COMANDO CONJUNTO DE LAS FF.AA.

DIRECTOR ADMINISTRATIVO FINANCIERO

INFORME DE ACTA ENTREGA-RECEPCIÓN

GRUSICOMGE-S-2023-0023-O

Quito D.M, 15 de febrero del 2023

PARA: Coronel de E.M.C. Carlos Jacinto Ampudia Gallardo
COMANDANTE DEL GRUPO DE SISTEMAS INFORMÁTICOS, COMUNICACIONES Y GUERRA ELECTRÓNICA CONJUNTO

ASUNTO: Informe Acta Entrega Recepción sobre el proceso de "La adquisición de infraestructura tecnológica e instalación del cableado estructurado del Comando Conjunto de las Fuerzas Armadas".

En la ciudad de Quito, a los 15 días del mes de febrero de 2023, en el Departamento de Sistemas Informáticos, comparece los señores: Capt. Téc. Avc. Muñoz Sánchez Fabricio Administrador del Contrato, Cbos. Téc. Avc. Garces Velastegui Dario, delegado técnico de recepción, Sgos-IF. Buila Rosero Silvia, técnico no interviniente**,** con el objeto de proceder a la entrega – recepción del PROCESO DE CONTRATO Nro. SIE-CCFFAA-021-2022 POR LA "ADQUISICIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA E INSTALACIÓN DEL CABLEADO ESTRUCTURADO DEL COMANDO CONJUNTO DE LAS FUERZAS ARMADAS".

PRIMERA: ANTECEDENTES

a) Que el artículo 51 de la Ley Orgánica del Sistema Nacional de Contratación Pública, respecto de la modalidad de adquisición bajo menor cuantía determina: "Se podrá contratar bajo este sistema en cualquiera de los siguientes casos: 1. Las contrataciones de bienes y servicios no normalizados, exceptuando los de consultoría cuyo presupuesto referencial sea inferior al 0,000002 del Presupuesto Inicial del Estado del correspondiente ejercicio económico; 2. Las contrataciones de obras, cuyo presupuesto referencial sea inferior al 0,000007 del Presupuesto Inicial del Estado del correspondiente ejercicio económico; 3. Si fuera imposible aplicar los procedimientos dinámicos previstos en el Capítulo II de este Título o, en el caso que una vez aplicados dichos procedimientos, éstos hubiesen sido declarados desiertos; siempre que el presupuesto referencial sea inferior al 0,000002 del Presupuesto Inicial del Estado del correspondiente ejercicio económico.".
b) En el artículo 139 del Reglamento General de la Ley Orgánica del Sistema Nacional de Contratación Pública, determina: "Procedimiento.-Para las contrataciones previstas en los números 1 y 3 del artículo 51 de la Ley Orgánica del Sistema Nacional de Contratación Pública, la entidad contratante convocará exclusivamente a los proveedores que sean micro o pequeñas empresas, artesanos o actores de la economía popular y solidaria, domiciliados en la circunscripción territorial en que se ejecutará el contrato; y que estén interesados en participar. Posteriormente, se realizarán las etapas de preguntas, respuestas y aclaraciones, presentación y apertura de ofertas,

y convalidación de errores de corresponder. Los proveedores invitados y habilitados que estén en condiciones de suministrar el bien o prestar el servicio, presentarán sus manifestaciones de interés a través del Portal COMPRASPÚBLICAS, en las cuales podrán mejorar las condiciones técnicas o económicas definidas por la entidad contratante, sin afectar la calidad del bien o servicio ofertado con observancia de los principios que rigen la contratación pública."

c) Mediante informe de necesidad Nro. No. GRUSICOMGE-S-2022-0080-O de fecha 11 de agosto de 2022, elaborado por el señor Mayo. Téc. Avc. Roberto Ayala, Jefe Dpto. Sistemas Informáticos del Grusicomge, en el cual se señala la necesidad para realizar la adquisición de infraestructura tecnológica e instalación del cableado estructurado del Comando Conjunto de las Fuerzas Armadas
d) Luego del proceso correspondiente, el delegado de la máxima autoridad del CC.FF.AA., mediante Resolución de Adjudicación Nro. SIE-CCFFAA-021-2022, de fecha 21 de septiembre del 2022, adjudico la ADQUISICIÓN DE EQUIPOS SISTEMA Y PAQUETES INFORMÁTICOS, al señor Carlos Enrique Romero Racines, representante legal de la compañía CONSTECOIN CIA. LTDA con RUC: 1708326242.
e) Con fecha 03 de octubre de 2022, se suscribió el contrato Nro. SIE-CCFFAA-021-2022, para "La adquisición de infraestructura tecnológica e instalación del cableado estructurado del Comando Conjunto de las Fuerzas Armadas".
f) Con oficio Nro. OFIC-350-2022 de fecha 02 de diciembre del 2022 la compañía CONSTECOIN CIA. LTDA solicita el cambio de los rack de 42u a 45u.
g) Con oficio Nro. OFIC-352-2022 de fecha 07 de diciembre del 2022 la compañía CONSTECOIN CIA. LTDA, solicita se otorgue una prorroga al contrato Nro. SIE-CCFFAA-021-2022, justificando motivos de fuerza mayor.
h) Con oficio Nro. CCFFAA-GRUSICOMGE-2022-8212-O de fecha 08 de diciembre del 2022 se autoriza la prórroga solicitada con oficio Nro. OFIC-352-2022.
i) Con oficio Nro.CCFFAA-DAJ-2022-8108-O de fecha 22 de diciembre del 2022 la dirección de asesoría jurídica del COMACO autoriza lo solicitado con oficio Nro. OFIC-350-2022 por parte de la compañía CONSTECOIN CIA. LTDA.
j) Con oficio Nro. OFIC-017-2023 del 08 de febrero del 2023 del 2023, la compañía CONSTECOIN CIA. LTDA, solicita se autorice el cambio de 12 cables SFP28 a SPF28, 25Gbps, de al menos 2 metros por 12 cables QSFP28 a SPF28, 100Gbps, de al menos 10 metros.
k) Con oficio Nro. CCFFAA-DAJ-2023-0085-O de fecha 15 de diciembre del 2023 la dirección de asesoría jurídica se autoriza el cabio de cables solicitado con oficio Nro. OFIC-017-2023 del 08 de febrero del 2023, en vista que se justifica una mejora tecnológica al proceso.
l) Se procedió a la recepción de los bienes mediante acta entrega recepción de fecha 14 de febrero del 2023, misma se suscribió a entera conformidad y en concordancia con el artículo 319 del RGLOSNCP.

SEGUNDA: CONDICIONES GENERALES DE EJECUCIÓN

La ejecución del contrato contemplo los siguientes productos y servicios con el consiguiente estado de cumplimiento.

ORD.	BIENES A ADQUIRIR	ESPECIFICACIONES TÉCNICAS	CONDICIONES DE USO	CANT	UNIDAD DE MEDIDA	CUMPLIMIENTO
1	Unidad de almacenamiento para ampliación cache para Nodos E560	*Se requiere que los discos sean totalmente compatibles con los nodos VxRail E560 que se encuentran en producción y se requiere incluir cualquier licenciamiento o software adicional que sea necesario para la ampliación. Se instalará al menos 1 en cada nodo. *Se requiere de al menos 800GB SSD SAS. *Se requiere que sea de uso mixto, al menos 12Gbps, 2.5''. **DEBE INCLUIR EN LA INSTALACION** *Instalación controlada de los nuevos discos durosde Cache en cada Nodo E560 *Instalación controlada de los nuevos discos duros de Almacenamiento en cada Nodo E560 *Instalación controlada de las tarjetas de red con conexión a 25Gbps tanto en los nodos E560 comoen el equipo S570	Van hacer utilizados para ampliar la capacidad de almacenamiento cache en los Nodos.	3	UNIDAD	CONFORME
2	Unidad de almacenamiento para ampliación de almacenamiento para Nodos E560	*Se requiere que los discos sean totalmente compatibles con los nodos VxRail E560 que se encuentran en producción y se requiere incluir cualquier licenciamiento o software adicional que sea necesario para la ampliación Se instalarán al menos 4 en cada nodo. *Se requiere de al menos 2.4 TB de 10K rpm SAS *Se requiere que sea compatible con almenos12Gbps y de 2.5'' **DEBE INCLUIR EN LA INSTALACION** *Instalación controlada de los nuevos discos durosde Cache en cada Nodo E560 *Instalación controlada de los nuevos discos duros de Almacenamiento en cada Nodo E560 *Instalación controlada de las tarjetas de red con conexión a 25Gbps tanto en los nodos E560 comoen el equipo S570	Van hacer utilizados para ampliar la capacidad de almacenamiento en los Nodos hiperconvergetes.	12	UNIDAD	CONFORME
3	Tarjeta de red para la actualización de conectividad para Nodos 560	Se requiere que la tarjeta de red incluya al menos dos (2) slots compatibles con módulos SFP28 de 25Gbps. **DEBE INCLUIR EN LA INSTALACION** *Instalación controlada de los nuevos discos durosde Cache en cada Nodo E560 *Instalación controlada de los nuevos discos durosde Almacenamiento en cada Nodo E560 *Instalación controlada de las tarjetas de red con conexión a 25Gbps tanto en los nodos E560 comoen el equipo S570	Las tarjetas de Red se requieren que sean totalmente compatibles con los nodosVxRail E560 que se encuentran en producción y se requiere incluir cualquier licenciamiento o software adicional que sea necesario para la ampliación Se instalará al menos 1 en cada nodo.	3	UNIDAD	CONFORME

4	Tarjeta de red para la actualización de conectividad para Nodos E570	*Se requiere que la tarjeta de red incluya al menosdos (2) slots compatibles con módulos SFP28 de almenos 25Gbps. **DEBE INCLUIR EN LA INSTALACION** *Instalación controlada de los nuevos discos durosde Cache en cada Nodo E560 *Instalación controlada de los nuevos discos duros de Almacenamiento en cada Nodo E560 *Instalación controlada de las tarjetas de red con conexión a 25Gbps tanto en los nodos E560 comoen el equipo S570	Las tarjetas de Red se requieren que sean totalmente compatibles con los nodosVxRail E570 que se encuentran en producción y se requiere incluir cualquier licenciamiento o software adicional quesea necesario para la ampliación Se instalara al menos 1 en cada nodo.	1	UNIDAD	
5	Equipo Nodo hiperconvergente	Cantidad: 1 (Uno) Se requiere que el Nodo ofertado sea configurado como parte del Cluster hiperconvergente que se dispone. Se requiere que los Nodos HIPERCONVERGENTES sean alojados en rack estándar de al menos 19 pulgadas. Se requiere que el Sistema HIPERCONVERGENTE tenga una escalabilidadde al menos 64 Nodos Se requiere que cada nodo cuente como mínimo con los siguientes puertos de red: •Al menos 2 slots que soporten módulos SFP+/SFP28 de al menos 10 y 25Gbps Ethernet •Al menos 1 puerto de al menos 100Mb Ethernet –Gestión Se requiere que cada nodo cuente al menos con la siguiente capacidad de cómputo: •Sockets: 1 de al menos 2.1GHz •Cores: mínimo 20 Cores •RAM: mínimo 384 GB •Tipo de procesador: Intel Xeon 5218R Se requiere que cada nodo cuente al menos conla siguiente capacidad de almacenamiento: •Cache: Al menos 2 x 800GB SSD 3.5” •Almacenamiento: Al menos 8 x 4TB 7.2K rpm 3.5” *El Sistema HIPERCONVERGENTE hará referencia a los siguientes subcomponentes: •Nodos HIPERCONVERGENTES •Virtualización Cómputo •Virtualización Almacenamiento •Sistema de Gestión. *Se requiere que el fabricante virtualizador del Sistema Hiperconvergente esté ubicado en el cuadrante de líderes, en el Cuadrante Mágico de Gartner para Software de infraestructura hiperconvergente disponible a la fecha de publicación del proceso. *Se requiere que el soporte del Sistema HIPERCONVERGENTE sea entregado en forma unificada: hardware de los Nodos, virtualización de cómputo, virtualización de almacenamiento y sistemas de gestión a través de un servicio de soporte integral y unificado. *Se requiere que el producto sea certificado e integrado por el fabricante como Sistema HIPERCONVERGENTE en todos sus componentes: Nodos HIPERCONVERGENTES, Virtualización Cómputo, Virtualización Almacenamiento y Sistema de Gestión están constituidos como un solo producto. *El software completo del Sistema HIPERCONVERGENTE, será de Virtualización Cómputo, Virtualización Almacenamiento ySistema de Gestión; y se requiere que venga cargado íntegramente desde el fabricante del	Va alojar los diferentes servidores virtuales con los sistemas y Servicios que brinda elComando Conjunto de las FuerzasArmadas.	1	UNIDAD	CONFORME

		sistema. *Se requiere que los componentes ofertados sean nuevos de fábrica, no re-manufacturados, ni reparados, ni reacondicionados en ninguna de suspartes. *Se requiere que las actualizaciones de software, firmware, parches/fixes sean certificadas y entregadas por el fabricante en forma integrada y considerando todos los componentes Virtualización Cómputo, Virtualización Almacenamiento ySistema de Gestión. Se requiere que el fabricante entregue periódicamente los detalles de parches soportados y su procedimiento de aplicación. *Se requiere que el fabricante ofrezca y certifique un esquema de atención directa de llamadas y problemas que se requiere ser provisto desde un centro de soporte unificado, desde donde deberán asistirse todos los problemas asociados a los componentes de red, computo, almacenamiento y virtualización, durante el tiempo que dure la garantía en la modalidad 7 x 24 x 365 con un tiempode respuesta en sitio de al menos 4 horas para solventar inconvenientes. *Se requiere que el contratista realice un mantenimiento preventivo semestral de la soluciónimplementada, mientras dure la garantía técnica *Se requiere que la infraestructura HIPERCONVERGENTE incluya todo el licenciamiento e instalación del software hipervisorque permita el cumplimiento de todo lo requerido. *Se requiere que el sistema cuente con una aplicación de soporte que reporte el estado del equipo al fabricante en forma automática. *Se requiere garantía técnica del fabricante por al menos 3 años. *Se requiere que el SistemaHIPERCONVERGENTE incluya y venga pre- cargado de fábrica con el Hipervisor, de modo de minimizar los tiempos de puesta en marcha además se requiere que sea 100% compatible conla actual plataforma de virtualización existente (VMWARE). *Se requiere que el fabricante del Sistema HIPERCONVERGENTE provea el soporte integrado de la capa de virtualización de cómputo (nivel 1, 2 y 3) *Se requiere que el hipervisor del sistema HIPERCONVERGENTE este ubicado en el cuadrante de líderes, en el Cuadrante Mágico de Gartner de Virtualización de servidores x86 disponible a la fecha de publicación del proceso. *Se requiere que el hipervisor incluya switches virtuales distribuidos a fin de manejar las configuraciones de éstos como una sola entidad *Se requiere que el hipervisor tenga una funcionalidad de registro o Log integrada a fin de proveer una visión de los eventos de hardware y software *Se requiere que el hipervisor disponga de funcionalidades de alta disponibilidad automática, distribución automática de recursos y migración dealmacenamiento en caliente. *Se requiere que la solución permita entregar estadísticas completas sobre las máquinasvirtuales, como consumos de CPU, RAM y Almacenamiento, así como los IOPs de lectura/escritura y latencias. *Se requiere garantía técnica del fabricante por al menos 3 años. *Se requiere que el sistema hiperconvergente incluya un software integrado de virtualización de almacenamiento *Se requiere que el fabricante del Sistema HIPERCONVERGENTE provea el soporteintegrado de la capa de virtualización de almacenamiento *Se requiere que la capa de virtualización de almacenamiento corra en el mismo Kernel del hipervisor a fin de optimizar el uso de los recursos y asegurar el performance *Se requiere que el sistema de virtualización de almacenamiento provea recursos de bloques a sistemas fuera del Sistema HIPERCONVERGENTE a través de protocolos estándares como iSCSI *Se requiere que la administración de la virtualización de almacenamiento este integrada a la administración de servidores virtuales y no ser una consola independiente				

