switches conectan los dispositivos en una red, y los routers conectan diferentes redes. Son dispositivos que crean los caminos para que viajen los datos y eligen las mejores rutas para que la información se transmita de forma rápida y segura.

Servicio:[16] 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:[17] 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.

Switches core:[18] 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

---

[13] https://protecciondatos-lopd.com/empresas/direccion-mac/#Que_es_la_direccion_MAC

[14] Resolución 18 0398 de 2004

[15] https://www.cisco.com/c/dam/global/es_mx/solutions/small-business/pdf/glosario-smb.pdf

[16] https://www.mintic.gov.co/portal/inicio/Glosario/

[17] https://www.cisco.com/c/dam/global/es_mx/solutions/small-business/pdf/glosario-smb.pdf

[18] https://www.redcomputo.com.co/switches-core

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

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.

Telecomunicación:[19] 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.

Trazabilidad:[20] La trazabilidad es la capacidad para rastrear un elemento del proyecto hasta otros elementos del proyecto relacionados, especialmente los que están relacionados con requerimientos. Los elementos del proyecto implicados en la trazabilidad se llaman elementos de trazabilidad. Entre los elementos de trazabilidad típico se incluyen diferentes tipos de requerimientos, elementos de modelos de análisis y diseño, artefactos de prueba y material de formación y documentación de soporte al usuario final.

Unidad de rack RU:[21] Es una unidad de medida usada para describir la altura del equipamiento preparado para ser montado en un rack de 19 o 23 pulgadas de ancho (48,26 cm o 58,42 cm). Una unidad rack equivale a 1,75 pulgadas (4,445 cm) de alto.

Zona de Cobertura:[22] 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 APLICACIÓN

El switch Core es el equipo encargado de centralizar y direccionar todo el tráfico de Datos, telefonía, videoconferencia e internet del Ejército Nacional, el cual cumple la función de interconectar a los diferentes medios de Carrier como son la RIC, Canales MPLS y canales Satelitales con los servidores, aplicativos, y equipos de Ciberdefensa, garantizando el correcto funcionamiento, seguridad y entrega de toda la Data de la Fuerza.

Realizar la adquisición del sistema switch de Core en alta disponibilidad para un comando funcional del Ejercito Nacional de Colombia, se deben considerar los siguientes aspectos durante la estructuración del proceso:

---

[19] https://www.mintic.gov.co/portal/inicio/Glosario/

[20] https://www.mintic.gov.co/portal/inicio/Glosario/

[21] https://www.cisco.com/c/dam/global/es_mx/solutions/small-business/pdf/glosario-smb.pdf

[22] https://www.mintic.gov.co/portal/inicio/Glosario/

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

2.2.1 En caso de establecerse condiciones de instalación, configuración y maquillado de todas las conexiones diferentes a lo descrito en esta Especificación Técnica, éstas deben ser acordadas entre la entidad contratante y el contratista.

2.2.2 En caso de existir controversia entre el texto donde se describen las características del elemento y si existieren figuras, prevalecerá el texto.

2.2.3 Se aclara que el contratista debe asumir los costos que generen por la realización de los ensayos, adecuaciones y recursos que se consideren necesarios para la instalación y el funcionamiento de toda la solución.

2.2.4 El proveedor cuando realice algún tipo de obra en los pisos, paredes, techos , guarda escobas, placas o vías de acceso, se compromete a entregar en perfecto estado todas las áreas donde haya realizado intervenciones, colocando materiales de igual o superior calidad a los existentes con terminación en resane, pisos, pintura del mismo color a la existente antes de la realización de la respectiva obra civil, en caso de presentarse algún daño, los costos de las reparaciones corren por cuenta del contratista.

3. REQUISITOS

3.1 REQUISITOS GENERALES

Se requiere el suministro de 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 switch de Core, conforme a cada una de los requerimientos relacionados en la presente especificación técnica.

3.2 REQUISITOS ESPECÍFICOS

No.	DESCRIPCION
3.2.1	
3.2.1.1	Se requiere el suministro y/o instalación y puesta en funcionamiento de equipos Switch 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.
3.2.1.2	El contratista encargado del proyecto debe garantizar la disponibilidad y provisión de todos los elementos y recursos necesarios para la implementación del Sistema, garantizando que todos los elementos sean totalmente nuevos.

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

3.2.1.3	Al finalizar la entrega a satisfacción, el contratista debe entregar al supervisor del contrato toda la documentación del proyecto terminado o elementos suministrados. Esta documentación debe incluir planos o diseños finales, certificaciones, manuales y documentos de garantías de los equipos utilizados en la implementación del sistema, según corresponda
3.2.1.4	En el marco del proceso de adquisición de los switch para la red del Ejército Nacional de Colombia, es importante que el oferente que se presente en el presente proceso, cuente con la debida autorización por parte de la casa matriz del equipo que está ofertando, para garantizar que está debidamente autorizado para distribuir y vender los equipos, se requiere que adjunte una certificación emitida por la casa matriz que lo acredite como distribuidor autorizado de la solución de equipos activos switch.
3.2.1.5	Es importante garantizar que los elementos suministrados sean de primera calidad y cumplan con las especificaciones pactadas. Por ello, el oferente deberá presentar una certificación donde garantice que todos los elementos suministrados son nuevos y de primera calidad, y no re-manufacturados. El contratista que resulte adjudicado se obliga a reparar o reemplazar cualquier elemento que presente problemas de calidad o defectos de fabricación durante un plazo mínimo de tres (3) años. En caso de que algún elemento suministrado deba ser enviado a reparación, el contratista deberá entregar uno (1) en reemplazo mientras dure la reparación, de igual o superior calidad y características que cumplan con todas las especificaciones y funcionalidades para garantizar el servicio. El contratista deberá disponer de líneas de atención para determinar las fallas y resolverlas en un plazo máximo de 48 horas, incluyendo los repuestos y el soporte técnico emitido por el fabricante. Cualquier gasto generado por la reparación o reemplazo será asumido por el contratista, sin afectar al Ejército Nacional.
3.2.1.6	Es obligación del contratista realizar las siguientes actividades para la migración del equipo: Planificación: La migración del switch Core 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 switch Core 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. Verificación y pruebas: Una vez que se ha completado la migración, es esencial verificar y probar el nuevo SWITCH CORE para asegurarse de que esté funcionando correctamente y cumpla con los requisitos de la red.

