ANEXO

ESPECIFICACIONES TECNICAS DE OBLIGATORIO CUMPLIMIENTO

Facatativá, XX de XXXXX de 2023

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

ESPECIFICACIONES TECNICAS DE OBLIGATORIO CUMPLIMIENTO

NORMAS O ESPECIFICACIONES TÉCNICAS, de acuerdo a plan de necesidades

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.
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 venderlos 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 nuevosy 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. 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
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 realizarbajo 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**
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
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 durantela 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, aceptary 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 osuministrarla 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 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.). El servicio será prestado en sitio en la ciudad de Bogotá de acuerdo a los tiempos de respuesta establecidos. . El tiempo máximo permitido para cambio de partes, repuestos o reparación del equipo es de 24 horas calendario una vez sea reportado el incidente.). Si después de 24 horas después de haber reportado el incidente y el contratistano 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.). 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).

	. En caso de cambio de equipos, repuestos o partes de contengan dispositivos o elementos de almacenamiento, estos serán destruidos o borrados de forma segurapor parte de la institución. . El contratista deberá suministrar, instalar, configurar y poner en perfecto funcionamiento los equipos, partes o repuestos garantizando la continuidad de los servicios.). 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. . 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.).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 cuandoasí se requiera.). 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 elsistema. 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 actividadespara 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**
3.3	**GENERALES**
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 manerasuministrara 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
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 - 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 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 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 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
	El Switch debe estar en la capacidad de administrar vía CLI otros Switch de la misma

3.3.1.18	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 máximoo sobre leds de los puertos mientras no se requieran, aunque tengan enlaces activos.
3.3.1.28	Capacidad de realizar scripting en CLI
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 10Gen 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 indicacionesque 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 OPTICA 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
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 BondingRequirements 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. 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 NACIONALY SISTEMA PARA MONITOREO DE LAS REDES DEL EJERCITO NACIONAL - PARA "NOC" DEL BAICC	

3.4	**SWITCH TIPO 1 EQUIPO DE CORE TIPO CHASSIS**	
3.41	El oferente deberá incluir la marca y referencia a ofertar en cada una de las tablas descritas a continuación	
	MARCA	
	REFERENCIA	
	URL DE DESCARGA FICHA TECNICA	
3.4.2	Tipo Modular	
3.4.3	Switch de capa 2, 3, 4.	
3.4.4	El equipo debe incluir al menos dos (2) bahías para módulos de administración. Los módulos de administración deben operar al menos en modo activo/pasivo.	
3.4.5	La solución debe incluir al menos 2 módulos de administración.	
3.4.6	El equipo debe incluir al menos cinco (5) bahías de ancho completo para módulos de Entrada/Salida (I/O).	
3.4.7	Incluir al menos: - 48 interfaces RJ45 1000Base-T POE+ Class 4 - 4 interfaces SFP56 Las interfaces incluidas deben ser todas no bloqueantes, se deben incluir los módulos SFP necesarios para su puesta en marcha	
3.4.8	Incluir al menos: - 24 interfaces RJ45 10GBase-T - 4 interfaces SFP56 Los interfaces incluidos deben ser todos no bloqueantes, se deben incluir los módulos SFP necesarios para su puesta en marcha	
3.4.9	Incluir al menos: - 48 interfaces 10G/25G SFP28 Los interfaces incluidos deben ser todos no bloqueantes, se deben incluir los módulos SFP necesarios para su puesta en marcha	
3.4.10	Incluir al menos: - 12 interfaces 40G/100G QSFP28 Los interfaces incluidos deben ser todos no bloqueantes, se deben incluir los módulos SFP necesarios para su puesta en marcha	
3.4.11	Una vez incluidos los interfaces solicitados, el equipo ofertado debe contar con al menos 01 bahías libres para crecimiento futuro.	
3.4.12	Cada bahía I/O debe soportar como mínimo un BW de conexión de 2.8 Tbps	
3.4.13	Capacidad de conectarse en stack con otro equipo igual ofreciendo las siguientes características: - La tecnología de stacking debe estar basada en Multi Chassis LAG (MC-LAG) Deben ser percibidos por los demás equipos como un único switch de modo que se pueda configurar agregación de puertos entre ellos - No deben compartir los servicios relacionados al plano de control, enrutamiento y gestión de modo que se pueda garantizar el alta disponibilidad ante la falla de un chasis y la actualización de software. - La configuración debe poder sincronizarse entre los miembros del stack - - Los miembros del stack deben operar en modo activo-activo tanto en L2 como enL3	