		*Se requiere que el sistema de almacenamiento semaneje como políticas, características como: •Desempeño •Nivel de protección •Calidad de Servicio Estas características deben tener la granularidad de disco virtual. *Se requiere garantía técnica del fabricante por al menos 3 años. *Se requiere que el Sistema HIPERCONVERGENTE ofertado soporte lossiguientes servicios de almacenamiento: -Replicación -Back up *Se requiere que estas aplicaciones de servicios de almacenamientos estén pre-cargadas de fábrica o ser instaladas a través de un portal integrado. *Se requiere que el fabricante del Sistema HIPERCONVERGENTE provea el soporte integrado de estas aplicaciones de servicios de almacenamiento, mientras dure la garantía técnicade la solución. *Se requiere que el SistemaHIPERCONVERGENTE soporte la funcionalidadde replicación de máquinas virtuales a un sistema externo, basado en el mismo hipervisor. El sistema externo podrá ser un Sistema HIPERCONVERGENTE o no, del mismo fabricanteo de un tercero *Se requiere que la replicación permita replicación con RPO = 0 (es decir replicación sincrónica) *Se requiere que las funciones de administración de cómputo y almacenamiento virtualizado sean integradas en una sola consola *Se requiere una consola integrada tipo GUI para realizar funciones de gestión. Al menos debe contar con las siguientes: •Aprovisionamiento de nodos nuevos •Actualización de parches de software del sistema •Visualizar la utilización de los recursos •Visualizar el estado de salud del sistema *Se requiere que se provea de capacidad de monitoreo remoto para diagnóstico y reparación. *Se requiere que el nuevo nodo herede o iguale el tiempo de soporte del sistema actual de hiperconvergencia con el que cuenta la Institución. *Se requiere se incluya el licenciamiento de gestiónde nube privada que actualmente existe en la institución VMware vRealize Suite Enterprise. *Se requiere que incluya el licenciamiento de la herramienta de backup que actualmente existe en la institución Veeam Backup and Replication Enterprise Plus. **DEBE INCLUIR EN LA INSTALACION DE LA AMPLIACION DE LA INFRAESTRUCTURA HCI** *Rackeo de los equipos *Conectorización de equipo al nuevo fabrica. *Energización de los equipos *Proceso de configuración inicial del equipo. *Configuración de direcciones IP de administracióny de front-end de la solución *Configuración de parámetros de red e integracióna nivel IP con la infraestructura de comunicaciones. *Creación de volúmenes que serán presentados alvSphere *Configuración del Hypervisor VMware *Revisión del estado de salud de la infraestructura *Pruebas de acceso a la plataforma hyperconvergente *Integración con la solución de respaldoexistente/ofertada *Configuración de la comunidad SNMP requeridapor el cliente.				
6	Equipos Switch de acceso	*Se requiere incluir mínimo 48 interfaces de almenos 1Gbps RJ-45 *Se requiere incluir mínimo 4 interfaces que soporten módulos de al menos 10 Gbps *Se requiere que cada equipo incluya mínimo 2 módulos transceivers SFP+ para conexiones de almenos 10Gbps del tipo SR (corta distancia), de al menos 42 en total *Se requiere que sea de mínimo de 24 interfaces PoE (802.3 af/at)	Los switch de acceso permitirán realizar la conexión entreel switch decore con losswitchs de pisoy a su	21	UNIDAD	CONFORME

		*Se requiere mínimo 370 Watts de capacidad de distribución de PoE (Budget) *Se requiere tener al menos una interfaz de consola RJ-45 *Se requiere factor de forma del tipo de al menos 1 RU *Se requiere capacidad de switching de al menos176 Gbps *Se requiere que soporte al menos 250 Mpps *Se requiere que la MAC address storage seamínimo de 32K *Se requiere que la latencia sea máxima de 1 µs *Se requiere que soporte Link Aggregation con almenos hasta 8 elementos *Se requiere Soportar al menos 16 LinkAggregation Groups *Se requiere Packet buffers de al menos 2 MB *Se requiere memoria DRAM de al menos 512 MB *Se requiere flash de al menos 64 MB *Se requiere MTBF superior al menos 10 años *Se requiere que la temperatura de operación seencuentre en al menos en el rango 5-45 ºC *Se requiere que acepte actualizaciones defirmware *Se requiere que soporte administración en la nube *Se requiere que soporte la administracióncentralizada como parte de un fabric *Se requiere que soporte administración por IPv4e IPv6 *Se requiere que soporte Telnet / SSH para acceso a la consola *Se requiere que soporte HTTP / HTTPS *Se requiere que soporte SNMP v1/v2c/v3 *Se requiere que se pueda configurar su relojmediante un SNTP Server *Se requiere contar con una línea de comandosestándar y una interfaz Web de configuración *Se requiere que soporte actualizaciones de Software por: TFTP/FTP/GUI. *Se requiere que soporte HTTP REST APIs para configuración y monitoreo *Se requiere soporte Link Aggregation estático *Se requiere soporte LACP *Se requiere soporte Spanning Tree *Se requiere soporte Jumbo Frames *Se requiere soporter Auto-negociacion para lavelocidad de los puertos y duplicidad *Se requiere soporte el estándar IEEE 802.1DMAC Bridging/STP *Se requiere soporte el estándar IEEE 802.1wRapid Spanning Tree Protocol (RSTP) *Se requiere soporte el estándar IEEE 802.1sMultiple Spanning Tree Protocol (MSTP) *Se requiere soporte la funcionalidad STP RootGuard *Se requiere soporte STP BPDU Guard *Se requiere soporte Edge Port / Port Fast o quivalente. *Se requiere soporte el estándar IEEE 802.1QVLAN Tagging *Se requiere soporte el estándar IEEE 802.3ad Link Aggregation con LACP *Se requiere que pueda balancear tráfico Unicast/Multicast sobre un puerto trunk (dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac) *Se requiere que soporte el estándar IEEE 802.1AX Link Aggregation *Se requiere que soporte instancias de Spanning Tree (MSTP/CST) *Se requiere que soporte el estándar IEEE 802.3xFlow Control con Back-pressure *Se requiere que soporte el estándar IEEE 802.310Base-T *Se requiere que soporte el estándar IEEE 802.3u100Base-TX *Se requiere que soporte el estándar IEEE 802.3z 1000Base-SX/LX *Se requiere que soporte el estándar IEEE 802.3ab 1000Base-T *Se requiere que soporte el estándar IEEE 802.3ae10 Gigabit Ethernet *Se requiere que soporte el estándar IEEE 802.3az Energy Efficient Ethernet *Se requiere que soporte el estándar IEEE 802.3 CSMA/CD como método de acceso y las especificaciones de la capa	vezestos con el patch panel para posterior conexión con cada computador, mismos deberán estar configurados para que su comportamiento sea en capa2			

		física *Se requiere que cuente con la funcionalidad de Control de Tormentas (Storm Control) *Se requiere que soporte la creación de VLANs porMAC, IP y Ethertype-based *Se requiere que soporte emergency location identifier numbers (ELINs) o similar en LLDP-MED *Se requiere que permita limitar la cantidad deMACs aprendidas por puerto *Se requiere que permita un mínimo de 16instancias de MSTP *Se requiere que permita controlar tormentas debroadcast independientemente en cada puerto *Se requiere que soporte un mecanismo dedetección y prevención de loops *Se requiere que soporte el RFC 2571 Architecturefor Describing SNMP *Se requiere que soporte el RFC 2865 RADIUS *Se requiere que soporte el RFC 1643 Ethernet-like Interface MIB *Se requiere que soporte el RFC 1213 MIB-II. *Se requiere que soporte el RFC 1354 IP Forwarding Table MIB *Se requiere que soporte el RFC 2572 SNMPMessage Processing and Dispatching *Se requiere que soporte el RFC 1573 SNMP MIBII *Se requiere que soporte el RFC 1157 SNMPv1/v2c *Se requiere que soporte el RFC 2030 SNTP *Se requiere que soporte el Port Mirroring *Se requiere que soporte Admin Authentication víaRFC 2865 RADIUS *Se requiere que soporte el estándar IEEE 802.1x authentication Port-based *Se requiere que soporte el estándar IEEE 802.1x Authentication MAC-based *Se requiere que soporte el estándar IEEE 802.1xGuest and Fallback VLAN *Se requiere que soporte el estándar IEEE 802.1xMAC Access Bypass (MAB) *Se requiere que soporte el estándar IEEE 802.1xDynamic VLAN assignment *Se requiere que soporte el estándar IEEE 802.1abLink Layer Discovery Protocol (LLDP) *Se requiere que soporte el estándar IEEE 802.1abLLDP-MED *Se requiere que soporte DHCP Snooping. *Se requiere que el servicio de soporte de fábrica sea 24x7 y que el reemplazo de partes por almenos 3 años. **DEBE INCLUIR EN LA INSTALACIÓN** *Instalación física y energizado de los equipos *Inicialización, configuración de IP de administración *Conexión de puertos de datos y administración. *Configuración de puertos de uplink y downlink de tal manera que quede formado un solo Fabric en conjunto con la red inalámbrica *Migración de las VLANs existentes de tal manera que se mantengan los dominios de broadcast que actualmente se encuentran en producción.				
7	Equipo Switch de Core	*Se requiere que incluya mínimo 24 puertos que soporten módulos de SFP o SFP+ de al menos 1 y10Gbps *Se requiere que cada equipo incluya al menos veinte y un (21) módulos transceivers SFP+ para conexiones de al menos 10Gbps del tipo SR (cortadistancia), al menos 42 en total *Se requiere que cada equipo incluya al menos un (1) cable pasivo de conexión directa, para conexiones de al menos 10Gbps de al menos 5 metros, al menos 2 en total *Se requiere que se incluya mínimo 2 puertos que soporten módulos QSFP+ o QSFP28 de al menos 40 y 100Gbps *Se requiere que cada equipo incluya al menos dos (2) cables pasivos de conexión directa, para conexiones de al menos 40Gbps de al menos 2 metros, al menos 4 en total *Se requiere que tenga al menos un (1) puerto de gestión dedicado	La adquisición de estos 2 equipos permitirán que tengan redundancia los switchs deCore deben estar configurados en alta disponibilidad (H/A), permitiendo tener conexión de la red en	2	UNIDAD	CONFORME

		*Se requiere que tenga al menos una (1) interfaz de consola RJ-45 *Se requiere que ocupe máximo 1 RU. *Se requiere que la capacidad de switching sea demínimo 880 Gbps *Se requiere que se maneje mínimo 1309 Mpps *Se requiere que el almacenamiento de direccionesMAC sea de mínimo 64K *Se requiere que la tabla de enrutamiento sea demínimo 24K entradas *Se requiere que el host table sea de mínimo 24Kentradas *Se requiere que soporte al menos protocolos de enrutamiento dinámico, BGP, IS-IS, PIM-SM/SSM *Se requiere que la latencia sea máxima de 1µs *Se requiere que soporte Link Aggregation con almenos 24 elementos *Se requiere que soporte al menos 24 Link Aggregation Groups *Se requiere que el Packet buffers sea de al menos8 MB *Se requiere que la memoria DRAM sea de al menos 4GB *Se requiere que la NAND sea de al menos 32 MB *Se requiere que incluya fuente redundante del tipoInterna (HotSwap) *Se requiere que el MTBF sea superior a 10 años *Se requiere que la temperatura de operación seencuentre en al menos en el rango 5-40 ºC *Se requiere que se pueda aceptar actualizacionesde firmware *Se requiere que soporte detección y notificaciónde conflictos de direcciones IP *Se requiere que soporte administración en la nube *Se requiere que soporte administración por IPv4 eIPv6 *Se requiere que soporte Telnet / SSH para acceso a la consola *Se requiere que soporte HTTP / HTTPS *Se requiere que soporte SNMP v1/v2c/v3 *Se requiere que se pueda configurar su reloj mediante un NTP Server *Se requiere que se cuente con una línea de comandos estándar y una interfaz Web de configuración *Se requiere que soporte actualizaciones de Software por: TFTP/FTP/GUI *Se requiere que soporte HTTP REST APIs para configuración y monitoreo *Se requiere que soporte Multi-Chassis LAG (MCLAG) *Se requiere que soporte STP sobre Multi-Chassis LAG (MCLAG) *Se requiere que soporte priorización de tráfico basada en 802.1p *Se requiere que soporte priorización de tráfico basada en IP TOS/DSCP *Se requiere que soporte marcado de tráfico con 802.1p y/o IP TOS/DSCP *Se requiere que soporte Link Aggregation estático *Se requiere que soporte LACP *Se requiere que soporte Spanning Tree *Se requiere que soporte Jumbo Frames *Se requiere que soporte Auto-negociacion para lavelocidad de los puertos y duplicidad *Se requiere que soporte el estándar IEEE 802.1DMAC Bridging/STP *Se requiere que soporte el estándar IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) *Se requiere que soporte el estándar IEEE 802.1sMultiple Spanning Tree Protocol (MSTP) *Se requiere que soporte la funcionalidad STPRoot Guard *Se requiere que soporte STP BPDU Guard *Se requiere que soporte Edge Port / Port Fast o quivalente. *Se requiere que soporte el estándar IEEE 802.1QVLAN Tagging *Se requiere que soporte Private VLAN *Se requiere que soporte el estándar IEEE 802.3ad Link Aggregation con LACP *Se requiere que balancee tráfico Unicast/Multicast sobre un puerto trunk (dst-ip, dst-mac, src-	todo momento, en estos se vaa encontrar toda la configuración de las vlans e intervlans de la red Lan del Comando Conjunto delas FFAA.			