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

	Se deberá entregar un informe detallado de las actividades realizadas para la migración del equipo, incluyendo: Copia de seguridad de los equipos Configuración del nuevo equipo Pruebas de funcionamiento Capacitación al personal Documentación (Topologías)
3.2.1.7	El personal que realice la instalación contará con el equipo de protección personal adecuado, como cascos, guantes, gafas de seguridad, botas dieléctricas de seguridad, pulseras electrostáticas, entre otros, para evitar posibles riesgos laborales. Por último, se debe tener en cuenta que el personal asignado al proyecto deberá seguir las instrucciones y lineamientos establecidos por el supervisor del contrato y el Ejército Nacional para garantizar la integridad de la obra y la seguridad de todas las personas involucradas en ella.
3.2.1.8	En caso de alguna situación de emergencia sanitaria, los trabajos se deberán realizar bajo todos los protocolos de Bioseguridad contemplados en la normatividad vigente a la fecha de ejecución del contrato, en caso tal de presentase algún funcionario con síntomas debe aislarse de inmediato y seguir las recomendaciones médicas para evitar la propagación de cualquier virus; se debe mantener en ese estado hasta que reúna los criterios necesarios (PRUEBA NEGATIVA) para que pueda regresar a trabajar.
3.2.1.9	Dentro de la primera semana, contada a partir de la fecha de perfeccionamiento del contrato, el contratista presentara el cronograma detallado donde se relaciona la secuencia de las actividades a desarrollar durante la instalación, configuración y puesta en funcionamiento de cada uno de los equipos relacionados en la presente especificación técnica. El cronograma será aprobado por el supervisor del contrato.
3.2.1.10	El contratista después de perfeccionado el contrato, en un plazo máximo de diez (10) días hábiles, enviará toda la documentación requerida por el EJC para elaborar los estudios de seguridad del personal técnico que realizará los trabajos de implementación de toda la solución.
3.2.1.11	El contratista entregará, previo al acta de recibo a satisfacción del contrato, un documento en dos originales impresos en una carpeta tipo folder, este será general y debe incluir todas las topologías, esquemas de conexión, configuraciones y versiones de software, certificados de licencias entregadas y cualquier otra información relevante al proyecto. También entregará una copia en medio magnética con toda la información (CD), para los fines propios de la supervisión del contrato.
3.2.1.12	El proveedor realizara la migración de los equipos teniendo en cuenta todas las configuraciones existentes, en los equipos incluyendo el direccionamiento IPV6. El proveedor debe realizar la instalación, configuración y marquillado de todas las conexiones que tengan los equipos instalados en la actualidad.
3.2.2	CONFIDENCIALIDAD DE LA INFORMACION

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

3.2.2.1	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 presente 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 presente 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. El contratista velara por la confidencialidad de los lugares que conozca y garantizara reserva de la información en tal sentido el supervisor del contrato coordinara la elaboración del respectivo estudio de seguridad y confidencialidad del personal asignado para la ejecución del contrato, en el evento de que alguna persona no apruebe el estudio realizado por la oficina de seguridad correspondiente el futuro

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

	contratista se comprometerá a cambiarlo de manera inmediata en igual sentido se compromete a que el personal asignado no será cambiado durante la ejecución del contrato salvo por expresa autorización del Ejercito Nacional.
3.2.3	NIVELES DE SERVICIO
3.2.3.1	El contratista deberá efectuar la garantía todas las veces que se requiera en caso de presentarse fallas en los sistemas o equipos adquiridos, esta garantía debe incluir como mínimo: a). Cambio de partes y/o repuestos y/o equipos nuevos b). Remplazo de equipos por otros de iguales o superiores características. c). Instalación y/o reparación de software. d). Configuraciones, puesta en producción y funcionamiento. e). El servicio será prestado en sitio en la ciudad de Bogotá de acuerdo a los tiempos de respuesta establecidos. f). El tiempo máximo permitido para cambio de partes, repuestos o reparación del equipo es de 24 horas calendario una vez sea reportado el incidente. g). Si después de 24 horas después de haber reportado el incidente y el contratista no ha solucionado el problema, se debe suministrar, instalar, configurar y poner en funcionamiento temporalmente, un equipo, repuestos o partes de iguales o superiores características técnicas, hasta tanto se dé solución definitiva a la novedad o incidente reportado, sin costo adicional para la institución, con el fin de garantizar la continuidad en la prestación de los servicios. h). De no ser posible la reparación del equipo, el contratista a través del fabricante repondrá el equipo en su totalidad por uno nuevo de iguales o superiores características técnicas, con un plazo máximo de 30 días calendario después de reportado el incidente. (El equipo debe ser nuevo y no re manufacturado). i). En caso de cambio de equipos, repuestos o partes de contengan dispositivos o elementos de almacenamiento, estos serán destruidos o borrados de forma segura por parte de la institución. j). El contratista deberá suministrar, instalar, configurar y poner en perfecto funcionamiento los equipos, partes o repuestos garantizando la continuidad de los servicios. k). En caso de que el repuesto ocasione la reinstalación o reconfiguración de software, sistema operativo o firmware, estas labores deben ser realizadas por el contratista sin costo adicional para la institución. l). Todos los gastos que se ocasionen por concepto de transporte de equipos y/o partes y otros gastos a fin de cumplir con las garantías correrán a todo costo por parte del contratista. m). El contratista debe prestar el servicio de garantías remotamente a través de herramientas WEB online de acuerdo a los tiempos de respuesta y en sitio cuando así se requiera. n). El contratista debe tener atención ilimitada por garantía a casos reportados por Comando de Personal, referentes a cualquier evento relacionado con el funcionamiento, administración, incidentes o eventos de seguridad de los sistemas, equipos o plataformas adquiridas, hasta dejar en completo funcionamiento el

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

	sistema. Es por ello que se requiere que el oferente certifique que, dentro de su nómina, cuenta con personal certificado en la marca de equipos switch core ofertados.
3.2.4	**REQUERIMIENTOS ADICIONALES**
3.2.4.1	El contratista realizara la migración de los equipos teniendo en cuenta todas las configuraciones existentes, en los equipos incluyendo el direccionamiento IPV6. El contratista debe realizar la instalación y configuración y maquillado de todas las conexiones que tenga el switch core en alta disponibilidad El contratista dentro de los 10 días hábiles siguiente del inicio de ejecución de contrato deberá presentar al Supervisor del Contrato, un cronograma de actividades para la ejecución del proyecto, teniendo en cuenta los tiempos de importación, configuración, instalación, pruebas y puesta en funcionamiento, así como la capacitación.