3.4.14	Incluir todo el hardware que requiera la conexión del stack para: - Al menos dos (2) enlaces de 100Gbps entre los equipos. - Longitud de los cables al menos de tres (3) metros
3.4.15	Al menos: - Throughput: 5.7 Bpps - Capacidad de conmutación: Al menos 14 Tbps.
3.4.16	Al menos: - RAM: 16 GB - Flash: 32 GB.
3.4.17	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.
3.4.18	Al menos - un (1) interfaz serial RJ45. - una (1) interfaz USB-C - un (1) interfaz Ethernet para administración fuera de banda. - un (1) puerto USB-A.
3.4.19	Al menos vía: - Línea serial de comandos (CLI) - Web - SSH v2 - REST API
3.4.20	Soporte de múltiples configuraciones almacenadas en la memoria flash. Capacidad de crear y almacenar de manera manual y automática la configuración a modo de checkpoints de modo que se pueda regresar de manera sencilla a una configuración anterior.
3.4.21	Al menos: - SNMP v1, v2c, v3 - RMON (events, alarm, history, and statistics group) - sFlow (RFC 3176)
3.4.22	Soporte al menos de: - IPv6 host - Dual Stack
3.4.23	Soporte de monitoreo de puertos de entrada y salida.
3.4.24	32000 direcciones MAC
3.4.14	Incluir todo el hardware que requiera la conexión del stack para: - Al menos dos (2) enlaces de 100Gbps entre los equipos. - Longitud de los cables al menos de tres (3) metros
3.4.15	Al menos: - Throughput: 5.7 Bpps - Capacidad de conmutación: Al menos 14 Tbps.
3.4.16	Al menos: - RAM: 16 GB - Flash: 32 GB.
3.4.17	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.

3.4.18	Al menos - un (1) interfaz serial RJ45. - una (1) interfaz USB-C - un (1) interfaz Ethernet para administración fuera de banda. - un (1) puerto USB-A.
3.4.19	Al menos vía: - Línea serial de comandos (CLI) - Web - SSH v2 - REST API
3.4.20	Soporte de múltiples configuraciones almacenadas en la memoria flash. Capacidad de crear y almacenar de manera manual y automática la configuración a modo de checkpoints de modo que se pueda regresar de manera sencilla a una configuración anterior.
3.4.21	Al menos: - SNMP v1, v2c, v3 - RMON (events, alarm, history, and statistics group) - sFlow (RFC 3176)
3.4.22	Soporte al menos de: - IPv6 host - Dual Stack
3.4.23	Soporte de monitoreo de puertos de entrada y salida.
3.4.24	32000 direcciones MAC
3.4.25	Al menos: - Soporte de 4094 VLAN ID.v - MVRP. - Mínimo 2000 Switched Virtual Interfaces (dual stack)
3.4.26	- VXLAN - GRE - Q-in-Q - BGP EVPN
3.4.27	Soporte de tramas de hasta 9198 bytes.
3.4.28	Al menos: - IEEE 802.1Q. - IEEE 802.1v. - IEEE 802.1w. - IEEE 802.1p. - IEEE 802.1X. - IEEE 802.3ad.
3.4.29	Listas de control de acceso (ACL) tanto para IPv4 e IPv6: - 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).
3.4.30	LACP IEEE 802.3ad: - Al menos 256 enlaces agregados c/u hasta con 8 puertos. - Soporte de grupos estáticos y dinámicos.
	Soporte de: - STP