		dst-ip, src-dst-mac, src-ip, src-mac) *Se requiere que soporte el estándar IEEE 802.1AX Link Aggregation *Se requiere que soporte instancias de Spanning Tree (MSTP/CST) *Se requiere que soporte el estándar IEEE 802.3xFlow Control con Back-pressure *Se requiere que soporte el estándar IEEE 802.310Base-T *Se requiere que soporte el estándar IEEE 802.3u100Base-TX *Se requiere que soporte el estándar IEEE 802.3z 1000Base-SX/LX *Se requiere que soporte el estándar IEEE 802.3ab 1000Base-T *Se requiere que soporte el estándar IEEE 802.3ae10 Gigabit Ethernet *Se requiere que soporte los estándares IEEE 802.3ba, 802.3bj, 802.3bm de al menos 40 y 100 Gigabit Ethernet *Se requiere que soporte el estándar IEEE 802.3 CSMA/CD como método de acceso y las especificaciones de la capa física *Se requiere que cuente con la funcionalidad de Control de Tormentas (Storm Control) *Se requiere que soporte la creación de VLANs porMAC, IP y Ethertype-based *Se requiere que soporte la funcionalidad de Virtual-Wire o equivalente/similar *Se requiere que soporte mínimo 4000 VLANs simultáneas *Se requiere que soporte IGMP Snooping *Se requiere que soporte emergency location identifier numbers (ELINs) o similar en LLDP-MED *Se requiere que permita un mínimo de 32instancias de MSTP *Se requiere que permita controlar tormentas debroadcast independientemente en cada puerto *Se requiere que soporte un mecanismo dedetección y prevención de loops *Se requiere que soporte SPAN *Se requiere que soporte RSPAN y ERSPAN *Se requiere que soporte ruteo estático *Se requiere que soporte RIP v2 *Se requiere que soporte OSPF v2 *Se requiere que soporte VRRP *Se requiere que soporte IS-IS *Se requiere que soporte BGP *Se requiere que soporte protocolos de ruteomulticast *Se requiere que soporte Equal Cost MultipathRouting (ECMP) *Se requiere que soporte Bidirectional ForwardingDetection (BFD) *Se requiere que soporte DHCP Relay *Se requiere que soporte DHCP Server *Se requiere que soporte el RFC 2571 Architecturefor Describing SNMP *Se requiere que soporte el RFC 2865 RADIUS *Se requiere que soporte el RFC 1643 Ethernet-like Interface MIB *Se requiere que soporte el RFC 1213 MIB-II *Se requiere que soporte el RFC 1354 IPForwarding Table MIB *Se requiere que soporte el RFC 2572 SNMPMessage Processing and Dispatching *Se requiere que soporte el RFC 1573 SNMP MIBII *Se requiere que soporte el RFC 1157SNMPv1/v2c *Se requiere que soporte el RFC 2030 SNTP *Se requiere que soporte Port Mirroring *Se requiere que soporte Admin Authentication víaRFC 2865 RADIUS *Se requiere que soporte el estándar IEEE 802.1x authentication Port-based *Se requiere que soporte el estándar IEEE 802.1x Authentication MAC-based *Se requiere que soporte el estándar IEEE 802.1xGuest and Fallback VLAN *Se requiere que soporte el estándar IEEE 802.1xMAC				

		Access Bypass (MAB) *Se requiere que soporte el estándar IEEE 802.1xDynamic VLAN assignment *Se requiere que soporte Radius CoA (Change ofAuthority) *Se requiere que soporte el estándar IEEE 802.1abLink Layer Discovery Protocol (LLDP) *Se requiere que soporte el estándar IEEE 802.1abLLDP-MED *Se requiere que soporte Radius Accounting *Se requiere que soporte EAP pass-through *Se requiere que soporte detección de dispositivos *Se requiere que soporte MAC-IP binding *Se requiere que soporte sFlow o similar *Se requiere que soporte Flow Export o similar *Se requiere que soporte ACLs *Se requiere que soporte múltiples ACLs de ingreso *Se requiere que soporte scheduling de ACLs *Se requiere que soporte DHCP Snooping *Se requiere que permita Dynamic ARP Inspection(DAI) *Se requiere que soporte Syslog *Se requiere que cuente con un sistema de temperatura y alerta. *Se requiere que el servicio de soporte de fábrica sea 24x7 y que el reemplazo de partes por almenos 3 años. **DEBE INCLUIR EN LA INSTALACIÓN** *Instalación física y energizado de los equipos *Inicialización, configuración de IP de administración *Conexión de puertos de datos y administración. *Configuración de puertos de uplink y downlink detal manera que quede formado un solo Fabric en conjunto con la red inalámbrica. *Migración de las VLANs existentes de tal manera que se mantengan los dominios de broadcast que actualmente se encuentran en producción.				
8	Equipos Access Point Wireless	*Se requiere que sea del tipo Indoor *Se requiere que soporte un throughput de almenos 867 Mbps *Se requiere que soporte al menos 512 usuariostotales conectados *Se requiere que implemente las tecnologías 802.11 a/b/g/n/ac *Se requiere que opere en las frecuencias de 2.4 /5 GHz *Se requiere que tenga al menos 2 radios *Se requiere que soporte 802.11ac Wave2 *Se requiere que soporte MU-MIMO *Se requiere que implemente 802.11ac VHT20/40/80 MHz *Se requiere que maneje una potencia máxima deal menos: *Se requiere al menos 23 dBm en la banda de 2.4GHz *Se requiere al menos 24 dBm en la banda de5GHz *Se requiere que llegue a una sensibilidad de RXde al menos -91 dBm *Se requiere que maneje al menos 2 spatial stream *Se requiere que tenga al menos 4 antenasinternas *Se requiere que la ganancia de las antenasinternas en 2.4GHz sea de al menos 4 dBi *Se requiere que la ganancia de las antenasinternas en 5GHz sea al menos 5 dBi *Se requiere que tenga al menos1 antena internaBLE *Se requiere que tenga al menos una (1) interfazde red de al menos 1 Gigabit Ethernet *Se requiere que soporte IEEE 802.3az *Se requiere que tenga conector de seguridad Kensington *Se requiere que soporte temperatura de operación de al menos hasta 45 º C *Se requiere que se implemente Transmit Beamforming (TxBF) *Se requiere que soporte WPA3 *Se requiere que tenga analizador de espectro *Se requiere que permita implementar MESH *Se requiere que permita el acceso de los dispositivos a la red inalámbrica y todas sus configuraciones deben ser centralizadas en un controlador inalámbrico	Los equipos access point serán distribuidos en todo el edificio del Comando Conjunto de las Fuerza Armadas, permitiendo tener la conexión inalámbrica del internet entodos los pisosy salas de reunión.	22	UNIDAD	CONFORME

		*Se requiere que soporter un modo de operación centralizado, o sea, su operación depende del controlador inalámbrico que es responsable de gestionar las políticas de seguridad, calidad de servicio (QoS) y monitoreo de la radiofrecuencia *Se requiere que identifique automáticamente el controlador inalámbrico al que se conectará *Se requiere que permita administrarse remotamente a través de enlaces WAN *Se requiere que permita configuraciones independientes en cada radio *Se requiere que el tráfico de los dispositivos conectados a la red inalámbrica se maneje de forma centralizada a través de un túnel establecido entre el punto de acceso y el controlador inalámbrico. En este modo todos los paquetes deben ser encapsulados a través de DTLS o IPSEChasta el controlador inalámbrico *Se requiere de forma opcional que permita que el tráfico de los dispositivos conectados a la red inalámbrica sea deforma distribuida (local switching), o sea, el tráfico sea conmutado localmente en la interfaz LAN del punto de acceso y no necesite ser encapsulado hasta el controlador inalámbrico *Se requiere que cuando el tráfico sea distribuido y la autenticación sea PSK, en caso de fallo en la conexión entre los puntos de acceso y el controlador inalámbrico, los usuarios asociados deben permanecer asociados a los puntos de acceso y al mismo SSID. Se requiere permitir la conexión de nuevos usuarios a la red inalámbrica *En conjunto con el controlador inalámbrico, se requiere optimizar el rendimiento y la cobertura inalámbrica (RF), realizando automáticamente el ajuste de potencia y la distribución adecuada de canales a ser utilizados *Se requiere que soporte la funcionalidad de ajuste automático de potencia para extender la coberturaen caso de falla de un punto de acceso vecino gerenciado por la misma controladora *Se requiere que soporte mecanismos para la detección y mitigación de puntos de acceso no autorizados, también conocidos como Rogue APs *En conjunto con el controlador inalámbrico, se requiere que permita implementar mecanismos de protección para identificar ataques a la infraestructura inalámbrica (wIDS / wIPS) *En conjunto con el controlador inalámbrico, se requiere que permita la creación de múltiples dominios de movilidad (SSID) con configuracionesdistintas de seguridad y red *En conjunto con el controlador inalámbrico, se requiere que permita implementar los siguientes métodos de autenticación: WPA (TKIP) y WPA2 (AES) *En conjunto con el controlador inalámbrico, se requiere que permita implementar el protocolo IEEE 802.1X con la asociación dinámica de VLAN para los usuarios en función de los atributos proporcionados por los servidores RADIUS *Se requiere que admita los siguientes métodos de autenticación EAP: EAP-AKA, EAP-SIM, EAP- FAST, EAP-TLS, EAP-TTLS y PEAP *Se requiere que permita implementar el estándar IEEE 802.11r para acelerar el proceso de roaming de los dispositivos a través de la función conocida como Fast Roaming *Se requiere que permita implementar el estándar IEEE 802.11k para permitir que un dispositivo conectado a la red inalámbrica identifique rápidamente otros puntos de acceso disponibles ensu área para que ejecute el roaming *Se requiere que permita implementar el estándar IEEE 802.11v para permitir que la red influya en lasdecisiones de roaming del cliente conectadas mediante el suministro de informacióncomplementaria, como la carga de utilización de lospuntos de acceso cercanos *Se requiere que permita implementar el estándar IEEE 802.11e. *Se requiere que permita implementar el estándar IEEE 802.11h *Se requiere que el punto de acceso soporte agregación de paquetes A-MPDU y A-MSDU				

		*Se requiere que el punto de acceso soporte (MLD) - Maximum Likelihood Demodulation *Se requiere que el punto de acceso soporte método de diversidad (MRC) Maximum Ratio Combining *Se requiere que soporte alimentación a través de Power Over Ethernet (PoE) conforme los estándares 802.3af o 802.3at *Se requiere que el punto de acceso sea compatible y sea administrado por la controladora inalámbrica de este proceso *Se requiere que cualquier licencia y / o software necesario para el cumplimiento de todas las características descritas en este término de referencia deberá ser suministrada *Se requiere que posea un certificado emitido por la Wi-Fi Alliance. *Se requiere que el servicio de soporte de fábrica sea 24x7 y que el reemplazo de partes por almenos 3 años. **DEBE INCLUIR EN LA INSTALACIÓN** *Instalación física y energizado de los equipos, los APs se instalarán junto a los puntos de red asignados por el cliente en las salas de reuniones de cada piso *Registro de los AP en el firewall interno o en la controladora (dependiendo de la solución) *Aplicación de los perfiles de seguridad definidos en la arquitectura aprobada por el cliente.				
9	Equipos Firewall Interno	*Se requiere que Throughput de por lo menos 45 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 (64 bytes) y IPv6 (86bytes) *Se requiere que soporte por lo menos 8 Millones conexiones simultaneas *Se requiere que soporte por lo menos 500K nuevas conexiones por segundo *Se requiere que el Throughput sea de al menos 48Gbps de VPN IPSec *Se requiere que soporte o este licenciado para manejar al menos 20K túneles de VPN IPSec site-to-site simultáneos *Se requiere que soporte o este licenciado para manejar al menos 100K túneles de clientes VPN IPSec simultáneos *Se requiere que el throughput sea de al menos 8.4Gbps de VPN SSL *Se requiere que soporte al menos 10K clientes de VPN SSL simultáneos *Se requiere que soporte al menos 12.5 Gbps de throughput de IPS *Se requiere que soporte al menos 10 Gbps de throughput de Inspección SSL *Se requiere que soporte al menos 26 Gbps de throughput de Application Control *Se requiere que soporte al menos 9.8 Gbps de throughput de NGFW *Se requiere que soporte al menos 7.1 Gbps de throughput de Threat Protection *Se requiere que tenga al menos 16 puertos de almenos 1Gbps RJ45. *Se requiere que tenga al menos 8 slots para módulos SFP de al menos 1Gbps *Se requiere que tenga al menos 4 slots para módulos SFP+ o SFP de al menos 10 y 1Gbps *Se requiere que cada equipo incluya al menos 2 módulos transceivers SFP+ para conexiones de almenos 10Gbps del tipo SR (corta distancia), al menos 4 en total *Se requiere que tenga al menos 4 slots para módulos SPF28, SFP+ o SFP de al menos 25, 10 y 1Gbps *Se requiere que tenga al menos 2 slots para módulos QSFP+ de al menos 40Gbps *Se requiere que este licenciado y/o tenga incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance *Se requiere que soporte por lo menos 250 sistemas virtuales lógicos (Contextos) por appliance *Se requiere que incluya una fuente de poder redundante *Se requiere que la solución consista en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola degestión y monitoreo.	Estos equipos van a permitir realizar la protección de la red interna de ataques externos, virus, ids. Ips. Los firewall internos identificar las ips maliciosas, adicional el registro de logs.	2	UNIDAD	CONFORME

		*Las funcionalidades de NGFW con las que se requiere contar son: reconocimiento de aplicaciones, prevención de amenazas,identificación de usuarios y control granular de permisos *Se requiere que la plataforma este optimizada para análisis de contenido de aplicaciones en capa7 *Se requiere que todo el equipo proporcionado seaadecuado para montaje en rack de al menos 19 ", incluyendo al menos un rail kit (si es necesario) y los cables de alimentación *Se requiere que la gestión de los equipos sea a través de una interfaz de administración Web en elmismo dispositivo de protección de la red *Se requiere que los dispositivos de protección de red soporten al menos 4094 VLANs Tags 802.1q *Se requiere que los dispositivos de protección de red soporten agregación de enlaces 802.3ad y LACP *Se requiere que los dispositivos de protección de red soporten Policy based routing y policy based forwarding *Se requiere que los dispositivos de protección de red soporten ruteo de tráfico multicast (PIM-SM y PIM-DM); *Se requiere que los dispositivos de protección dered soporten DHCP Relay *Se requiere que los dispositivos de protección dered soporten DHCP Server *Se requiere que los dispositivos de protección dered soporten sFlow *Se requiere que los dispositivos de protección dered soporten Jumbo Frames *Se requiere que los dispositivos de protección dered soporten subinterfaces Ethernet lógicas *Se requiere que sea compatible con NATdinámica (varios-a-1) *Se requiere que sea compatible con NAT dinámica (muchos-a-muchos). *Se requiere que soporte NAT estática (1-a-1) *Se requiere que admita NAT estática (muchos-a-muchos) *Se requiere que sea compatible con NAT estático bidireccional 1-a-1 *Se requiere que sea compatible con la traducciónde puertos (PAT) *Se requiere que sea compatible con NAT Origen *Se requiere que sea compatible con NAT de destino; *Se requiere que soporte NAT de origen y NAT dedestino de forma simultánea; *Se requiere que soporte NAT de origen y NAT de destino en la misma política *Se requiere que soporte Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico *Se requiere que sea compatible con NAT64 y NAT46 *Se requiere que implemente el protocolo ECMP *Se requiere que soporte SD-WAN de forma nativa *Se requiere que soporte el balanceo de enlace hash por IP de origen *Se requiere que soporte el balanceo de enlace porhash de IP de origen y destino *Se requiere que soporte balanceo de enlace por peso. Se requiere que en esta opción sea posible definir el porcentaje de tráfico que fluirá a través decada uno de los enlaces. *Se requiere que sea compatible con el balanceo en al menos tres enlaces *Se requiere que implemente balanceo de enlaces sin la necesidad de crear zonas o uso de instanciasvirtuales *Se requiere que permita el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticasde uso de las interfaces de red *Se requiere que permita el envío de logs a sistemas de gestión externos simultáneamente *Se requiere que tenga la opción de enviar logs a los sistemas de control externo a través de TCP y SSL *Se requiere que soporte protección contra lasuplantación de identidad (anti-spoofing) *Se requiere que permita implementar la optimización del				