ESPECIFICACONES TECNICAS DE LOS EQUIPOS A ADQUIRIR

ITEM No.1. ADQUISICIÓN DE EQUIPO SWITCH CORE EDIFICIO COMANDO DE PERSONAL

No.	REQUERIMIENTOS GENERALES
3.3	
3.3.1	**SISTEMA DE SWITCH CORE CAPA 3**
3.3.1.1	El sistema debe contemplar un sistema de switch de core en alta disponibilidad compuesto por 02 equipos activos switch, los cuales deben quedar interconectados por dos cables QSFP para STACK, incluye suministro, instalación y configuración de equipos. Cada equipo deberá estar en la capacidad de:
3.3.1.2	Switch de 24 puertos slot SFP+ 1G/10G + 12 puertos RJ45 1G/2.5G/5G/10G Base-T + Tarjeta 4 puertos 40/100 Gbps de tipo QSFP/QSFP28/
3.3.1.3	Unidades de Rack 1(Una)
3.3.1.4	El sistema debe traer incluido los módulos SFP+ 1G/10G + que se requieran para la migración, estos son necesarios para la implementación, de la misma manera suministrara para la implementación los patch cord de fibra óptica OM3 o superior, que se requieran para la migración del equipo, sin superar la cantidad de puertos del mismo.
3.3.1.5	Apilamiento: Soporte de apilamiento de hasta 4 Switches, comportándose como uno solo, administrable con una sola dirección IP y velocidad de stacking mínimo de 160Gbps.
3.3.1.6	- Switching fabric Minima 1,92Tbps
3.3.1.7	- Forwarding Rate Mínimo 1190 Mpps
3.3.1.8	- Soporte V LANS 4k
3.3.1.9	- 8 colas de prioridad por puerto
3.3.1.10	- Clasificación de tráfico tipo wirespeed
3.3.1.11	- QoS basado en políticas sobre VLAN, puerto, MAC

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

3.3.1.12	- Capacidad de remarcado extensivo
13.3.1.13	- Taildrop para control de congestión de encolamiento
3.3.1.14	- Marcado DiffServ y Ipprecedence sobre capa 2, 3 y 4.
3.3.1.15	- ACLs Basado en cabeceras de capa 3, capa 4 y hardware ACL.
3.3.1.16	**Accesorios** Los necesarios para su instalación y funcionamiento. **Certificaciones de organismos de seguridad** - EN55032 class A, EN55024, EN61000-3-levels 2, EN60950-1, EN60825-1, AS/NZS, 60950, FCC class A, VCCI class A, UL60950-1, CAN/CSA-C22.2 No.60950-1-03, UL, cUL, EU RoHS compliant, China RoHS compliant
3.3.1.17	**Normas soportadas IEEE Standards:** - IEEE 802.3ab 1000BASE-T - IEEE 802.3ae 10 Gigaxbit Ethernet - IEEE 802.3ba 40GBASE-X - IEEE 802.3z 1000BASE-X - IEEE 802.3bj 100GBASE-X - IEEE 802.3bz 2.5GBASE-T 5GBASE-T - IEEE 802.1ad Provider bridges (VLAN stacking, Q-in-Q) - IEEE 802.1Q Virtual LAN (VLAN) bridges - IEEE 802.1v VLAN classification by protocol and port - IEEE 802.3ac VLAN tagging - IEEE 802.1X authentication protocols (TLS, TTLS, PEAP and MD5) - IEEE 802.1X multi-supplicant authentication - IEEE 802.1X port-based network access control - IEEE 802.1p Priority tagging - IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) **RFC Standards:** - RFC 894 Standard for the transmission of IP data grams over Ethernet networks - RFC 950 Internet standard subnetting procedure - RFC 951 Bootstrap Protocol (BootP) - RFC 1027 Proxy ARP - RFC 1035 DNS client - RFC 1042 Standard for the transmission of IP data grams over IEEE 802 networks - RFC 1071 Computing the Internet checksum - RFC 1122 Internet host requirements - RFC 1542 Clarifications and extensions for BootP - RFC 1591 Domain Name System (DNS) - RFC 1812 Requirements for Ipv4 routers - RFC 1981 Path MTU discovery for Ipv6 - RFC 2460 Ipv6 specification - RFC 2464 Transmission of Ipv6 packets over Ethernet networks - RFC 3484 Default address selection for Ipv6 - RFC 3596 DNS extensions to support Ipv6

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

	- RFC 4007 Ipv6 scoped address architecture - RFC 4193 Unique local Ipv6 unicast addresses - RFC 4291 Ipv6 addressing architecture - RFC 4443 Internet Control Message Protocol (ICMPv6) - RFC 2863 Interfaces group MIB - RFC 3176 sFlow: a method for monitoring traffic in Switched and routed networks - RFC 4862 Ipv6 Stateless Address Auto-Configuration (SLAAC) - RFC 5014 Ipv6 socket API for source address selection - RFC 5095 Deprecation of type 0 routing headers in Ipv6 - RFC 5175 Ipv6 Router Advertisement (RA) flags option Internets - RFC 1518 An architecture for IP address allocation with CIDR - RFC 1519 Classless Inter-Domain Routing (CIDR) - RFC 1212 Concise MIB definitions - RFC 1213 MIB for network management of TCP/IP-based Internets: MIB-II - RFC 1215 Convention for defining traps for use with the SNMP - RFC 1227 SNMP MUX protocol and MIB - RFC 1239 Standard MIB - RFC 1724 RIPv2 MIB - RFC 4292 IP forwarding table MIB - RFC 2578 Structure of Management Information v2 (SMIv2) - RFC 2579 Textual conventions for SMIv2 - RFC 3810 Multicast Listener Discovery v2 (MLDv2) for Ipv6 - RFC 3956 Embedding the Rendezvous Point (RP) address in an Ipv6 multicast address - RFC 2580 Conformance statements for SMIv2 - RFC 2616 Hypertext Transfer Protocol – HTTP/1.1 - RFC 2821 Simple Mail Transfer Protocol (SMTP) - RFC 6105 Ipv6 Router Advertisement (RA) guard - RFC 1155 Structure and identification of management information for TCP/IP based - RFC 2674 Definitions of managed objects for bridges with traffic classes, multicast filtering and VLAN extensions - RFC 2741 Agent extensibility (AgentX) protocol - RFC 2787 Definitions of managed objects for VRRP - RFC 2819 RMON MIB (groups 1,2,3 and 9) - RFC 3411 An architecture for describing SNMP management frameworks - RFC 3412 Message processing and dispatching for the SNMP - RFC 3415 View-based Access Control Model (VACM) for SNMP - RFC 2453 RIPv2 - RFC 5246 TLS v1.2 - RFC 854 Telnet protocol specification - RFC 2818 HTTP over TLS ("HTTPS") - RFC 2865 RADIUS authentication - RFC 2866 RADIUS accounting - RFC 2868 RADIUS attributes for tunnel protocol support