3.4.31	- RSTP - MSTP - RPVST+ - STP Root guard - STP BPDU port protection
3.4.32	Soporte al menos de: - LLDP - LLDP-MED
3.4.33	Manejo de VLAN de voz.
3.4.34	Al menos: - IPv4 - IPv6
3.4.35	Al menos: - Rutas IPv4 unicast: 61000 - Rutas IPv6 unicast: 61000 - Rutas IPv4 multicast: 8000 - Rutas IPv6 multicast: 8000 - Tamaño de la tabla host (ARP): 49000 - Grupos IGMP: 8000 - Grupos MLD: 8000
3.4.36	Al menos: - Enrutamiento: estático. - Enrutamiento Inter-Vlan. - OSPFv2 - ECMP - BGP, BGP-4 - Policy-based routing
3.4.37	Al menos: - Enrutamiento: estático. - OSPFv3 - BGP, MP-BGP
3.4.38	Al menos: - Equal-Cost Multipath habilita multiples enlaces de igual costo para incrementar la redundancia y escalabilidad.
3.4.39	Al menos: - IGMP Snooping - IGMP v2/v3 (Internet Group Management Protocol) - MLD v1/v2 - PIM DM/SM
3.4.40	Soporte para asignar direccionamiento IP dinámico mediante protocolo DHCP Soporte de protección de DHCP de servidores no autorizados
3.4.41	- VRRP - VRF (256 VRFs) - Policy Base Routing
3.4.42	- Al menos 8 colas por puerto. - VOQ (Virtual Output Queuing) para aislar la congestión, prevenir HOLB y proveerfull line rate hacia hacia los puertos de egreso.
	Soporte de: - Flow Control 802.3x - COS mapping

3.4.43	- DSCP local-priority mapping - Strict priority queuing (SP) - DWRR Deficit Weighted Round Robin - Egress queue shaping - Asignación del tag 802.1p basada en dirección IP, IP ToS, protocolo de capa 3, puerto TCP/UDP, DiffServ
3.4.44	Soporte de: - Autenticación por dirección MAC - RADIUS - TACACS+ - Autenticación basada en WEB.
3.4.45	- Protección de broadcast de ARP - Dynamic IP Lockdown que ayuda a prevenir el IP Source Address Spoofing - MAC Address lockout para prevenir la conexión de MAC particulares - Capacidad de configurar políticas en el plano de control de modo que se pueda limitar los flujos por protocolos hacia el CPU impidiendo ataques DOS. - DHCP protection - ICMP throttling para evitar ataques DOS ICMP - ACLs basadas en identidad de los usuarios, para facilitar la integración con sistemas de Control de Acceso a la red (NAC) - IGMP y MLD snooping - ND Snooping - UDLD - RadSec
3.4.46	Tunelización de tráfico hacia un gateway para aplicar las mismas políticas de autenticación, acceso y seguridad que en la red inalámbrica simplificando la configuración a nivel de la infraestructura LAN
3.4.47	- Motor que automáticamente monitorea y analiza eventos que pueden impactar enla salud de la red. Este debe estar ubicado en el mismo switch para hacer análisis y monitoreo de eventos de manera distribuida. - Telemetría avanzada que permite identificar y resolver de manera sencilla problemas relacionados a la red, sistemas, seguridad y aplicación a través de agentes Python y REST APIs.
3.4.48	Capacidad de poder enviar los parámetros de red iniciales al switch vía bluetooth utilizando una app móvil. Una vez hecho esto la configuración final es obtenida vía un gestor centralizado.
3.4.49	Capacidad de monitorear la calidad del tráfico de voz utilizando pruebas UDP jitter y UDP jitter for VoIP
3.4.50	Debe traer todos los accesorios para montaje y operación en rack estándar de 19".
3.4.51	Máximo 7 RUs (unidades de rack).
3.4.52	Soporte: - 110-127 VAC a 200-240 VAC - 50 Hz a 60 Hz. - Certificación Platino 80plus.org
3.4.53	- El equipo debe soportar de fuentes de poder redundante, con característica de instalación en caliente (hot-swap). - Redundancia N+1 y N+N