		tráfico entre dos dispositivos *Se requiere que Para IPv4, soporte enrutamientoestático y dinámico (RIPv2, OSPFv2 y BGP) *Se requiere que Para IPv6, soporte enrutamientoestático y dinámico (OSPFv3) *Se requiere que soporte OSPF graceful restart *Se requiere que sea compatible con el modo Sniffer para la inspección a través del puerto espejodel tráfico de datos de la red *Se requiere que soporte modo capa 2 (L2) para la inspección de datos y visibilidad en línea del tráfico *Se requiere que soporte modo capa 3 (L3) para la inspección de datos y visibilidad en línea del tráfico *Se requiere que soporte el modo mixto de Sniffer,L2 y L3 en diferentes interfaces físicas *Se requiere que soporte la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente *Se requiere que soporte la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3 *Se requiere que soporte configuración de alta disponibilidad activo / pasivo y activo / activo: En lacapa 3 y con al menos 3 dispositivos en el clúster *Se requiere que la configuración de alta disponibilidad sincronice sesiones *Se requiere que la configuración de alta disponibilidad sincronice al menos políticas del Firewall, NAT, QoS y objetos de la red *Se requiere que la configuración de alta disponibilidad sincronice las asociaciones de seguridad VPN *Se requiere que la configuración de alta disponibilidad sincronice Tablas FIB *Se requiere que en modo HA (Modo de alta disponibilidad) permita la supervisión de fallos de enlace *Se requiere que soporte la creación de sistemas virtuales en el mismo equipo *Se requiere que para una alta disponibilidad, el uso de clústeres virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentescontextos *Se requiere que permita la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales *Se requiere que la solución permita su gestión a través de acceso SSH y una interfaz web (HTTPS), permitiendo al menos la exportación de configuración de sistemas virtuales (contextos) porambos tipos de acceso *Se requiere que permita el control, inspección y descifrado de SSL para tráfico entrante (Inbound) ysaliente (Outbound), debe soportar el control de loscertificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos) *Se requiere que soporte una solución de seguridad integral que abarque toda la red cableada e inalámbrica *Se requiere que la solución integral permita identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas paramejorar la seguridad general y el rendimiento de una red; *Se requiere que incluya un servicio de soporte queofrezca a los clientes un chequeo de salud periódico, y permita crear con un informe de auditoría mensual personalizado de sus appliancesNGFW y WiFi *Se requiere que la consola de administración soporte como mínimo, inglés y español. *Se requiere que la consola soporte la administración de switches y puntos de acceso para mejorar el nivel de seguridad *Se requiere que la solución soporte integración nativa de equipos de la misma marca para protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.				

		*Se requiere que soporte controles de zona de seguridad *Se requiere que cuente con políticas de control por puerto y protocolo *Se requiere que cuente con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones *Se requiere que permita el control de políticas porusuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad *Se requiere que pueda aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad *Se requiere que además de las direcciones yservicios de destino, los objetos de servicio deInternet puedan agregarse directamente a las políticas de firewall *Se requiere que soporte automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública. *Se requiere que soporte el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF) *Se requiere que soporte la integración con nubespúblicas e integración SDN como AWS, Azure,GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes *Se requiere que soporte el protocolo estándar dela industria VXLAN *Se requiere que la solución permita la implementación sin asistencia de SD-WAN *Se requiere que en SD-WAN soporte, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN *Se requiere que la solución soporte la integraciónnativa con una solución de sandboxing, protección de correo electrónico, cache y web application firewall. *Se requiere que los dispositivos de protección de red tengan la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo *Se requiere que la solución detecte miles de aplicaciones clasificadas en al menos 18 categorías que al menos incluyan: Tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos y correo electrónico *Se requiere que se reconozca al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http- proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs *Se requiere que identifique el uso de tácticas evasivas, tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor Se requiere que para tráfico cifrado SSL, pueda descifrarlo con el fin de leer el payload e identificarlas firmas de la aplicación conocidas por el fabricante *Se requiere que Identifique el uso de tácticasevasivas a través de las comunicaciones cifradas Se requiere que actualice de la base de firmas dela aplicación de forma automática *Se requiere que permita limitar el ancho de bandautilizado por las aplicaciones, basado en IP, por política de usuarios y grupos *Se requiere que para mantener la seguridad de red eficiente soporte el control de las aplicacionesdesconocidas *Se requiere que permita la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acciónde fabricante				

		*Se requiere que el fabricante permita solicitar la inclusión de aplicaciones en su base de datos *Se requiere que permita la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc)permitiendo granularidad de control/reglas para el mismo *Se requiere que permita la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo *Se requiere que permita la diferenciación y manejode las aplicaciones de chat; por ejemplo, permitir aHangouts el chat, pero impedir la llamada de video *Se requiere que permita la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.)permitiendo granularidad de control/reglas para el mismo *Se requiere que sea posible la creación de gruposdinámicos de aplicaciones, basado en sus características, como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc) *Se requiere que sea posible crear grupos dinámicos de aplicaciones basados en sus características, como: Nivel de riesgo de laaplicación *Se requiere que se posible crear grupos estáticos de aplicaciones basadas en sus características, como: Categoría de Aplicación *Se requiere que se posible configurar ApplicationOverride seleccionando las aplicaciones individualmente *Se requiere que soporte controles de zona de seguridad *Se requiere que cuente con políticas de control por puerto y protocolo *Se requiere que cuente con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones *Se requiere que permita el control de políticas porusuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad *Se requiere que pueda aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad *Se requiere que además de las direcciones yservicios de destino, los objetos de servicio deInternet puedan agregarse directamente a las políticas de firewall *Se requiere que soporte automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública. *Se requiere que soporte el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF) *Se requiere que soporte la integración con nubespúblicas e integración SDN como AWS, Azure,GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes *Se requiere que soporte el protocolo estándar dela industria VXLAN *Se requiere que la solución permita la implementación sin asistencia de SD-WAN *Se requiere que en SD-WAN soporte, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN *Se requiere que la solución soporte la integraciónnativa con una solución de Sandboxing, protección de correo electrónico, cache y Web applicationfirewall. *Se requiere que los dispositivos de protección de red tengan la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo *Se requiere que la solución detecte miles de aplicaciones clasificadas en al menos 18 categorías que al menos incluyan: Tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos y correo electrónico *Se requiere que reconozca al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-				

		in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http- proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs *Se requiere que identifique el uso de tácticas evasivas, tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor. *Se requiere para tráfico cifrado SSL, que se pueda descifrarlo con el fin de leer el payload e identificarlas firmas de la aplicación conocidas por el fabricante *Se requiere que Identifique el uso de tácticasevasivas a través de las comunicaciones cifradas *Se requiere que actualice de la base de firmas de la aplicación de forma automática *Se requiere que limite el ancho de banda utilizadopor las aplicaciones, basado en IP, por política de usuarios y grupos *Se requiere que para mantener la seguridad de red eficiente soporte el control de las aplicaciones desconocidas *Se requiere que permita la creación de formanativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acciónde l fabricante *Se requiere que el fabricante permita solicitar la inclusión de aplicaciones en su base de datos *Se requiere que permita la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc)permitiendo granularidad de control/reglas para el mismo *Se requiere que permita la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo *Se requiere que permita la diferenciación y manejode las aplicaciones de chat; por ejemplo, permitir aHangouts el chat, pero impedir la llamada de video *Se requiere que permita la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.)permitiendo granularidad de control/reglas para el mismo *Se requiere que sea posible la creación de gruposdinámicos de aplicaciones, basado en sus características, como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc) *Se requiere que sea posible crear grupos dinámicos de aplicaciones basados en sus características, como: Nivel de riesgo de laaplicación *Se requiere que sea posible crear grupos estáticos de aplicaciones basadas en sus características, como: Categoría de Aplicación *Se requiere que sea posible configurar ApplicationOverride seleccionando las aplicaciones individualmente *Se requiere que identifique el uso de tácticas evasivas, tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor *Se requiere que para tráfico cifrado SSL, pueda descifrarlo con el fin de leer el payload e identificarlas firmas de la aplicación conocidas por el fabricante *Se requiere que Identifique el uso de tácticas evasivas a través de las comunicaciones cifradas *Se requiere que actualice de la base de firmas dela aplicación de forma automática. *Se requiere que limite el ancho de banda utilizadopor las aplicaciones, basado en IP, por política de usuarios y grupos *Se requiere que para mantener la seguridad de red eficiente soporte el control de las aplicaciones desconocidas *Se requiere que permita la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acciónde l fabricante *Se requiere que el fabricante permite solicitar la inclusión de aplicaciones en su base de datos				

		*Se requiere que permita la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc)permitiendo granularidad de control/reglas para el mismo *Se requiere que permita la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo *Se requiere que permita la diferenciación y manejo de las aplicaciones de chat; por ejemplo, permitir a Hangouts el chat, pero impedir la llamadade video *Se requiere que permita la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.)permitiendo granularidad de control/reglas para el mismo *Se requiere que sea posible la creación de gruposdinámicos de aplicaciones, basado en sus características, como: Se requiere que Tecnologíautilizada en las aplicaciones (Client-Server, BrowseBased, Network Protocol, etc) *Se requiere que sea posible crear grupos dinámicos de aplicaciones basados en sus características, como: Nivel de riesgo de laaplicación *Se requiere que sea posible crear grupos estáticos de aplicaciones basadas en sus características, como: Categoría de Aplicación Se requiere que sea posible configurar ApplicationOverride seleccionando las aplicaciones individualmente *Para proteger el entorno contra los ataques, debeincluir los módulos de IPS, antivirus y antispyware integrado en el propio equipo *Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirusy antispyware) *Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante *Debe sincronizar las firmas de IPS, antivirus, antispyware cuando se implementa en alta disponibilidad *Debe soportar granularidad en las políticas de IPS,Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio yla combinación de todos estos elementos *Deber permitir el bloqueo de vulnerabilidades y exploits conocidos. *Debe incluir la protección contra ataques de denegación de servicio *Debe tener el mecanismo de inspección IPS: Análisis de decodificación de protocolo *Debe tener el mecanismo de inspección IPS: Análisis para detectar anomalías de protocolo; *Debe tener el mecanismo de inspección IPS: Desfragmentación IP *Debe tener el siguiente mecanismo de inspección IPS: Reensamblado de paquetes TCP *Debe tener el mecanismo de inspección IPS: Bloqueo de paquetes con formato incorrecto(malformed packets) *Debe ser inmune y capaz de prevenir los ataquesbásicos, tales como inundaciones (flood) de SYN, ICMP, UDP *Debe detectar y bloquear los escaneos de puertosde origen *Debe bloquear ataques realizados por gusanos (worms) conocidos *Debe contar con firmas específicas para la mitigación de ataques DoS y DDoS; *Debe contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow) *Debe poder crear firmas personalizadas en la interfaz gráfica del producto Identificar y bloquear la comunicación con redes debots *Debe permitir registrar en la consola de supervisión al menos la siguiente información sobreamenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones y las medidas adoptadas por el dispositivo *Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación *Debe tener la función de protección a través de laresolución				

		de direcciones DNS, la identificación de nombres de resolución de las solicitudes a losdominios maliciosos de botnets conocidos; *Los eventos deben identificar el país que origino laamenaza *Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) ygusanos (worms) *Debe tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP *Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando al menos usuarios, grupos de usuarios, origen,destino, zonas de seguridad. Es decir, cada políticade firewall puede tener una configuración diferentede IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad *Debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, usando la autenticación LDAP, Active Directory, E- directorio y base de datos local *Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basado en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites de usuarios o cualquier restricción de uso *Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten laspolíticas de granularidad / control basado en usuarios y grupos de usuarios; *Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en las políticas/control basado en usuarios y grupos de usuarios; *Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autentificación residente en el equipo de seguridad (portal cautivo) *Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario enel uso de las aplicaciones que se encuentran en estos servicios; *Debe permitir la creación de grupos de usuarios enel firewall, basada en atributos de LDAP / AD *Debe permitir la integración con tokens para la autenticación de usuarios, incluyendo por lo menosacceso a Internet y gestión de la plataforma *Debe soportar al menos dos tokens de formanativa, lo que permite la autenticación de dos factores Con el fin de controlar el tráfico y aplicaciones cuyoconsumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere que la solución, además de permitir o denegar ese tipo de tráfico, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming *Debe soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen *Debe soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino *Debe soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo *Debe soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo por lomenos Skype, BitTorrent, Azureus y YouTube *Debe soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto *En QoS debe permitir la definición de tráfico con ancho de banda garantizado *En QoS debe permitir la definición de tráfico con máximo ancho de banda *En QoS debe permitir la definición de colas de prioridad *Debe soportar la marcación de paquetes DiffServ,incluso por aplicación				

		*Debe soportar la modificación de los valores de DSCP para Diffserv; *Debe soportar priorización de tráfico utilizandoinformación de Tipo de Servicio (Type of Service). *Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes *Debe soportar la creación de políticas por geolocalización, permitiendo bloquear el tráfico de cierto(s) País/Países *Debe permitir la visualización de los países de origen y destino en los registros de acceso *Debe permitir la creación de zonas geográficas pormedio de la interfaz gráfica de usuario y la creaciónde políticas usando las mismas *Debe soportar VPN de sitio-a-sitio y cliente-a-sitio *Debe soportar VPN IPSec *Debe soportar VPN SSL *La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256 y SHA-512 *La VPN IPSec debe ser compatible con Diffie- Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14 *La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2) *La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard) *Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall *Debe soportar VPN para IPv4 e IPv6, así como eltráfico IPv4 dentro de túneles IPv6 IPSec *Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo quefacilita el proceso throubleshooting *Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy *Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL *Debe soportar autenticación vía AD/LDAP, Secure ID, certificado y base de usuarios local *Debe permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL *Debe mantener una conexión segura con el portaldurante la sesión *El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y MacOS. *Servicio de soporte de fábrica 24x7 y reemplazo de partes por al menos 3 años. **DEBE INCLUIR EN LA INSTALACIÓN** *Definición de los parámetros red: Dirección IP, Máscar, Gateway, DNS. *Registro y licenciamiento *Actualización de firmware/software hasta laversión estable más reciente. Implementación de HA según corresponda. *Configuración de las interfaces/zonas de producción. *Configuración de hasta reglas de acuerdo con lapolítica de seguridad del cliente / el LLD. *Configuración de rutas estáticas y/o ruteodinámico. * Definición de usuarios y roles. * Creación de perfiles IPS (Default) Creación de perfiles AppControl (Custom) * Integración con el esquema de autenticaciónexterna (LDAP, RADIUS)				
10	Equipo Controladora de Red Inalambrica	*Puede ofertarse un equipo independiente o el Firewall Interno además debe cumplir lassiguientes características *Debe soportar al menos 4096 puntos de acceso inalámbricos (APs) *Debe soportar al menos 2048 puntos de acceso inalámbricos configurados en modo túnel *Debe contar con un servidor DHCP integrado *Debe soportar vlan interface y vlan trunk *Debe soportar el mapeo de SSID a VLAN	Este equipo permitirá tenerla administración de todos access point del edifcio, accediendo a todos losequipos wireless	2	UNIDAD	CONFORME