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

	- RFC 3280 Internet X.509 PKI Certificate and Certificate Revocation List (CRL) profile - RFC 3546 Transport Layer Security (TLS) extensions - RFC 3579 RADIUS support for Extensible Authentication Protocol (EAP) - RFC 3580 IEEE 802.1x RADIUS usage guidelines - RFC 3748 PPP Extensible Authentication Protocol (EAP) - RFC 3416 Version 2 of the protocol operations for the SNMP - RFC 3417 Transport mappings for the SNMP - RFC 3630 Traffic engineering extensions to OSPF - RFC 4552 Authentication/confidentiality for OSPFv3 - RFC 3418 MIB for SNMP - RFC 4022 MIB for the Transmission Control Protocol (TCP) - RFC 4113 MIB for the User Datagram Protocol (UDP) - RFC 1112 Host extensions for IP multicasting (IGMPv1) - RFC 2236 Internet Group Management Protocol v2 (IGMPv2) - RFC 2710 Multicast Listener Discovery (MLD) for Ipv6 - RFC 2715 Interoperability rules for multicast routing protocols - RFC 2597 DiffServ Assured Forwarding (AF) - RFC 3246 DiffServ Expedited Forwarding (EF) - RFC 3973 PIM Dense Mode (DM) - RFC 4541 IGMP and MLD snooping Switches - RFC 4601 Protocol Independent Multicast – Sparse Mode (PIM-SM): protocol specification (revised) - RFC 4604 Using IGMPv3 and MLDv2 for sourcespecific multicast - RFC 1246 Experience with the OSPF protocol - RFC 1370 Applicability statement for OSPF - RFC 1765 OSPF database overflow - RFC 2370 OSPF opaque LSA option - RFC 2740 OSPFv3 for Ipv6 - RFC 3101 OSPF Not-So-Stubby Area (NSSA) option - RFC 3509 Alternative implementations of OSPF area border routers - RFC 3623 Graceful OSPF restart - RFC 5329 Traffic engineering extensions to OSPFv3 - RFC 2211 Specification of the controlled-load network element service - RFC 5798 Virtual Router Redundancy Protocol version 3 (VRRPv3) for Ipv4 and Ipv6 - RFC 1058 Routing Information Protocol (RIP) - RFC 2080 RIPng for Ipv6 - RFC 2081 RIPng protocol applicability statement - RFC 2082 RIP-2 MD5 authentication - RFC 4251 Secure Shell (SSHv2) protocol architecture - RFC 4252 Secure Shell (SSHv2) authentication protocol - RFC 4253 Secure Shell (SSHv2) transport layer protocol - RFC 4254 Secure Shell (SSHv2) connection protocol - RFC 855 Telnet option specifications

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

	- RFC 857 Telnet echo option - RFC 858 Telnet suppress go ahead option - RFC 1091 Telnet terminal-type option - RFC 2822 Internet message format - RFC 3046 DHCP relay agent information option (DHCP option 82) - RFC 3306 Unicast-prefix-based Ipv6 multicast addresses - RFC 3376 IGMPv3 - RFC 2474 DiffServ precedence for eight queues/port - RFC 2697 A single-rate three-color marker - RFC 2698 A two-rate three-color marker - RFC 2475 DiffServ architecture - RFC 1350 Trivial File Transfer Protocol (TFTP) - RFC 1985 SMTP service - RFC 2049 MIME - RFC 2131 DHCPv4 (server, relay and client) - RFC 2132 DHCP options and BootP vendor extensions - RFC 3315 DHCPv6 (server, relay and client) - RFC 3633 Ipv6 prefix options for DHCPv6 - RFC 3646 DNS configuration options for DHCPv6 - RFC 3993 Subscriber-ID suboption for DHCP relay agent option - RFC 4330 Simple Network Time Protocol (SNTP) version 4 - RFC 5905 Network Time Protocol (NTP) version 4 **Otros:** - ITU-T G.8032 Ethernet ring protection Switching - Bootstrap Router (BSR) mechanism for PIM-SM - IGMP/MLD multicast forwarding (IGMP/MLD proxy) - TACACS+ Accounting, Authentication, Authorization (AAA) - Generic VLAN Registration Protocol (GVRP) - MLD snooping (MLDv1 and v2) - PIM and SSM for Ipv6 - OSPF link-local signaling - OSPF MD5 authentication - OSPF restart signalingSSH remote login - SSLv2 and SSLv3 - Out-of-band LSDB resync - IGMP query solicitation - IGMP snooping (IGMPv1, v2 and v3) - IGMP snooping fast-leave - AES (ECB, CBC, CFB and OFB Modes) - 3DES (ECB, CBC, CFB and OFB Modes) - CCM - CMAC - GCM