3.4.54	Incluir: - Fuentes de poder AC. - El Equipo debe venir con todas las fuentes de poder disponibles en su máxima capacidad.
3.4.55	- Energy Efficient Ethernet IEEE 802.3az para las interfaces Ethernet.
3.4.56	EN62368-1:2014 UL 60950-1, CSA 22.2 No 60950- 1IEC 62368-1 Ed. 2
3.4.57	EN 55022 Class A; CISPR 22 Class A; IEC/EN 61000-3-2 IEC/EN 61000-3-3; ICES-003 Class A; FCC (CFR 47, Part 15) Class A; GB9254EN55032:2012 Class A CISPR32:2012 Class A
3.4.58	Garantía limitada de por vida que incluya al menos: Reemplazo de hardware y actualizaciones de software de por vida, creación ilimitada de casos de servicio.
3.4.59	Servicios de reposición de partes y piezas (Hardware): - Duración: al menos 01 años. - Nivel: 24x7 con 4 horas de despacho una vez confirmado el daño / NBD - Soporte en sitio / Soporte telefónico - Servicio de solución de problemas de HW a las 6 horas de llamada.
3.4.60	Servicios de actualización del sistema operativo y atención a casos: - Duración: al menos 01 años. - Nivel: 24x7 / 9x5
3.4.61	Para garantizar la protección de inversión, alineación con las tendencias tecnológicas de la industria, soporte y vigencia tecnológica y estar preparados para los requerimientos futuros, los equipos de comunicación ofertados para el presente ítem, deben corresponder a una marca o fabricante que figure dentro de los líderes en el Cuadrante Mágico de Gartner para soluciones de acceso LAN Wired and Wireless durante los últimos tres años (2020, 2021 y 2022) y para su acreditación deberá presentar el informe correspondiente a cada año.

ITEM No.3. ADQUISICIÓN DE EQUIPO SWITCH L3 DE DISTRIBUCION PARA REDES LAN A NIVEL NACIONAL		
No. 3.5	**REQUERIMIENTOS GENERALES**	
3.5.1	El oferente deberá incluir la marca y referencia a ofertar en cada una de las tablas descritas a continuación	
	MARCA	
	REFERENCIA	
	URL DE DESCARGA FICHATECNICA	
3.5.2	El sistema debe contemplar el suministro de equipos tipo switch de distribución, en el almacén de telemática COMOL 1 centro de costo 3578004052 ubicado en la calle103A # 11b - 00 Barrio Chico Usaquén Bogotá D.C.	
3.5.3	La solución debe cumplir con al menos las siguientes características técnicas paralos dispositivos:	

3.5.4	Seguridad mediante el uso de agentes Phyton y API Rest. Interfaz Api Rest programable. Memoria QuadCore Arm Cortex A72 a 1,8 GHz Fuente de alimentación fija. 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 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 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) 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) El consumo de energía debe ser de 59W a 230 VAC. Rendimiento por encima de 95.2 Mpps.
3.6	**CONMUTACION DE CAPA 2**
	Soporte de VLAN y soporte etiquetado IEEE 802.1Q(4094 ID de VLAN) Y 2K VLAN´S simultaneas. • Debe ser compatible con paquetes JUMBO.

3.6.1	• 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.

CONCIDERACIONES TECNICAS ADICIONALES

El oferente deberá adjuntar a la oferta el cuadro de marcas y modelos a ofertar donde deberá indicar la información que se relaciona a continuación:

	DESCRIPCIÓN DEL ELEMENTO O BIEN	MARCA	REFERENCIA

1	SISTEMA SWITCH DE CORE CAPA 3 DE ACUERDO A ESPECIFICACIONES TECNICAS ET- 05621 EQUIPOS PARA REDES DE DATOS COM-01		
2	TARJETA 12 PUERTOS RJ45 1G/2.5G/5G/10G Base-T PARA SWITRCH CORE DE ACUERDO A ESPECIFICACIONES TECNICAS ET- 05621 EQUIPOS PARA REDES DE DATOS COM-01		
3	PATCH CORD DE FIBRA OPTICA DE ACUERDO A ESPECIFICACIONES TECNICAS ET-05621 EQUIPOS PARA REDES DE DATOS COM-01		
4	FUENTES DE PODER DE ACUERDO A ESPECIFICACIONES TECNICAS ET-05621 EQUIPOS PARA REDES DE DATOS COM-01		
Item No.	**DESCRIPCIÓN DEL ELEMENTO O BIEN**	**MARCA**	**REFERENCIA**
5	SWITCH TIPO 1 (SWITCH DE ACCESO)		
6	SWITCH TIPO 2 (SWITCH DE CORE)		
7	BANDEJAS PARA FIBRA OPTICA		
8	FIBRA OPTICA MULTIMODO OM4		
9	CABLE UTP CAT 6A		
Item No.	**DESCRIPCIÓN DEL ELEMENTO O BIEN**	**MARCA**	**REFERENCIA**
10	SWITCH 24 10/100/1000T, 4 x 1G SFP - JEMPP-CEDE6-DIPCO-ET-05621/COM-1		

PERSONAL TECNICO REQUEERIDO PARA LA EJECUCION DEL PROYECTO LOTE 1 DIPER

	PERSONAL REQUERIDO.
	El siguiente personal dará cumplimiento y llevará a cabo la ejecución de las actividades para la totalidad de los ítems objeto de este proceso, en todas sus especificaciones técnicas (Todas las sedes) UN (1) GERENTE PROYECTO El oferente deberá adjuntar a la oferta la hoja de vida de un profesional quien se desempeñará como gerente de proyecto y liderará los aspectos relacionados con la ejecución del contrato para coordinar las actividades con el personal asignado por el contratista. Debe ser Ingeniero Sistemas o Electrónico o Telecomunicaciones, Especialista en gerencia integral de proyectos y PMP y/o SCRUM y/o itil v3 o posterior, vigentes. Con mínimo 5 años de experiencia a partir de la expedición de la tarjeta profesional, debe contar con mínimo 2 años de experiencia en instalación de equipos activos switch, debe tener certificación de entrenamiento en diseño de redes de las marcas Allied Telesis o Cisco o Extreme Networks o Aruba. **EQUIPO TECNICO DE INSTALACION:** El oferente deberá adjuntar a la oferta hoja de vida de dos (2) personas que cumplan con el perfil técnico, tecnólogo o ingeniero de sistemas - electrónico – eléctrico - telecomunicaciones o afines de

	acuerdo a SNIES, idóneo en la instalación, configuración, pruebas y puesta en funcionamiento del sistema requerido en la presente especificación técnica, por lo anterior el oferente deberá adjuntar junto con la hoja de vida del personal, los certificados que correspondan a la instalación de cada sistema así: • Certificado de entrenamiento nivel experto en configuración de equipos activos o diseño de redes, de las marcas Allied Telesis o Cisco o Extreme Networks o Aruba. • Certificado en direccionamiento IP (IPV4 O IPV6) para que realice la configuración necesaria en los equipos activos. • Certificación en infraestructura de telecomunicaciones Deberá anexar como mínimo, dos (02), certificaciones de experiencia en instalación y configuración de equipos activos switch Core. El oferente deberá certificar que los profesionales de instalación hacen parte del equipo de ingeniería u operaciones de la compañía.

Nota: Los oferentes deberán diligenciar en su totalidad el cuadro de marcas y referencias, sin dejar espacio alguno, ni tachones o enmendaduras, con la finalidad de que el comité evaluador pueda comparar los cumplimientos técnicos de la solución requerida vs la solución ofertada.

EL OFERENTE _____
REPRESENTANTE LEGAL O APODERADO
Nombre
Identificación
Razón Social
C.C. / Nit. Nº XXXXXXX