		*Debe soportar VLANs dinámicas *Debe soportar ruteo estático, dinámico y por políticas *Debe soportar RIP, OSPF y BGP *Debe soportar PIM Mode *Debe soportar conversión de multicast a unicast *Debe soportar transferencia de datos centralizados hasta la controladora sin VLANs *Debe soportar transferencia de datos distribuidalocalmente *Debe soportar transferencia de datos dividibasada en políticas *Debe permitir la administración del controlador vía: •HTTPS, usando un navegador •SSH, Telnet y consola •SNMP v1 y v2 *Debe soportar alta disponibilidad 1+1 *Debe tener una conmutación sin errores en modode alta disponibilidad *Debe permitir el monitoreo del estado, uso y utilización de cada radio y canal de los puntos de acceso (APs) que controla *Debe permitir el monitoreo de la potencia de la señal, relación señal-ruido, usuario, IP, tipo de dispositivo, política de firewall, uso de ancho de banda, visibilidad de las aplicaciones de cada Cliente conectado a la Red *Debe permitir el monitoreo de puntos de acceso no autorizados (Tipo Rogue) *Deber permitir el monitoreo de la jerarquía de conectividad tipo Mesh *Debe permitir el monitoreo de la salud de la red inalámbrica, tendencias en los clientes, puntos de acceso (APs) sobrecargados, errores excesivos enradio frecuencia *Debe permitir el monitoreo de información de ubicación vía una API *Debe permitir la configuración y administración dela red inalámbrica, cableada y sistema de seguridad de manera centralizada *Debe permitir la captura remota de paquetes inalámbricos *Debe soportar que puntos de acceso (APs) sean habilitados remotamente sobre enlaces WAN *Debe tener la opción de encriptar el tráfico de datos de los APs remotos *La conectividad de clientes debe mantenerse en los APs remotos aun en caso de la caída del enlaceWAN al menos para SSIDs abiertos o que usen PSK *Debe soportar topologías mesh de múltiples saltos *Debe soportar varias instancias de redes Mesh. *Debe permitir la configuración de la cantidadmáxima de saltos en una red Mesh *Debe soportar enlaces punto a punto *Debe soportar al menos: •IEEE 802.1x (EAP, Cisco-LEAP o similar, PEAP, EAP-TLS, EAP-TTLS, EAP-SIM, EAP-AKA) •RFC 2716 PPP EAP-TLS •RFC 2865 autenticación con RADIUS •RFC 3579 RADIUS support for EAP •RFC 3580 IEEE 802.1x Lineamientos RADIUS •RFC3748 EAP •WEP64 – 64-bit •WEP128 – 128-bit •WPA personal y empresarial, incluyendo soportepara Multiple PreShared Keys (M-PSKs) •WPA2 personal y empresarial – estándar 802.11i •Autenticación por dirección MAC •Autenticación por dirección MAC vía RADIUS •Autenticación basada en Certificados para BYOD *Debe soportar al menos los siguientes servidoresde autenticación: •Base de datos interna •RADIUS •LDAP •TACACS+ *Debe soportar al menos los siguientes protocolosde encriptación: •CCMP/AES •TKIP •TKIP+AES	pertenecientes al edificio.			

		•DTLS •L2TP/IPSec (RFC 3193) •XAUTH/IPSec *Debe soportar VPNs de los siguientes tipos: •SSL •IPSec *Debe incluir un portal cautivo: •Que se autentique contra servidores deautenticación internos y externos •Que sea totalmente personalizable, incluyendo ellenguaje *Debe permitir el redireccionamiento a un portalcautivo externo *Debe permitir la administración de usuarios tipovisita a través de un portal. •Debe permitir configurar tiempo de expiración •Debe permitir configuración de tiempo de inicio •Debe permitir la creación de cuentas en grupo *Debe soportar DDARP o similar para la selección automática de canales para alcanzar un desempeño óptimo *Debe soportar el balanceo inteligente de clientes entre radios *Debe distribuir clientes de forma balanceada entrelos APs en los canales disponibles *Debe ajustar automáticamente la potencia de transmisión para extender la cobertura en caso de que un AP falle *Debe incluir un analizador de espectro *Debe soportar clientes IPv6 *Debe soportar la administración a través de IPv6 *Debe soportar protocolos de ruteo trabajando en IPv6 y opcionalmente debe soportar la funcionalidad de firewall y UTM *Debe soportar los siguientes estándares IEEE: •802.11ax, *802.11a, •802.11b, •802.11d, •802.11g, •802.11k, •802.11n, •802.11r, •802.11v, •802.11w, •802.11ac, •802.1Q, •802.3ad, •802.3af, •802.3at, •802.3az, •802.11ax, •802.3bz~~7~~ *Servicio de soporte de fábrica 24x7 y reemplazode partes por al menos 3 años.				
11	Equipo Switch Spine de Data Center	*Se requiere que soporte sistemas operativos delfabricante del hardware y como opcional de terceros *Cada switch debe contar con al menos 24 slotspara módulos SFP28 *Cada switch debe contar con al menos 4 slots paramódulos QSFP28 *Cada switch debe incluir al menos 4 cables QSFP28 a QSPF28, 100Gbps, de al menos 1 metro. 8 en total *Cada switch debe soportar una capacidad de Switching de al menos 2.16 Tbps full-duplex *Cada switch debe soportar una capacidad de Throughput de al menos 1.42 Bpps full-duplex *El Switch de mantener una latencia igual o menora 881 nano segundos *Debe soportar PTP 1588v2 *Debe soportar al menos 32K direcciones MAC *Debe soportar al menos 16K dispositivos IPv4 *Debe soportar al menos 8K dispositivos IPv6 *Debe soportar al menos 128K rutas IPv4 *Debe soportar al menos 64K rutas IPv6 *Debe soportar al menos 16K rutas multicast *Debe soportar al menos 2K ACL de ingreso Capa2 *Debe soportar al menos 256 ACL de egreso Capa2	Este equipo permitirá gestionar el tráfico de red a nivel de capa3, cada puertode este equipoiran conectados los 22 switch de piso, mismos estarán configurados en alta disponibilidad.	2	UNIDAD	CONFORME

		*Debe soportar al menos 2K ACL de ingreso IPv4 *Debe soportar al menos 2K ACL de egreso IPv4 *Debe soportar al menos 1K ACL de ingreso IPv6 *Debe soportar al menos 1K ACL de egreso IPv6 *Debe soportar al menos 4K VLANs *Debe soportar al menos 63 instancias de MSTP *Debe soportar al menos 150 instancias de PVST *Debe soportar al menos 128 LAG *Deber soportar al menos 16 miembros por cadaLAG *Debe soportar el balanceo en LAG basado en Capa 2 o en cabeceras IPv4 o IPv6 *Debe soportar sistemas operativos del fabricante del hardware y de terceros *Debe soportar funciones de red estándar, interfaces y funciones de scripting de comandos que permitan la integración de operaciones con redes Legacy *Debe soportar la abstracción del hardware usandoSAI (Switch Abstraction Interface) o Open Programmability System (OPS). *Debe proveer un entorno de desarrollador generalizado y sin restricciones a través de ControlPlane Services (CPS) o similar *Debe incluir protocolos de conmutación y enrutamiento de capa 2 y 3, junto con servicios de Multicast e IP integrados, calidad de servicio y características de administración y automatización *Debe aprovechar las mejores prácticas y herramientas comunes de código abierto (modelos de datos YANG, commit scratchpad o similar) *Debe soportar API programables, automatización de la CLI mediante lotes y alias para simplificar la gestión de la configuración. *Debe manejar conmutación Ethernet en Capa 2 y 3 escalable, diseñada para fabrics de centros de datos, con implementación de QoS en LAG Multi- Chassi (VLT) o similar, ACL y funcionalidades basadas en estándares IPv4, IPv6 y Multicast *Debe soportar compatibilidad con Múltiples clientes (Multitenant) mediante VRF LITE, integraciones de VMWare NSX o equivalente y Overlays basadasen estándares (BGP EVPN) *Debe soportar la interconexión de centros de datos y optimizaciones mediante BGP EVPN Symmetric IRB o similar, no numerado, supresión de ARP, rutas de tipo 5. Filtración dinámica de rutas a través de VRF utilizando políticas basadas en mapas de ruta y mecanismos RT disponibles en EVPN. *Debe permitir aumentar la región de movilidad de máquinas virtuales (VM) extendiendo las VLAN de capa 2 dentro o entre dos centros de datos con capacidades VxLAN y/o VLT. *Debe brindar soporte para redes convergentespara Data Center Bridging, con control de flujoprioritario (802.1Qbb), ETS (802.1Qaz) o similares DCBx y TLV iSCSI *Debe soportar Redes definidas por software que utilizan estándares Openflow 1.0/1.3 con compatibilidad con varios controladores para alta disponibilidad *Debe incluir capacidades mejoradas de depuración y solución de problemas que incluyan local mirroring, ERPM/similar, muestreo de flujos (sFLOW) o equivalente *Debe incluir sensores de monitoreo de telemetría, que transmitan datos usando gPB y Grpc o similar *Debe contar con Interfaz OpenConfig gNMI o similar para la gestión del sistema, compatibilidad con Hash simétrico para LAG y ECMP *Debe soportar el clúster de Microsoft NLB o equivalente, soportar el perfil de telecomunicaciones PTP G.8275.2, SyncE y PTP híbrido *Debe soportar fuentes de poder AC y DCreemplazables en caliente *Debe incluir 2 fuentes de poder AC en alta disponibilidad con flujo de salida de aire caliente por las fuentes de poder *Debe soportar ventiladores redundantesreemplazables en caliente *Debe soportar al menos los siguientes estándares: •802.1AB LLDP •TIA-1057 LLDP-MED				

		•802.3ad Link Aggregation •802.1D Bridging, STP •802.1p L2 Prioritization •802.1Q VLAN Tagging *802.1Qbb PFC o similar •802.1Qaz ETS o similar •802.1X Network Access Control •802.3ac Frame Extensions for VLAN Tagging •802.3x Flow Control •Jumbo MTU de al menos 9216 bytes •802.1D Compatible •802.1s MSTP •802.1w RSTP •802.1t RPVST+ •VLT (Virtual Link Trunking) •VRRP Activo/Activo •RSTP y RPVST+ •Port Mirroring en puertos VLT •DCB, iSCSI, FIP Snooping Bridge o similar •RPM/ERPM sobre VLT o similar •4254 SSHv2 •791 IPv4 •1305 NTPv4 •2131 DHCPv4 (server and relay) •5798 VRRPv3 •2372 Direccionamiento IPv6 •2460 Protocolo IPv6 •2463 ICMPv6 •2328 OSPFv2 •5340 OSPF para IPv6 (OSPFv3) •4541 IGMPv1/v2/v3 y MLD v1/v2 Snooping •2865 RADIUS •3162 Radius e IPv6 •1492 TACACS •4271 BGP-4 •2545 BGP-4 extensión Multiprotocol para ruteoIPv6 entre dominios *Debe soportar al menos: •SNMPv1/2c •IPv4/IPv6 Management support (Telnet, FTP,TACACS, RADIUS, SSH, NTP) •Syslog •Port Mirroring •RPM/ERPM o similar •3176 SFlow o similar •RestConf APIs (Layer 2 features) •XML Schema o equivalente •CLI Commit (Scratchpad) *Debe soportar al menos: •Lista de prefijos •Route-Map •Rate Shaping (Egreso) •Rate Policing (Ingreso) •Algoritmos de programación - Round Robin - Weighted Round Robin - Deficit Round Robin - Strict Priority - Weighted Random Early Detect *Debe soportar al menos: •802.1Qbb o similar •802.1Qaz o similar •DCBx •DCBx Application TLV (iSCSI, FCoE) •RoCEv2 •Software Defined Networking OpenFlow 1.3(Nativo) *Servicio de soporte de fábrica 24x7 y reemplazode partes por 3 años.				

12	Equipo Switch Leaf de Data Center	*Debe soportar sistemas operativos del fabricante del hardware y como opcional de terceros *Cada switch debe contar con al menos 24 slots para módulos SFP28 *Cada switch debe incluir al menos 6 cables SFP28a SPF28, 25Gbps, de al menos 2 metros. 12 en total *Cada switch debe incluir al menos 4 módulosSFP+ 10G-Base SR, 8 en total *Cada switch debe contar con al menos 4 slots paramódulos QSFP28 *Cada switch debe soportar una capacidad deSwitching de al menos 2.16 Tbps full-duplex *Cada switch debe soportar una capacidad deThroughput de al menos 1.42 Bpps full-duplex *El Switch de mantener una latencia igual o menora 881 nano segundos *Debe soportar PTP 1588v2 *Debe soportar al menos 32K direcciones MAC *Debe soportar al menos 16K dispositivos IPv4 *Debe soportar al menos 8K dispositivos IPv6 *Debe soportar al menos 128K rutas IPv4 *Debe soportar al menos 64K rutas IPv6 *Debe soportar al menos 16K rutas multicast *Debe soportar al menos 2K ACL de ingreso Capa2 *Debe soportar al menos 256 ACL de egreso Capa2 *Debe soportar al menos 2K ACL de ingreso IPv4 *Debe soportar al menos 2K ACL de egreso IPv4 *Debe soportar al menos 1K ACL de ingreso IPv6 *Debe soportar al menos 1K ACL de egreso IPv6 *Debe soportar al menos 4K VLANs *Debe soportar al menos 63 instancias de MSTP *Debe soportar al menos 150 instancias de PVST *Debe soportar al menos 128 LAG *Deber soportar al menos 16 miembros por cadaLAG *Debe soportar el balanceo en LAG basado en Capa 2 o en cabeceras IPv4 o IPv6 *Debe soportar funciones de red estándar, interfaces y funciones de scripting de comandos que permitan la integración de operaciones con redes Legacy *Debe soportar la abstracción del hardware usando SAI (Switch Abstraction Interface) o Open Programmability System (OPS) *Debe proveer un entorno de desarrollador generalizado y sin restricciones a través de ControlPlane Services (CPS) o similar *Debe incluir protocolos de conmutación y enrutamiento de capa 2 y 3, junto con servicios de Multicast e IP integrados, calidad de servicio y características de administración y automatización *Debe aprovechar las mejores prácticas y herramientas comunes de código abierto (modelos de datos YANG, commit scratchpad) *Debe soportar API programables, automatización de la CLI mediante lotes y alias para simplificar la gestión de la configuración. *Debe manejar conmutación Ethernet en Capa 2 y 3 escalable, diseñada para fabrics de centros de datos, con implementación de QoS en LAG Multi- Chassi (VLT) o similar, ACL y funcionalidades basadas en estándares IPv4, IPv6 y Multicast. *Debe soportar compatibilidad con Múltiples clientes (Multitenant) mediante VRF LITE, integraciones de VMWare NSX o similar y Overlays basadas en estándares (BGP EVPN) *Debe soportar la interconexión de centros de datos y optimizaciones mediante BGP EVPN Symmetric IRB o similar, no numerado, supresión de ARP, rutas de tipo 5. Filtración dinámica de rutas a través de VRF utilizando políticas basadas en mapas de ruta y mecanismos RT disponibles en EVPN. *Debe permitir aumentar la región de movilidad de máquinas virtuales (VM) extendiendo las VLAN decapa 2 dentro o entre dos centros de datos con capacidades VxLAN y/o VLT. *Debe brindar soporte para redes convergentespara Data Center Bridging, con control de flujoprioritario (802.1Qbb) o similar, ETS (802.1Qaz) o similar, DCBx y TLV iSCSI	Estos equipos permiten controlar el trafico entre segmentos de red a nivel de capa 2 y 3	2	UNIDAD	CONFORME