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

	- XTS - DSA - ECDSA - RSA - SHA-1 - SHA-2 (SHA-224, SHA-256, SHA-384. SHA-512) - HMAC (SHA-1, SHA-2(224, 256, 384, 512) - Ficha técnica Del equipo ofertado (es obligatorio adjuntar la ficha técnica junto con el presente anexo) - Hasta 96K MAC address entries. - 4 GB DDR SDRAM - Optical Digital Diagnostic Monitoring (DDM) - Automáticamente detecte flaps y apague el puerto. - Ping polling para IPV4 e IPV6. - SNMPv6, TELNET v6, SSHv6. - Que pueda limitar el ancho de banda del puerto a 64 kbps. - QoS basado en Políticas sobre VLAN puerto y/o MAC. - Clasificación general de paquetes
3.3.1.18	El Switch debe estar en la capacidad de administrar vía CLI otros Switch de la misma marca de fabricante que estén dentro de la red de datos. De manera virtual incluirlos dentro de su plataforma y poderlos gestionar, administrar y automatizar. Bajo su plataforma poder guardar copias de seguridad de configuraciones y firmware
3.3.1.19	Monitoreo constante de enlaces de fibra óptica, evitando espionaje en las comunicaciones de fibra. Al detectar intrusión, el enlace debe ser shut down automáticamente y alertar al responsable de red. Se debe explicar en la propuesta como el Switch realiza esta función.
3.3.1.20	Al menos dos (2) mecanismos adicionales al STP, RSTP y MSTP para detectar puertos involucrados en loop y poder tomar acciones de forma predeterminada por comandos sobre dichos puertos (mecanismos diferentes a los protocolos basados en Spanning Tree).
3.3.1.21	- Mecanismo para detectar si una Mac Address se está viendo por más de un puerto y poder tomar acciones de forma predeterminada por comandos sobre dichos puertos
3.3.1.22	- Capacidad de formar anillos y recuperarse ante la falla de un enlace del anillo máximo en 50 milisegundos
3.3.1.23	El Switch debe estar en la capacidad de evitar bucles que se presenten en la red de datos, se debe contar con thrash limiting para detectarlos antes que se produzca una tormenta de broadcast e interrumpa los servicios de red
3.3.1.24	Compatibilidad con PVST+
3.3.1.25	Capacidad de formar stacking con distancia de al menos 1500 metros bien sea por puertos SFP+ o QSFP+
3.3.1.26	UDLD
3.3.1.27	Mecanismo que apoye el ahorro de energía sobre fuentes que no se usen al máximo o sobre leds de los puertos mientras no se requieran, aunque tengan enlaces activos.
3.3.1.28	Capacidad de realizar scripting en CLI

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

3.3.1.29	Debe poder operar OSPF, BGP4, BGP4+, PIM4-DM, PIM4-SSM, PIM6-DM, PIM6-SSM Q-in-Q, RIPng
3.3.1 30	Debe soportar el protocolo G.8032 para anillos
3.3.1.31	Secure copy (SCP)
3.3.1.32	Triple-autenticacion: basada en MAC, basada en web y por IEEE 802.1X
3.3.1.33	Soporte para TACACS+ commands
3.3.1.34	ACL basadas en cabeceras de capa 3 y 4.
3.3.1.35	ACL de capa 2 para Ipv6
3.3.1.36	Soporte para jumbo frames de mínimo 9KB
3.3.1.37	Capacidad de stacking de 160 Gbps de ancho de banda
3.3.1.38	Que posea puerto USB para poder cargar software, configuraciones o backups
3.3.1.39	Soporte para OpenFLow al menos versión 1.3
3.3.1.40	Buffer de memoria para paquetes de al menos 16MB.
3.3.1.41	Capacidad de 2 fuentes de poder simultáneos, removibles en caliente. (El contratista deberá entregar una fuente de poder para el equipo de core.
3.3.1.42	Debe soportar VRF Lite.
3.3.1.43	Debe tener administración por CLI y Web.
3.3.1.44	Cada switch debe venir con su propio cable de stack de 100Gbps, con conector tipo QSFP28 y de 1 Metro de distancia mínimo, el cable debe ser original y de la misma marca del fabricante del switch, debe venir con garantía del mismo fabricante del swtich.
3.3.1.45	Se debe suministrar para cada uno de los switch la totalidad de módulos SPF a 10G en cada uno de los puertos respectivamente y según especificación técnica.
3.3.1.46	El sistema debe traer incluido los cassettes (sextuplex), y patch cord de fibras requeridas entre el switch de core y los gabinetes (06) pisos existentes entre el DATACENTER y los pisos del edificio COPER, realizando un enlace de fibra entre cada uno de los gabinetes, esta implementación se realizará de acuerdo a las indicaciones que establezca la fuerza, implementando enlaces redundantes y configurando LACP a 20g para cada uno de los pisos, con las siguientes especificaciones así:
3.3.2	**PATCH-CORD DE FIBRA ÓPTICA MULTIMODO**
3.3.2.1	Los PATCH-CORD a suministrar deberán ser elaborados de fábrica certificados, multimodo con chaqueta LSZH que se ajusten a las normas IEC o EIA o TIA. Con conexión OM3 y conector estándar LC
3.3.2.2	Cordon Duplex (2-fiber) jacketed zipcord, Tight buffered
3.3.2.3	Clase: Fibra Multimodo
3.3.2.4	Tipo: Patch Cords Fibra Óptica
3.3.2.5	Clasificación de Fibra Óptica: OM3
3.3.2.6	Modo de Transmisión: Duplex
3.3.2.7	Tipos de Conectores: LC a LC
3.3.2.8	Pulitura: UPC
3.3.2.9	Tipo de Chaqueta: Chaqueta LSZH
3.3.2.10	Color Chaqueta: Aqua

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

3.3.2.11	Espesor de Cable: Chaqueta 2mm
3.3.2.12	Velocidad de Transmisión: 10 GBIT
3.3.2.13	Metraje: 3m
3.3.3	**MODULOS SFP MM 10G**
3.3.3.1	Maximum Distance OM3 - 300 m
3.3.3.2	Longitud de Onda 850 nm
3.3.3.3	Temperatura de operación 0°C to 70°C (32°F to 158°F)
3.3.4	**NORMATIVIDAD TÉCNICA**
3.3.4.1	Se deben cumplir o exceder las siguientes especificaciones de instalación, documentación, componentes y sistemas de la industria.
3.3.4.2	ANSI/TIA-568-C.0 Generic Telecommunications Cabling for Customer Premises 2009. Norma que dicta las directrices para cableado genérico de telecomunicaciones en instalaciones de clientes.
3.3.4.3	ANSI/TIA-568-C.1 Commercial Building Telecommunications Cabling Standard 2009. Norma internacional que estipula las condiciones del cableado de telecomunicaciones para una edificación comercial.
3.3.4.4	ANSI/TIA-568.2-D Commercial Building Telecommunications Cabling Standard Agosto 2009. Norma que crea y estipula directrices de los diferentes componentes de un sistema de telecomunicaciones basado en transmisión en cables de pares trenzados.
3.3.4.5	ANSI-J-STD 607 y adendos "Commercial Building Grounding and Bonding Requirements for Telecommunications" (Requisitos para Telecomunicaciones de Puesta y Unido a Tierra en Edificios Comerciales).
3.3.4.6	IEC/TR3 61000-5-2 – Ed. 1.0 y enmiendas
3.3.4.7	"Electromagneticcompatibility (EMC) – Part 5: Installation and mitigationguidelines – Section 2: Earthing and cabling" (Compatibilidad electromagnética (EMC) – Parte 5: Directrices de instalación y mitigación – Sección 2: Conexión a tierra y cableado).
3.3.4.8	ISO/IEC 11801:2000 Ed2.0 y enmiendas "Information technology – Generic cabling for customer premises" (Cableado Genérico para Propiedades de Usuario).
3.3.4.9	ANSI/TIA 942 Telecommunications Infrastructure Standard for Data Centers.
3.3.4.10	ISO/IEC 24764 draft Generic cabling for Data Centre premises.
3.3.4.11	NEMA, NEC: En caso de existir vacíos en lo referente a aspectos particulares en las Normas locales.
3.3.4.12	El proveedor deberá cumplir con el Reglamento Técnico de Instalaciones Eléctricas (RETIE) que se encuentra en la norma NTC 2050.
3.3.4.13	El proveedor debe suministrar la Lista de Artículos objeto del presente expediente en medio físico y magnético, que contendrá exactamente la siguiente información, estructurada en los campos que a continuación se indican, del siguiente modo: PNR= Número de pieza/referencia, código EAN si lo tiene. NCAGE=Identidad del fabricante verdadero con página web, números de teléfono, Dirección Ciudad, País. DESCRIPCION= Nombre o designación con que dicho fabricante identifica cada artículo objeto de la presente adquisición. NSN/NOC= Número OTAN de Catálogo.

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

	Si los artículos ya dispusieran de número OTAN de catálogo por que provienen de un país OTAN el contratista solamente entregará la lista de los nombres técnicos cada uno con su NOC. NOTA: Para los elementos que no cuenten con el código OTAN (NSN/NOC= Número OTAN de Catálogo) los adjudicatarios deberán suministrar la información restante solicitada en el presente numeral (PNR, NCAGE, DESCRIPCIÓN).

ITEM No.2. ADQUISICIÓN DE EQUIPO SWITCH CORE EJERCITO NACIONAL Y SISTEMA PARA MONITOREO DE LAS REDES DEL EJERCITO NACIONAL - PARA "NOC" DEL BAICC	
3.4	SWITCH TIPO 1 EQUIPO DE CORE TIPO CHASSIS
3.4.1	Tipo Modular
3.4.2	Switch de capa 2, 3
3.4.3	El equipo debe incluir más de cuatro (4) bahías de ancho completo para módulos de Entrada/Salida (I/O).
3.4.4	- La solución debe incluir 48 interfaces de 1G, RJ45 1000Base-T POE+ Class 4 Las interfaces incluidos deben ser todas no bloqueantes
3.4.5	Interfaces - interfaces de 25G y/o 10G SFP/SFP+ Ethernet - Interfaces 40G/100Gbps QSFP Ethernet - Las interfaces incluidas deben ser todas no bloqueantes, se deben incluir los módulos SFP de acuerdo a necesidad descrita.
3.4.6	Cada chassis debe Incluir mínimo: - Configurables 4 Fuentes de Poder redundantes de mínimo 1800W AC 1 módulo de disipadores de temperatura.
3.4.7	- La velocidad de conexión de los módulos o bahías debe ser de mínimo de 2,8 Tbps
3.4.8	El equipo debe tener la capacidad de conectarse en stack o stacking o contar con una tecnología similar que permita realizar la administración de forma homologa, debe cumplir las siguientes características: - Ser percibido por los demás equipos como un único switch de modo que se pueda configurar agregación de puertos entre ellos. - Garantizar alta disponibilidad ante la falla de un chasis y la actualización de software. - La configuración debe sincronizarse entre los miembros del stack

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

	- Operación de los miembros del stack en modo activo-activo tanto en L2 como en L3. - Incluir todo el hardware que requiera la conexión del stack o tecnología similar para minimo dos (2) enlaces de 100Gbps entre los equipos.
3.4.9	El equipo debe tener como mínimo: - Throughput: 5 Bpps - Capacidad de conmutación: minimo 14 Tbps.
3.4.10	Debe soportar los siguientes Protocolos: - Protocolos de enrutamiento (RIP, OSPF) - PBR - PIM SM - PVLAN, - VRRP, - QoS, - 802.1X, - IP SLA - IPV4 – IPV6
3.4.11	Debe soportar los siguientes protocolos avanzados de conmutación: - BGP. - BSR, - MSDP, - PIM SM, - PIM SSM, - IP SLA, - OSPF
3.4.12	De soportar tecnologías de segmentación de Red: - VRF, - Software-Defined Access VXLAN - MPLS.
3.4.13	- El sistema operativo debe incluir la última versión completa (con todos los protocolos, servicios y funcionalidades que el equipo sea capaz de realizar) liberada por el fabricante a la fecha de la compra.

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

3.4.14	Debe soportar las siguientes características de protocolo Enrutamiento IP: - RIPv2, y RIPng - OSPFv2 y OSPFv3 - BGPv4 - VRF, VPN - Multicast (IPv4/IPv6) - MPLS - Border Gateway Protocol version 4 Protocol-Independent Multicast (PIM) Sparse- Mode (PIM- SM)
3.4.15	El equipo debe soportar las siguientes especificaciones físicas: - 8 unidades de Rack máximo - Voltaje de operación AC: min 92V a max 262V, entre min 48 a max 63 Hz - Temperatura de operación -5° a 40° C a 10,000 pies -
3.4.16	Acceso y configuración: - Línea serial de comandos (CLI) - Web - SSH v2
3.4.17	El switch debe estar en la capacidad de realizar monitoreo de puertos de entrada y salida (Mirroring) deberá contar con minimo 4 puertos de esta característica.
3.4.18	Listas de Control de Acceso: - Aplicables a puertos y VLANs Parámetros configurables de Capa 2 (MAC origen/destino), Capa 3 (IP/subred origen/destino) y Capa 4 (ICMP/UDP/TCP especificando puerto).