		*Debe soportar Redes definidas por software que utilizan estándares Openflow 1.0/1.3 con compatibilidad con varios controladores para alta disponibilidad *Debe incluir capacidades mejoradas de depuración y solución de problemas que incluyan local mirroring, ERPM/similar, muestreo de flujos (sFLOW) o equivalente *Debe incluir sensores de monitoreo de telemetría, que transmitan datos usando gPB y gRPC o una funcionalidad equivalente/similar *Debe contar con Interfaz OpenConfig gNMI o una interfaz equivalente para lagestión del sistema, compatibilidad con Hash simétrico para LAG y ECMP *Debe soportar el clúster de Microsoft NLB o equivalente, soportar el perfil de telecomunicaciones PTP G.8275.2, SyncE y PTP híbrido *Debe soportar fuentes de poder AC y DCreemplazables en caliente *Debe incluir 2 fuentes de poder AC en alta disponibilidad con flujo de salida de aire caliente por las fuentes de poder *Debe soportar ventiladores redundantesreemplazables en caliente *Debe soportar al menos los siguientes estándares: •802.1AB LLDP •TIA-1057 LLDP-MED •802.3ad Link Aggregation •802.1D Bridging, STP •802.1p L2 Prioritization •802.1Q VLAN Tagging •802.1Qbb PFC o similar •802.1Qaz ETS o similar •802.1X Network Access Control •802.3ac Frame Extensions for VLAN Tagging •802.3x Flow Control •Jumbo MTU de al menos 9216 bytes •802.1D Compatible •802.1s MSTP •802.1w RSTP •802.1t RPVST+ •VLT (Virtual Link Trunking) •VRRP Activo/Activo •RSTP y RPVST+ •Port Mirroring en puertos VLT •DCB, iSCSI, FIP Snooping Bridge o similar •RPM/ERPM sobre VLT o similar •4254 SSHv2 •791 IPv4 1305 NTPv4 •2131 DHCPv4 (server and relay) •5798 VRRPv3 •2372 Direccionamiento IPv6 •2460 Protocolo IPv6 •2463 ICMPv6 •2328 OSPFv2 •5340 OSPF para IPv6 (OSPFv3) •4541 IGMPv1/v2/v3 y MLD v1/v2 Snooping •2865 RADIUS •3162 Radius e IPv6 •1492 TACACS •4271 BGP-4 •2545 BGP-4 extensión Multiprotocol para ruteoIPv6 entre dominios *Debe soportar al menos: •SNMPv1/2c •IPv4/IPv6 Management support (Telnet, FTP,TACACS, RADIUS, SSH, NTP) •Syslog •Port Mirroring •RPM/ERPM o similar •3176 SFlow o similar •RestConf APIs (Layer 2 features) •XML Schema o equivalente •CLI Commit (Scratchpad) *Debe soportar al menos: •Lista de prefijos •Route-Map •Rate Shaping (Egreso)				

		•Rate Policing (Ingreso) •Algoritmos de programación -Round Robin -Weighted Round Robin -Deficit Round Robin -Strict Priority -Weighted Random Early Detect *Debe soportar al menos: •802.1Qbb o similar •802.1Qaz o similar •DCBx •DCBx Application TLV (iSCSI, FCoE) •RoCEv2 •Software Defined Networking OpenFlow 1.3(Nativo) *Servicio de soporte de fábrica 24x7 y reemplazode partes por 3 años. **DEBE INCLUIR EN LA INSTALACION** *Instalación física y energizado de los equipos *Inicialización, configuración de IP de administración *Conexión de puertos de datos y administración. *Configuración de puertos de uplink y downlink de tal manera que quede formado un solo Fabric que permita su gestión a través de la herramienta de administración de la infraestructura devirtualización de la solución HCI *Migración de los puertos de la solución de HCI, respaldo y almacenamiento a los equipos Leaf, incluyendo la actualización a 25Gbps de los nodosE560 y S570 existentes *El equipo de Red que actualmente se encuentra en producción debe instalarse y configurarse para brindar conectividad a los puertos de administración de todo el equipo de Data Center. *Migración de los puertos de conexión hacia el Internet, WAN, Firewalls Internos y Externos a los equipos Leaf Edge				
13	Equipo Switch Leaf Edge	*Debe soportar sistemas operativos del fabricantedel hardware y como opcional de terceros *Cada switch debe contar con al menos 28 slotspara módulos SFP+ *Cada switch debe incluir al menos 1 cables SFP+a SPF+, 10Gbps, de al menos 1 metro. 2 en total *Cada switch debe incluir al menos 8 módulosSFP+ 10GBase-SR, 16 en total *Cada switch debe incluir al menos 12 módulosSFP 1000-Base-T, 24 en total *Cada switch debe contar con al menos 2 slots paramódulos QSFP28 *Cada switch debe soportar una capacidad deSwitching de al menos 960 Gbps full-duplex *Cada switch debe soportar una capacidad deThroughput de al menos 720 Mpps full-duplex *Debe soportar al menos 128 instancias de PVST *Debe soportar una tabla ARP de al menos 200K *Debe soportar al menos 200K rutas IPv4 *Debe soportar al menos 64K dispositivos IPv6 *Debe soportar al menos 130K rutas IPv6 *Debe soportar al menos 8K dispositivos Multicast *Debe soportar al menos 32 enlaces por cadagrupo de Link Aggregation y al menos 128 grupos *Debe soportar al menos 4K VLANs en capa 2 *Debe soportar al menos 500 VLANs en capa 3 *Debe soportar al menos 32 instancias MTSP *Debe soportar balanceo de carga LAG basado encapa 2 o cabeceras IPv4 o IPv6 *Debe soportar al menos 6K ACL capa 2 de ingreso *Debe soportar al menos 1K ACL capa 2 de egreso *Debe soportar al menos 6K ACL IPv4 de ingreso *Debe soportar al menos 1K ACL IPv4 de egreso *Debe soportar al menos 3K ACL IPv6 de ingreso *Debe soportar al menos 500 ACL IPv6 de egreso *Debe soportar funciones de red estándar, interfaces y funciones de scripting de comandos que permitan la integración de operaciones con redes Legacy *Debe soportar la abstracción del hardware usando SAI (Switch Abstraction Interface) o Open Programmability System (OPS) *Debe proveer un entorno de desarrollador generalizado y	Este equipo permitirá el enrutamiento a nivel de capa 3 para posterior conexión con los equipos decapa 2.	2	UNIDAD	CONFORME

		sin restricciones a través de ControlPlane Services (CPS) o similar *Debe incluir protocolos de conmutación y enrutamiento de capa 2 y 3, junto con servicios de Multicast e IP integrados, calidad de servicio y características de administración y automatización *Debe aprovechar las mejores prácticas y herramientas comunes de código abierto (modelos de datos YANG, commit scratchpad o similar) *Debe soportar API programables, automatización de la CLI mediante lotes y alias para simplificar la gestión de la configuración. *Debe manejar conmutación Ethernet en Capa 2 y 3 escalable, diseñada para fabrics de centros de datos, con implementación de QoS en LAG Multi- Chassi (VLT) o similar, ACL y funcionalidades basadas en estándares IPv4, IPv6 y Multicast *Debe soportar compatibilidad con Múltiples clientes (Multitenant) mediante VRF LITE, integraciones de VMWare NSX o similar y Overlays basadasen estándares (BGP EVPN) *Debe soportar la interconexión de centros de datos y optimizaciones mediante BGP EVPN Symmetric IRB o similar, no numerado, supresión de ARP, rutas de tipo 5. Filtración dinámica de rutas a través de VRF utilizando políticas basadas en mapas de ruta y mecanismos RT disponibles en EVPN. *Debe permitir aumentar la región de movilidad de máquinas virtuales (VM) extendiendo las VLAN decapa 2 dentro o entre dos centros de datos con capacidades VxLAN y/o VLT. *Debe brindar soporte para redes convergentespara Data Center Bridging, con control de flujoprioritario (802.1Qbb) o similar, ETS (802.1Qaz), DCBx y TLV iSCSI *Debe soportar Redes definidas por software que utilizan estándares Openflow 1.0/1.3 concompatibilidad con varios controladores para alta disponibilidad *Debe incluir capacidades mejoradas de depuración y solución de problemas que incluyan local mirroring, ERPM, muestreo de flujos (sFLOW) *Debe incluir sensores de monitoreo de telemetría, que transmitan datos usando gPB y gRPC o una funcionalidad equivalente/similar *Debe contar con Interfaz OpenConfig gNMI o una interfaz equivalente para lagestión del sistema, compatibilidad con Hash simétrico para LAG y ECMP *Debe soportar el clúster de Microsoft NLB o equivalente, soportar el perfil de telecomunicaciones PTP G.8275.2, SyncE y PTP híbrido *Debe soportar fuentes de poder AC y DCreemplazables en caliente *Debe incluir 2 fuentes de poder AC en alta disponibilidad con flujo de salida de aire caliente por las fuentes de poder *Debe soportar ventiladores redundantesreemplazables en caliente *Debe soportar al menos los siguientes estándares: •802.1AB LLDP •TIA-1057 LLDP-MED •802.1s MSTP •802.1w RSTP •802.1t RPVST+ •802.3ad Link Aggregation •802.1D Bridging, STP •802.1p L2 Prioritization •802.1Q VLAN Tagging •802.1Qbb PFC o similar •802.1Qaz ETS o similar •802.1X Network Access Control •802.3ac Frame Extensions for VLAN Tagging •802.3x Flow Control •Jumbo MTU de al menos 9216 bytes •VLT (Virtual Link Trunking) •DCB, FSB, iSCSI sobre VLT o similar *Debe soportar al menos los siguientes: •4254 SSHv2 •791 IPv4 •1305 NTPv4				

		•2131 DHCPv4 (server and relay) •5798 VRRPv3 •2460 Protocolo IPv6 •2463 ICMPv6 •2328 OSPFv2 *2865 RADIUS •3162 Radius e IPv6 •4271 BGP-4 *Debe soportar al menos: •SNMPv1/2c •SSHv2 •FTP, TFTP, SCP •Syslog •Port Mirroring •RADIUS •802.1X •Netconf APIs •XML Schema o similar •CLI Commit (Scratchpad) •sFlow o similar *Debe soportar al menos: •Lista de prefijos •Route-Map •Rate Shaping (Egreso) •Rate Policing (Ingreso) •Algoritmos de programación - Round Robin -Weighted Round Robin -Deficit Round Robin -Strict Priority •Weighted Random Early Detect *Debe soportar al menos: •802.1Qbb Priority-Based Flow Control •802.1Qaz Enhanced Transmission Selection(ETS) •DCBx Data Center Bridging eXchange •DCBx Application TLV (iSCSI, FCoE) *Servicio de soporte de fábrica 24x7 y reemplazode partes por 3 años. **DEBE INCLUIR EN LA INSTALACION** *Instalación física y energizado de los equipos *Inicialización, configuración de IP de administración *Conexión de puertos de datos y administración. *Configuración de puertos de uplink y downlink de tal manera que quede formado un solo Fabric que permita su gestión a través de la herramienta de administración de la infraestructura devirtualización de la solución HCI *Migración de los puertos de la solución de HCI, respaldo y almacenamiento a los equipos Leaf, incluyendo la actualización a 25Gbps de los nodosE560 y S570 existentes *El equipo de Red que actualmente se encuentra en producción debe instalarse y configurarse para brindar conectividad a los puertos de administración de todo el equipo de Data Center *Migración de los puertos de conexión hacia el Internet, WAN, Firewalls Internos y Externos a los equipos Leaf Edge.				

ORD.	**ESPECIFICACIONES TÉCNICAS DEL SERVICIO**	**JUSTIFICACIÓN**	**CUMPLIMIENTO**
	El proveedor debe incluir en el mantenimiento todos los accesorios necesarios para el trabajo de acuerdo con la infraestructura que el Comaco considera, sin que esto tenga un costo adicional para la entidad.		CONFORME
1	Los accesorios que debe incluir el servicio de mantenimiento son: Bandeja de Fibra Optica deslizable de 3 Socalos, Cantidad: 10, Su tamaño no debe ser mayor a una unidad y debe poder acomodar hasta 3 placas adaptadoras de fibra óptica multimodo y monomodo en las siguientes configuraciones: - 12, 16 y 24 adaptadores LC (6, 8 y 12 adaptadores dúplex)	Servicio de instalación para reparación de fibra óptica y accesorios de fibra para la infraestructura de cableado estructurado del comando conjunto de las fuerzas armadas.	CONFORME

	- 1, 2, 4, 6 y 8 adaptadores MTP - 6, 8 y 12 adaptadores SC - 6, 8 y 12 adaptadores ST - 6 y 8 adaptadores híbridos ST-SC - 6 y 8 adaptadores FC. § Placa adaptadora ciega para crecimiento a futuro § Debe tener placas adaptadoras de 6, 8 y 12 puertos de fibra que permitan la codificación por colores de los conectores. § Debe tener placas adaptadoras con mecanismo de engarce y retiro utilizando un solo dedo § Debe acomodar placas adaptadoras híbridas para conexiones ST a SC. § Debe tener diseño modular con organizadores de fibra internos que proporcionen almacenamiento de reserva que cumpla con los radios mínimos de curvatura de fibra y la longitud de almacenamiento recomendada. § Debe tener una cubierta frontal que pueda usarse como superficie de rotulado y para proteger los jumpers. Está cubierta debe permitir su reubicación a otra posición durante la terminación para mantener la identificación de circuitos. § Debe acomodar una bandeja para empalmes mecánicos o de fusión. Debe estar disponible con un mecanismo deslizable que permita al panel deslizarse hacia el frente o hacia atrás, y debe tener seguros desmontables que permitan su retiro del rack o gabinete. Debe estar certificado por Underwriters Laboratories para las normas de Estados Unidos y por C22.2 de las Normas de Telecomunicaciones Canadienses. Caset adaptador para 12 hilos LC, con sleeve de cerámica, **cantidad: 20.** Tapa ciega para fibra, color negro, LC **cantidad: 10** Bandeja Interna para Fusion de 12 Hilos, **cantidad: 9** Bandeja Interna para Fusion de 24 Hilos, **cantidad: 2** Prensa o glándula de conexión **cantidad: 20** Todos los componentes para el mantenimiento deben ser de la misma marca de cableado estructurado. Bandeja de Fibra Óptica deslizable de 4 Socalos, Cantidad: 6 (seis), Peso: 20.25 lbs, Dimensiones: 19.3” L x 20.5” D x 1.7” H, Materiales: Acero Laminado en frio y termoplastico retardante., La bandeja se debe deslisar tanto para adelante como para atrás. 1U de espacio, Color negra. Bandeja de fusión interna para 24 hilos **cantidad: 4** Adaptador (Cuplas) para 12 Hilos **cantidad: 22** Termo contraíbles para Fusion **cantidad: 48** Pigtail LC OM4 de 1 Mtr LS0H **cantidad: 48** Todos los componentes deben ser de la misma marca de cableado estructurado. Patch cord de Fibra Optica OM4 con cambio de polaridad de 3 metros. Cantidad: 56 de 2 metros y 66 de 3 metros. Color Aqua, Todos los jumpers ofertados tienen la misma configuración de polaridad. No se requieren dos tipos diferentes de configuraciones en ambos extremos del enlace. En caso de que se requiera, el jumper permite su cambio de polaridad sin dañar los hilos de fibra óptica. Conector LC = LC, OM4 XGLO 550 50/125 Multimodo, LSOH (IEC 60332-3C), Debe ser de la misma		

	marca del cableado estructurado ofertada, Están construido con cable de fibra óptica multimodo que cumpla con los requisitos para Ethernet 10G especificados en IEEE 802.3; así como con las normas IEC 60793-2-10 y TIA 492AAAD para OM4 en cuanto a las especificaciones para ancho de banda láser en retraso de modo diferencial (DMD - Differential Mode Delay). Normativas a cumplir: ISO/IEC 11801-1 • ANSI/TIA 568.3-D • TIA-604-10 • IEC 61754-20 • IEC 61753 Category C. • Telcordia GR-326-CORE issue 4 • RoHS Compliant . Organizador horizontal de 19" de 6" de profundidad de 1 U Y 2U. Cantidad: 16 (Dieciseis) de 1U, 24 (Veinte y Cuatro) de 2U. 6 pulgadas de profundidad, 19 pulgadas de ancho, 1U, Color negro, Debe ser de la misma marca del cableado estructurado.		
	El servicio de mantenimiento debe incluir todos los componentes necesarios para cumplir con el objetivo principal. Se requiere que cumpla con las especificaciones de la Clase FA/Categoría 7 A según ISO/IEC -11801. Se requiere obligatoriamente que el proponente anexe con la propuesta los catálogos de los productos ofertados. Cada catálogo debe mostrar el código del producto ofertado. No se aceptarán propuestas con catálogos que contengan códigos diferentes a los ofertados o descripciones diferentes a las solicitadas en el presente documento, de presentarse alguna inconsistencia se verificará el número de parte en el sitio web del fabricante y debe coincidir con las especificaciones solicitadas en el presente documento. Se requiere que todos los componentes del canal de cobre y fibra sean de una sola marca a fin de garantizar el funcionamiento end-to-end del mismo. Se exigirá que el sistema de cableado estructurado tenga una garantía expedida por el fabricante por un mínimo de 25 años sobre todos y cada uno de los componentes instalados. Así mismo se requerirá la entrega por parte del fabricante de los componentes pasivos, de una garantía que certifique el funcionamiento de todas las aplicaciones diseñadas para correr en redes sobre Clase FA. También se exigirá que todas las ofertas presentadas vengan acompañadas de una carta emitida por el fabricante en donde se avale el respaldo de este a la empresa oferente y se asuma un compromiso por la garantía, el fabricante incluirá garantía de mano de obra necesaria para los cambios requeridos por este concepto especificando las condiciones para el cumplimiento. Cantidad: 48.800 metros. ISO/IEC 11801Ed3 “Information technology - Generic cabling for customer premises” (Cableado Genérico para Propiedades de Usuario). CENELEC EN 50173:2000 y enmiendas “Information Technology - Generic cabling systems” (Tecnología de la Información - Sistemas de Cableado Genéricos). IEC 61156-5:2009 Multicore and symmetrical pair/quad cables for digital communications – Part 5: Symmetrical pair/quad cables with transmission characteristics up to 1000 MHz – Horizontal floor wiring – Sectional specification (Cables en pares o cuartetos simétricos y multinúcleo para comunicaciones – Parte 5: Cables en pares o cuartetos simétricos con características de transmission hasta 1000 MHz – Cableado horizontal – Especificaciones seccionales). IEC 61076-3-104:2017 Connectors for electronic equipment – Product requirements – Part 3-104: Detail specification for 8-way, shielded free and fixed connectors for data transmissions with frequencies up to 2000 MHz (Conectores para equipo electrónico – Requisitos de productos – Parte 3-104: Especificaciones detalladas para conectores fijos y libres de 8 vías para transmisión de datos con frecuencias de hasta 2000 MHz). IEC 61156-5 Simetría de cables para categoría 7ª. IEC/TR3 61000-5-2 - Ed. 1.0 y enmiendas“Electromagnetic compatibility (EMC) - Part 5 Installation and mitigation guidelines - Section 2: Earthing and cabling” (Compatibilidad electromagnética (EMC) – Parte 5: Directrices de instalación y mitigación – Sección 2: Conexión a tierra y cableado).	Servicio de instalación y mantenimiento del cableado de cobre en su totalidad para dar correcto funcionamiento al core de negocio del Comando Conjunto de las Fuerzas Armadas, que permita mitigar al 100% todos los inconvenientes que se han generado desde hace varios años.	CONFORME

	IEC 61935-1 1st Ed. (2015) Generic cabling systems Specification for the testing of balanced communication cabling in accordance with ISO/IEC 11801 –Installed cabling (Sistemas de Cableado Genérico – Especificaciones para las pruebas de cableado balanceado de comunicaciones en conformidad con ISO/IEC 11801) Building Industries Consulting Services, International (BICSI) Telecommunications Distribution Methods Manual (TDMM) – 12-13th edition. BICSI 007-2017, Information Communication Technology Design and Implementation Practices for Intelligent Buildings and Premises. Estar en grupos de unidades de 4-pares. Manejar anchos de banda de 1000 MHz según lo especificado por el estándar ISO 11801. El cable debe cumplir con IEC 61156-5 Ed. 2.0, IEC 60754, and IEC 61034, EN 50288 • EN55022 • EN 50173 • EN55024. Es requisito obligatorio para su verificación anexar documentos que indiquen que el cable es tipo LS0H de 1000 MHz con conductores 23 AWG. El cable debe venir marcado como Cat 7A. El contratista deberá allegar una muestra del cable con esta especificación. El cable debe venir marcado con el nombre del fabricante que ofrece también la conectividad. El cable debe ser S/FTP con un foil recubriendo cada uno de los pares y una malla alrededor de los 4 pares. El cable debe cumplir mínimo con los siguientes rangos de temperatura: Para la instalación desde 0 ºC a +60 ºC, para Almacenamiento desde – 20 ºC a +75 ºC y para operación desde – 20 ºC a +75 ºC. Es requisito obligatorio que se anexe catálogo que muestre que estos 3 rangos de temperatura con sus límites de temperatura inferior y superior se cumplen. El cable debe cumplir con IEC 60754 e IEC 61034., IEC 60332-1 y 60332-3 de tipo LS0H (LSZH-3). Es requisito indispensable que se anexe catálogo del cable y pueda verificarse la información en el sitio web en donde se muestre que estos estándares se cumplen. Se verificará a través de un laboratorio reconocido por la NRTL (UL o ETL) las características de flamabilidad de la chaqueta IEC 60332-3, El cable debe tener un diámetro máximo de 7.8 mm. Resistencia DC < 7 / 100m o de acuerdo con los requisitos normativos. Resistencia DC desbalanceado del 2% o de acuerdo con los requisitos normativos. Capacitancia mutua 5.6 nF/100m o de acuerdo con los requisitos normativos. Capacitancia desbalanceada < 150 pF/100m. Impedancia (ohms) de 1-100 MHz: 100 ± 15% 100-250 MHz: 100 ± 22% 250-1000 MHz: 100 ± 25% o de acuerdo a los requisitos normativos listados en el presente documento, El cable categoría 7ª debe haber sido probado por un laboratorio externo en función de los requerimientos ISO 11801. y IEC 61156. Se debe anexar certificado de cumplimiento del número de parte ofrecido. La ficha técnica original del cable del fabricante deberá exhibir el desempeño típico en un modelo de canal de 100 metros a 1000 MHz, los requisitos mínimos solicitados se listan a continuación: Pérdidas de inserción: máxima 56 dB ACR mayor a 22.8 dB PSNEXT, mayor a 80 dB RL mayor a 24 dB La información se podrá consultar a través de la página web del fabricante. Patch panel de 24 puertos, Cantidad: 44, § Tener capacidad para 24 puertos por cada unidad de rack (1RMS = 44.5 mm [1.75 in.]). § Cumplir con la norma ANSI/EIA-310-D o su más reciente versión para asegurar que su montaje es compatible con racks de 19 in. § El panel de parcheo debe ser modular y permitir el montaje de cualquier combinación de módulos categoría 7A, de categorías inferiores blindadas y no blindadas, de fibra óptica o de coaxial en caso de requerirse.		

	§ Para ofrecer una densidad estándar en el uso del espacio en racks, gabinetes y espacios de telecomunicaciones, debe permitir el montaje de hasta 24 conectores por cada unidad de rack. Los paneles de parcheo deben ser planos para enrutar los cordones de parcheo por medio de organizadores horizontales, los cuales deben colocarse en forma alternada con los paneles. § Para agilizar la terminación del blindaje de los cables y su conexión a tierra, los paneles deben tener lengüetas resilientes metálicas en cada puerto que permitan la conexión a tierra de los conectores al momento de su inserción y terminales de tierra que aseguren que cada módulo y cable sea adecuadamente unido a tierra. § Para facilitar la administración y el acomodo de los cables en su parte posterior, el panel debe tener integrado un organizador posterior de cables provisto con liberadores de tensión. El panel debe incluir un cinturón. Plástico para sujetar cada cable a los liberadores de tensión. § El material del panel de parcheo debe ser acero laminado en frío, de 0.060" de espesor, que brinde un peso ligero, pero de alta fortaleza para ofrecer la robustez y resistencia mecánica requerida. Debe tener acabado electrorrecubierto no texturizado en color negro. § Tener números de identificación de puertos impresos indeleblemente en el panel frontal que permitan una correcta visibilidad para facilitar la administración de sus puertos. Adicionalmente, el panel debe incluir portaetiquetas transparentes autoadheribles y tiras de designación blancas. § El panel debe incluir los tornillos para su montaje en rack y una terminal para puesta a tierra Tener números de identificación de puertos impresos indeleblemente en el panel frontal Debe ser de la misma marca del cableado estructurado. Patch cord cat 7a de 1 y 2 metros, conector tera a rj45. Cantidad: 1 metro 550 unidades, de 2 metros 1600 unidades § Estar probados 100% en transmisión con analizadores de red grado laboratorio para un desempeño apropiado § Utilizar cable multifilar blindado y apantallado con un forro cilíndrico LS0H § Tener varias opciones de ensambles en 1, 2, y 4 pares para soportar una amplia gama de aplicaciones. § Tener botas liberadoras de tensión, disponibles en varios colores. § Estar disponible en longitudes estándar de 1, 2, 3 y 5 metros con otras longitudes disponibles bajo pedido. § Cumplir y exceded las especificaciones de desempeño eléctrico para ISO/IEC categoría 7. Las versiones de 2 y 4 pares deben utilizar diseño de cuadrante blindado para aislar completamente las partes. Proporcionar una instalación rápida y fácil con una sola herramienta para preparar y terminar los cables. Las versiones de 2 y 4 pares deben exceder los requerimientos ISO/IEC 11801.		

	Permitir la combinación de los conectores de 2 pares y 4 pares a ser utilizados en conjunto con otras aplicaciones de múltiple soporte desde una salida de 4 pares. Compatible con cables S/FTP sólidos 22 awg o 23 awg. Deben ser certificadas por Underwriters Laboratories bajo los Estándares, estadounidenses y los Estándares de telecomunicaciones canadienses C22.2. Es requisito obligatorio anexar el certificado UL para validación. Se debe tener la posibilidad de patch cords de longitudes desde 1 metro hasta 10 metros dependiendo la ubicación del terminal IP y del mobiliario. Tener disponible una versión de patch cord de 4 pares conector estándar rectangular en un extremo con una conexión de tipo RJ45 blindada en el otro extremo. Tener disponible una versión de patch cord de 2 pares conector estándar rectangular en un extremo con una conexión de tipo RJ45 blindada en el otro extremo. Tener disponible una versión de patch cord de 1 par para soportar aplicaciones de voz y fax. Los patch cords empleados en el área de trabajo serán los mismos a emplearse en el área de administración en los patch panels. Deben ser certificadas por Underwriters Laboratories bajo los Estándares Estadounidenses y los Estándares de telecomunicaciones canadienses C22.2. Es requisito obligatorio anexar el certificado UL para validación. Las interfaces utilizadas en los plugs deben cumplir con la ISO/IEC 11801. Cable de fibra troncal de 6 hilos om4 con armadura cubierta LS0H de 60, 70 y 80 metros. Cantidad: 2 (dos) de 80 metros, 3 (tres) de 70 metros, 2 (dos) de 60 metros. 4 (cuatro) de 10 metros. Fibra OM4 50/125 Uso Indoor ChaquetaLSO-3C, Color Aqua Conectores tipo LC 2.0 mm Max Insertion Loss (dB): 0,25 Min Return Loss (dB): 30 Cable Diameter [para 6 hilos] mm (in.): 3.0 (0.12) Min Bend Radius Operational [para 6 hilos] mm (in.): 30 (1.2) Max Pulling Eye Diameter [para 6 hilos] mm (in.): 44.5 (1.75) Estandar: IEC60793-2-10 A1a.3 Medidas [Metros]: 60, 70, 80, 10 Debe ser de la misma marca del cableado estructurado.		

	Cable de fibra optica con armadura OM4 de 4 y 6 hilos. Cantidad: 1 (Uno) de 4 hilos 500 metros, 1 (Uno) de 6 hilos 200 metros. **4 hilos y 6 hilos.** FO OM4 50/125µm • Tipo tubo suelto • Con Armadura Metálica • Chaqueta tipo MDPE (Polietileno de media densida) • CUMPLIMIENTO DE ESTANDARES • ISO/IEC 11801:2002 Enmienda 2 OM4 • IEC 60794-3-10 • ANSI/TIA-568.3-D • ANSI/TIA-598-D • ANSI/TIA-492 AAAD • IEC 60793-2-10 Tipo de fibra A1a.3 • Telcordia GR-20-CORE • Atenuación máxima (dB/km) 850nm: 3.0 / 1300nm: 1.0 • Tensión máxima de tracción [Newtons] • Instalación : 2700 • A largo plazo : 810 • Temperatura de Operación °C (°F): -30 to 60 (-22 to 140) • Temperatura de instalación °C (°F): -10 to 60 (-14 to 140) • Radio de curvatura mínimo • Instalación: 20 x diámetro • A largo plazo: 10 x diámetro. Debe ser de la misma marca del cableado estructurado. Instalación Cable troncal de cobre cat 6a cubierta LS0H de 6 cables cada uno con jacks rj45 en los extremos. Cantidad: 4 (cuatro). • Se requiere que este ensamblado en fábrica y verificado 100% en su transmisión con analizadores de red grado laboratorio para un desempeño apropiado hasta 500 MHz. • Se requiere que sea compatible retroactivamente con categorías inferiores. • Se requieren que estén terminados y probados en fábrica con módulos apantallados categoría 6A para área de trabajo, panel de parcheo o conectores modulares (plugs) de 8 posiciones. • Se requiere tener en cada extremo los cables individuales etiquetados e identificados para una correcta orientación de salidas. • Se requiere tener un patrón único en corte recto que optimice la orientación del cable, independientemente del lado desde donde se alimente, limitando el cruce de cables. • Se requiere que longitud de 8 metros. • Se requiere que cada cable del ensamble tenga una etiqueta con identificación única para efectos de administración. Se requiere utilizar una cubierta exterior continuo que envuelva y proteja totalmente el conjunto de cables y que tenga la misma clasificación que sus cables individuales la cual puede ser CMR, CMP o LS0H. • Se requiere que estén construidos con cables de par trenzado balanceado categoría 6A F/UTP (blindado) de cuatro pares con las siguientes especificaciones: • Se requiere que estén construidos en total conformidad con las normas IEC 61156-5, ANSI/TIA-568-C.2 e ISO/IEC 11801 Ed. 2 o sus más recientes versiones para categoría 6A/Clase EA. • Se requiere que tenga un forro de cable de forma cilíndrica libre de plomo disponible en opciones LSOH, CMR y CMP, con un diámetro externo nominal menor o igual a 6.9 mm y que cumplen con las siguientes normas:		