ITEM No.3. ADQUISICIÓN DE EQUIPO SWITCH L3 DE DISTRIBUCION PARA REDES LAN A NIVEL NACIONAL	
No. 3.5	REQUERIMIENTOS GENERALES
3.5.1	La solución debe cumplir con al menos las siguientes características técnicas para los dispositivos:
3.5.2	• Seguridad mediante el uso de agentes Phyton y API Rest. • Interfaz Api Rest programable. • Memoria QuadCore Arm Cortex A72 a 1,8 GHz

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

	• Fuente de alimentación fija. • Alta disponibilidad con PoE • Debe ser compatible con SNMP • SNMPRead único de lectura para CPU. • (IEEE 802.1p) para clasificación en tiempo real. • Asegurar la seguridad de puerto de escritura • Prioridad de POE de escritura • Monitoreo remoto (RMON) y sFlow (RFC 3176). • Debe permitir protocolos de TFTP y SFTP. • IP SLA for Voice.x • Debe permitir soporte de captura y lectura de SNMP de la base de información de administración (MIB) • Debe soportar Network Time Protocol (NTP) • De soportar IEEE 802.1AB Link Layer Discovery Protocol (LLDP). • Debe permitir velocidad de configuración de escritura y dúplex, • Permitir velocidades de transmisión de las tramas de salida por cola mediante Egress Queue Shaping (EQS) • capacidades de IPv6: • El host IPv6 permite que los conmutadores se administren en una red IPv6 • Transiciones de doble pila (IPv4 e IPv6) de IPv4 a IPv6, que admite conectividad para ambos protocolos • MLD snooping reenvía el tráfico de multidifusión IPv6 a la interfaz adecuada • IPv6 ACL/QoS admite ACL y QoS para el tráfico de red IPv6 • El enrutamiento IPV6 admite protocolos estáticos y OSPFv3 • La seguridad proporciona protección RA, bloqueo dinámico de IPv6 y espionaje ND • Alta disponibilidad • Debe permitir fuentes de alimentación redundantes e intercambiables en caliente. • Redundancia N+1 y N+N para una alta confiabilidad • Detección de enlace unidireccional (UDLD) • Protocolo de control de agregación de enlaces (LACP) IEEE 802.3ad • Debe ser compatible con el estándar IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocolo (RSTP) y IEEE 802.1s Multiple Spanning Tree Protocol (MSTP). • Protocolo de redundancia de enrutador virtual (VRRP) • Compatibilidad con PoE preestándar • Debe tener una capacidad de enrutamiento/conmutación de por lo menos 128Gbps • Como mínimo debe mantener una latencia de: • 1Gbps: 2.28 µSec • 10Gbps: 1.46 µSec • Debe soportar una capacidad de apilamiento hasta de ocho (08 miembros)

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

	• El consumo de energía debe ser de 59W a 230 VAC. • Rendimiento por encima de 95.2 Mpps.
3.6	**CONMUTACION DE CAPA 2**
3.6.1	• Soporte de VLAN y soporte etiquetado IEEE 802.1Q(4094 ID de VLAN) Y 2K VLAN´S simultaneas. • Debe ser compatible con paquetes JUMBO. • Debe admitir un tamaño de trama de hasta 9198 bytes. • Debe ser compatible con PVST+. • Debe contar con MVRP. • Soporte de protocolos BPDU • Debe soportar hasta 4 grupos de duplicación. • Protocolo de administración IGMP.
3.7	**SERVICIOS DE CAPA 3**
3.7.1	• Debe soportar protocolo ARP • Debe soportar protocolos DHCP y DHCP Relay
3.8	**ENRUTAMIENTO CAPA 3**
3.8.1	• OSPF /OSPFv2 para IPv4 • OSPF3 para IPv6 • Enrutamiento IP estático. • Personalización de parámetros TCP • Soporte de paquete de error ICPM • Amplias capacidades de visualización • Sistema de nombres de dominio de multidifusión mDNS (Multicast Domain Name System) • Multiples rutas de igual costo Equal-Cost Multipath (ECMP) • Open shortest path first (OSPF) • Routing Interior Gateway Protocol (IGP)
3.9	**SEGURIDAD**
3.9.1	• Criptografía validada FIPS 140-2 • Soporte de lista control de acceso Access control list (ACL) • Secure Sockets Layer (SSL) • Secure FTP • Security banner
3.10	**MULTICAST**
3.10.1	• Protocol Independent Multicast (PIM) • Multicast Listener Discovery (MLD) • Internet Group Management Protocol (IGMP) • Any-Source Multicast (ASM) • Compatibilidad con Qinq.
3.10.2	El oferente deberá certificar mediante carta emitida por el fabricante, que es canal autorizado para vender los productos ofertados.

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

3.11 REQUISITOS DE EMPAQUE Y ROTULADO

3.11.1 Empaque.

Todos los equipos deberán venir correctamente empacados de acuerdo a la normatividad vigente para equipos tecnológicos.

3.11.2 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.

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.

4.1.1 Muestreo.

Para verificar los requisitos generales, de empaque y rotulado se deben someter a evaluación todo el SISTEMA SWITCH CORE que se vaya a suministrar. Evaluando todos sus componentes.

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 indicados en los numerales 3.1 y 3.3.

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

4.2.1 Muestreo.

Para verificar los requisitos específicos se deben someter a evaluación todo el SISTEMA SWITCH CORE que se vaya a suministrar. Evaluando todos sus componentes.

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

El criterio para aceptar o rechazar el producto depende del cumplimiento de todos los requisitos indicados en el numeral 3.2 y las condiciones indicadas en el numeral 5. MÉTODOS DE ENSAYO.