	○ LS0H: IEC 60754, IEC 61034 e IEC 60332-3C ○ CMR: UL y CSA FT4 ○ CMP: UL y CSA FT6 • Se requiere que tenga una construcción consistente en cuatro pares de conductores de cobre sólido de 0.58 mm (0.023 in) (23 AWG) de diámetro, con un elemento aislador central que mantenga la geometría de par para un desempeño óptimo en NEXT. • Se requiere que tenga una película de celofán que rodee todo el conjunto de los pares del cable, un alambre de drenado y una pantalla de aluminio rodeando todo el conjunto que virtualmente elimina el acoplamiento de alien crosstalk. • Se requiere que cumpla con los siguientes parámetros de desempeño: **TRANSMISSION PERFORMANCE** GUARANTEED WORST CASE SIEMON TYPICAL Se requiere que sea de la misma marca del cableado estructurado.		
	Punto de Red de area de usuarios. Los faceplates deben tener capacidad para alojar módulos de adaptadores RJ45, conectores de fibra óptica SFF, RCA, tomas cat7A/ o conectores tipo F. También deben tener porta etiquetas con protector transparente de acrílico. Los faceplates deberán estar disponibles en configuración de uso vertical y en configuración de uso horizontal. Se deberán ofrecer adaptador angulado por cada face plate ofertado. Deberán estar disponibles en varios colores. Los faceplates deben tener capacidad para alojar los outlets propuestos, y categoría 7A. También deben tener porta etiquetas con protector transparente de acrílico. Los faceplates deberán ser de tipo piramidal, con el fin de proporcionar cuidados en los radios mínimos de curvatura del cable. Los Faceplates permitirán la instalación de extender la profundidad a través de adaptadores angulados para uno o dos puertos. Deberán ser compatibles con el troquelado de las canalizaciones de mobiliario, no se permitirá modificaciones de las áreas de las canalizaciones de los muebles. Deben ser de la misma marca de la conectividad propuesta. FacePlate de 1 Orificio (960 unidades). Adaptador Angulado de 1P para faceplate (550 unidades) Adaptador Angulado de 2P para faceplate (205 unidades) Conector / Jack tera (1920 unidades) Las versiones de 2 y 4 pares deben exceder las especificaciones de desempeño eléctrico ISO/IEC Clase FA/Categoría 7 A.	Servicio de instalación de cableado estructurado para los puestos de trabajo de todo el personal del Comando Conjunto de las Fuerzas Armadas que permita mitigar los problemas existentes de conectividad y seguridad que existen desde hace varios años.	CONFORME
	El servicio de mantenimiento de racks de comunicaciones deben considerar todos los componentes para la correcta instalación de Gabinetes de piso de 42 U con profundidad de 1.2metros y 80cm de ancho. Cantidad: 11 (Once). Con profundidad de 1.0metros y 80cm de ancho. Color negro. 71% de porcentaje de perforación en puertas.	Servicio de instalación de componentes para el cableado estructurado de los ambientes de racks de comunicaciones del edificio que permitan mantener disponibilidad de	CONFORME

Frequency (MHz)	Insertion Loss (dB)		NEXT (dB)		PS NEXT (dB)		ACR (dB)		PSACR (dB)		ACR-F (dB)		PS ACR-F (dB)		Return Loss (dB)		Propagation Delay (ns)	
1.0	2.1	1.8	75.3	86.0	73.3	82.3	73.2	84.2	71.2	80.5	73.3	91.0	71.3	85.0	20.0	33.0	570	570
4.0	3.8	3.4	66.3	77.0	64.3	73.3	62.5	73.6	60.5	69.9	61.3	79.0	59.3	73.0	23.0	35.5	552	552
10.0	5.9	5.4	60.3	71.0	58.3	67.3	54.4	65.6	52.4	61.9	53.3	71.0	51.3	65.0	25.0	38.0	545	545
16.0	7.5	6.9	57.2	68.0	55.2	64.2	49.8	61.1	47.8	57.3	49.2	67.0	47.2	61.0	25.0	35.2	543	543
20.0	8.4	7.7	55.8	67.0	53.8	62.8	47.4	59.3	45.4	55.1	47.3	65.0	45.3	59.0	25.0	35.0	542	542
31.25	10.5	9.9	52.9	64.0	50.9	59.9	42.4	54.1	40.4	50.0	43.4	61.0	41.4	55.0	23.6	33.1	540	540.4
62.5	15.0	14.3	48.4	59.0	46.4	55.4	33.4	44.7	31.4	41.1	37.4	55.0	35.4	49.0	21.5	32.2	539	538.6
100.0	19.1	18.1	45.3	56.0	43.3	52.0	26.2	37.9	24.2	33.9	33.3	51.0	31.3	45.0	20.1	31.6	538	537.6
200.0	27.6	27.3	40.8	52.0	38.8	47.8	13.2	24.7	11.2	20.5	27.3	45.0	25.3	39.0	18.0	29.8	537	536.5
250.0	31.1	31.1	39.3	50.0	37.3	46.0	8.3	18.9	6.3	14.9	25.3	43.0	23.3	37.0	17.3	28.7	536	536.3
300.0	34.3	35.0	38.1	49.0	36.1	45.0	3.9	14.0	-1.9	10.0	23.8	38.0	21.8	35.0	17.3	28.0	536	536.1
400.0	40.1	40.0	36.3	47.0	34.3	43.0	-3.8	7.0	-5.8	3.0	21.3	36.0	19.3	33.0	17.3	27.1	536	535.8
500.0	45.3	42.0	34.8	47.0	32.8	42.0	-10.4	5.0	-12.4	0.0	19.3	34.0	17.3	32.0	17.3	26.0	536	535.6
550.0*	-	43.0	-	46.0	-	42.0	-	3.0	-	-1.0	-	33.0	-	31.0	-	26.0	536	-
625.0*	-	44.9	-	46.0	-	41.0	-	1.1	-	-3.9	-	33.0	-	29.0	-	25.0	535	-
750.0*	-	49.0	-	45.0	-	41.0	-	-4.0	-	-8.0	-	32.0	-	27.0	-	25.0	535	-

*Performance for frequencies beyond TIA requirements are for information only.

All performance based on 100 meters (328 ft.)

<table>
<tr>
<td></td>
<td>Cumplimiento de estándares: EIA/ECA-310-E, IP20.
Organizador de Cable 28 (veinte y ocho) unidades, 42U 6 pulgadas.
Accesorio de soporte para PDU 6 (seis) unidades.
Tapa ciega de 1 U, 30 (treinta) unidades.
Barra de aterramiento de tierra 11 (once) unidades.
El gabinete y sus accesorios deben ser de la misma marca del cableado estructurado.</td>
<td>conectividad para todos los pisos y usuarios del comando conjunto de las fuerzas armadas.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Prueba del canal de cable de cobre.
Todas las pruebas de campo de la Categoría 7 A /Clase Fa deben ser realizadas con un dispositivo aprobado de prueba de campo de par trenzado balanceado bajo IEC 61935 y/o aprobados por el fabricante de cableado estructurado.

Todos los canales instalados de la Categoría 7 A /Clase Fa deben funcionar igual o mejor que los requerimientos mínimos especificados en la tabla a continuación:

<table>
<tr><th>Parámetro</th><th>1000 MHz</th></tr>
<tr><td>Pérdida de inserción (Máximo)</td><td>67.6 dB</td></tr>
<tr><td>Pérdida NEXT (Mínimo)</td><td>47.9 dB</td></tr>
<tr><td>PS NEXT(Mínimo)</td><td>44.9 dB</td></tr>
<tr><td>ACR (Mínimo)</td><td>-19.6 dB</td></tr>
<tr><td>PS ACR (Mínimo)</td><td>-22.6 dB</td></tr>
<tr><td>ELFEXT (Mínimo)</td><td>27.4dB</td></tr>
<tr><td>PS ELFEXT (Mínimo)</td><td>24.4 dB</td></tr>
<tr><td>Pérdida del retorno (Mínimo)</td><td>6.0 dB</td></tr>
<tr><td>Retardo de Prop (Mínimo)</td><td>545 ns</td></tr>
<tr><td>Retardo de sesgo (Mínimo)</td><td>30 ns</td></tr>
</table>

Todos los cables de backbone de par trenzado balanceado que excedan 90 m (295 ft) o 100 m (328 ft) deben ser probados al 100% por continuidad si no se requieren aseguramiento de las aplicaciones.

Los cables horizontales y de backbone de par trenzado balanceado Categoría 7 A /Clase Fa, cuya longitud no exceda 90 m (295 ft) para el enlace básico y 100 m (328 ft) para el canal serán probados al 100 por ciento de acuerdo con ISO/IEC 11801: Los parámetros de prueba incluyen el mapa de cables más la continuidad del blindaje SFTP (cuando esté presente), pérdida de inserción, longitud, pérdida NEXT (par a par), pérdida NEXT (sumatoria de potencias), pérdida ELFEXT (par a par), pérdida ELFEXT (sumatoria de potencias), pérdida del retorno, pérdida de inserción, demora de la propagación y lapso de inclinación.</td>
<td>El servicio de instalación de cableado estructurado debe considerar también las debidas pruebas de funcionamiento adecuado, cumpliendo con los parámetros que mandan las normativas de tecnología, así como las mejores prácticas y consideraciones que se deben tomar en cuenta para que un servicio de instalación cumpla con éxito el objetivo principal del Comando Conjunto de las Fuerzas Armadas.</td>
<td>CONFORME</td>
</tr>
</table>

	Criterios de equipo de prueba: Todos los probadores de campo de par trenzado balanceado deben ser calibrados en fábrica cada año calendario por el fabricante del equipo de prueba de campo, tal como se estipula en los manuales suministrados con la unidad de prueba de campo. Antes del comienzo de la prueba se debe proporcionar el certificado de calibración para revisión. Las configuraciones de auto-prueba proporcionadas en este probador de prueba de campo deben estar configuradas en los parámetros predeterminados. Las configuraciones de la prueba seleccionadas de las opciones suministradas en los probadores de prueba deben ser compatibles con el cable instalado bajo prueba. **Pruebas de fibra óptica:** Los cables horizontales de fibra deben ser probados al 100% por pérdida de inserción y longitud. La pérdida de inserción debe ser probadas a 850 nm y 1300 nm para cableado multimodo de 50/125µm y 62.5/125µm por lo menos en una dirección usando el procedimiento de prueba Método B (1-jumper) tal como se especifica en los procedimientos descritos por el fabricante. La longitud debe ser probada usando un dispositivo de medición de prueba óptica OLTS.		
	Administración y documentación para el proyecto: Los cables horizontales y de backbone deben estar etiquetados en cada extremo. El cable o su etiqueta deben estar marcados con su identificador. En cada placa frontal se debe marcar un identificador único que la identifique como hardware de conexión. Cada puerto en la placa frontal debe estar etiquetado con su identificador. En cada pieza del hardware de conexión se debe marcar un identificador único para identificarlo como hardware de conexión. Cada puerto en el hardware de conexión debe ser etiquetado con su identificador. Se deberán marcar las canalizaciones, espacios de telecomunicaciones, Fire Stops, Gabinetes en la parte frontal y posterior cada elemento con su identificador único. Los identificadores se revisarán en conformidad con los requisitos de la entidad, así mismo se deberá marcar en conformidad con el estándar ISO 14763-2.1 ó ANSI/TIA 606B.		CONFORME

TERCERA: LIQUIDACIÓN ECONÓMICA

Ord.	Detalle	Valor
1	Valor del contrato	$593.125,00
2	Valor del 12% del IVA	$71.175,00
3	Valor total	$664.300,00
4	(-) Valor amortizado (anticipo)	$415.187,50
5	Valor a cancelar	$177.187,50

CUARTO: LIQUIDACIÓN DE PLAZOS

El plazo para la entrega del proyecto a entera satisfacción del CONTRATANTE es de (89) días calendarios, contados a partir de la firma del contrato, más la prórroga otorgada hasta por (45) días.

Fecha de firma de contrato	03-10-2022
Plazo	89 días
Fecha de finalización del plazo	31-12-2022
Fecha de otorgamiento hasta 45 días de prorroga adicional	31-12-2022

Fecha de finalización de la prorroga	14-02-2022
Fecha efectiva de entrega del proyecto	15-02-2022

Es necesario señalar que a pesar que se excede con un día el plazo para la entrega del proyecto, no se cobró multa por el mismo, en vista que oficio Nro. CCFFAA-DAJ-2023-0085-O de fecha 15 de febrero del año en curso, se entrega el criterio jurídico para el cambio de los cables solicitados con oficio Nro. OFIC-017-2023 del 08 de febrero del 2023; adicional en el último párrafo del mismo oficio se señala lo siguiente *"Respecto a la autorización de ampliación del plazo para la entrega de los bienes objeto de esta contratación; no se deberá contabilizar el tiempo para el pronunciamiento jurídico y elaboración del informe de la administración, así como de la comisión de recepción del objeto de este contrato como mora, toda vez que el mismo se suspende hasta la aceptación expresa por parte de la administración para receptar los bienes objeto de este contrato.".*

En tal virtud el contratista cumplió con la ejecución del objeto del contrato dentro del plazo establecido, de conformidad con el artículo 319 del Reglamento General de la Ley Orgánica del Sistema Nacional de Contratación Pública.

QUINTO: CONSTANCIA DE LA RECEPCIÓN

Las personas que intervienen en la presente entrega-recepción del proyecto referente a "LA ADQUISICIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA E INSTALACIÓN DEL CABLEADO ESTRUCTURADO DEL COMANDO CONJUNTO DE LAS FUERZAS ARMADAS", el 15 del mes de febrero del 2023, verificado por lo antes indicado, procedieron a las firmas de la acta de recepción con lo que se resuelve dar por recibido a entera satisfacción el proyecto.

Para constancia de lo actuado y en fe de aceptación, suscriben la presente Acta de Entrega-Recepción en un (1) Original y dos (2) copias de igual tenor y valor.

Firmado electrónicamente por:
SILVIA JUDIT BUILA ROSERO

Silvia Buila Rosero
Sgos-IF
TÉCNICO NO-INTERVINIENTE

Firmado electrónicamente por:
DARIO JAVIER GARCES VELASTEGUI

Dario Garces Velastegui
Cbos. Téc. Avc.
TÉCNICO DELEGADO

Firmado electrónicamente por:
JOSE FABRICIO MUNOZ SANCHEZ

José Fabricio Muñoz
Capt. Téc. Avc.
ADMINISTRADOR DEL CONTRATO

Firmado electrónicamente por:
CARLOS ENRIQUE ROMERO RACINES

Carlos Romero Racines
RUC. 1791710568001
REPRESENTANTE LEGAL
CONSTECOIN CIA LTDA.

Firmado electrónicamente por:
CARLOS ENRIQUE ROMERO RACIÑES