5. MÉTODOS DE ENSAYO

El proveedor deberá hacer entrega total de los BIENES objeto de la presente especificación técnica en perfecto estado de funcionamiento, una vez realizadas y superadas a satisfacción del MDN-EJC las pruebas técnicas que resulten aplicables a cada uno de los equipos para la verificación de su idoneidad técnica y funcionalidad, en la unidad militar de acuerdo a la tabla de cantidades donde se estipula el sitio de instalación.

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 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 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.
- 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.
- 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.
- 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.

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

- 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 de delegación 4519 del 27 de mayo de 2016 ""Por la cual se delegan unas funciones y competencias relacionadas con la contratación de bienes y servicios con destino al Ministerio de Defensa Nacional, a las Fuerzas Militares y la Policía Nacional y se dictan otras disposiciones" y las demás normas que la modifiquen o aclaren.
- Resolución No. 4130 del 16 de junio de 2022 "MANUAL DE CONTRATACIÓN Y DE CONVENIOS" del Ministerio de Defensa Nacional y las demás normas que la modifiquen aclaren.
- Resolución 2710 del 03 de octubre de 2017 del Ministerio de Tecnologías de la Información y las Comunicaciones "Por la cual se establecen lineamientos para la adopción del protocolo IPv6" y las demás normas que la modifiquen o aclaren.
- Directiva de Seguridad de la Información del Ministerio de Defensa 2014-18 "Lineamiento de seguridad de la información para sector defensa" y las demás normas que la modifiquen o aclaren.
- Directiva permanente 00200 de 2017 "Lineamientos y políticas para la administración y operación de los recursos informáticos de tecnologías de la información y las comunicaciones TIC en el Ejército Nacional".

6.2 ANTECEDENTES

Omitido.

7. ANEXOS

Omitido

8. CONTROL DE REVISIONES

Revisión y/o Actualización	Modificaciones	Fecha
00	Creación de la especificación técnica corresponde a la solicitud No. 2023308006005133 MDN-COGFM-COEJC-SECEJ-JEMGF-COPER-DIPER-47.1 del comando de Personal del Ejército Nacional, de fecha 24 de marzo del 2023, con la cual se realizará la contratación para la adquisición de switch CORE en alta disponibilidad, en beneficio de la red de datos del edificio del Comando de Personal COPER" - La Dirección de Personal (DIPER) en la presente especificación técnica garantiza la pluralidad de oferentes.	01/06/2023

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

	- La Dirección de Personal (DIPER) en la presente especificación técnica garantiza los requisitos generales y específicos, los cuales fueron revisados técnicamente y satisfacen las necesidades del Ejército Nacional. - La Dirección de Personal (DIPER) la presente especificación técnica garantiza que fue elaborada de manera profesional, con la mayor transparencia, siempre buscando dejar en alto el nombre del Ejército Nacional.	
01	- Cambio de Nombre a la ET - Se actualiza el numeral de Aplicación - Modificación de requisitos específicos - División de la especificación por Ítems - Se Incluye Ítem 2 Adquisición de equipo switch Core Ejército nacional y sistema para monitoreo de las redes del Ejército nacional - para "NOC" del BAICC. - Se Incluye Ítem 3 adquisición de equipo switch L3 distribución a nivel nacional - Se actualiza numeración - Se actualiza normas que deben consultarse	04/08/2023
02	Se realiza modificación por cambio de versión, se realiza inclusión de requerimientos de cumplimiento técnico conforme con avances de la tecnología y las siguientes modificaciones, así: - Se realiza la siguiente modificación de todo el ítem 2 de acuerdo a estudio técnico realizado por el personal del BAICC soportado mediante oficio radicado No **2023575029362263.** - Se modifica la especificación técnica en el ítem No 2 cambiando en su totalidad el ítem actualizando la necesidad técnica en las especificaciones de los puertos de comunicación y requerimientos establecidos a nivel técnico para brindar la correcta operación de todos los servicios informáticos de la fuerza.	27/12/2023

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

	- Se elimina ítem 3.4.5 por estar duplicado, se corrige numeración - se elimina la palabra debe del Item 2 - se elimina "No se permite servicios relacionados al plano de control, enrutamiento y gestión de modo que se pueda". Por lo anterior, queda sin validez la especificación técnica versión 1 y a partir del momento rige la presente versión	
03	Se realizaron las siguientes modificaciones a la especificación técnica ADQUISICIÓN DE REDES DE DATOS Y EQUIPOS DE RED PARA UNIDADES MILITARES No. JEMPP-CEDE6-DIPCO-ET-01465/ COMUN-07. Así: Se actualiza la Especificación técnica en atención al oficio No. 2024575018950833 de fecha 24 de julio de 2024 Solicitud actualización especificación técnica 0562, Oficio No. 2024575018955153 de fecha 24 de julio de 2024 Estudio de Marcado Especificaciones Técnicas 05621, 2024575018963943 de fecha 24 de julio de 2024 Justificación modificación Especificaciones técnicas 05621, en cumplimiento a la circular 2023218004540933 del 09 de marzo y el boletín 030 del 17 de febrero de 2023 emitid o por JEMPP, acogiéndose al numeral 05. Del boletín 030 del 17 de febrero de 2023: Por mejora del documento técnico al ser revisado. Se modifica línea de mando de la especificación técnica de la siguiente manera JEMPP-CEDE6-DIPCO-ET-05621/COM-03. Se realizan las siguientes modificaciones en atención a que no afectan el contenido técnico, refiriéndose a la descripción de marca y lugar de entrega: • Se elimina ítem 3.4.1 por no ser especificación técnica. • Se elimina ítem 3.5.1 y 3.5.2 por no ser especificación técnica. • Se ajusta numeración del ítem 3.5 de la presente especificación técnica.	13/08/2024

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

	El Batallón de Interoperabilidad, cómputo y comunicaciones BAICC, en la presente especificación técnica garantiza la pluralidad de oferentes. - El Batallón de Interoperabilidad, cómputo y comunicaciones BAICC en la presente especificación técnica garantiza los requisitos generales y específicos, los cuales fueron revisados técnicamente y satisfacen las necesidades del Ejército Nacional. - El Batallón de Interoperabilidad, cómputo y comunicaciones BAICC técnica garantiza que la presente especificación fue elaborada de manera profesional, con la mayor transparencia, siempre buscando dejar en alto el nombre del Ejército Nacional. Por lo anterior, queda sin validez la especificación técnica versión 2 y a partir del momento rige la presente versión.	

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