

MANTENIMIENTO Y SOPORTE PARA LA CAPACIDAD DE
PROTECCION CONTRA ATAQUE DE DENEGACION DE
SERVICIO DDOS No. JEMPP-CEDE6-DIPCO-ET-05732/COM-00



ESPECIFICACIÓN TÉCNICA

DIRECCIÓN DE ESTRUCTURACIÓN TÉCNICA

DEPARTAMENTO DE LOGÍSTICA

CEDE 4

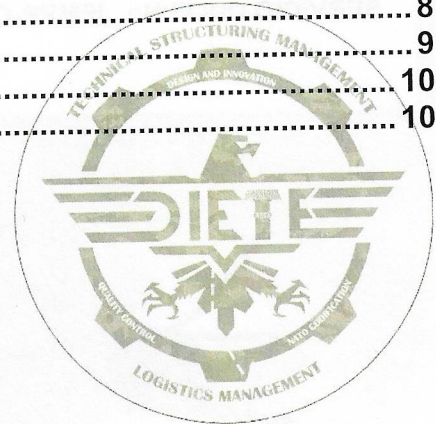


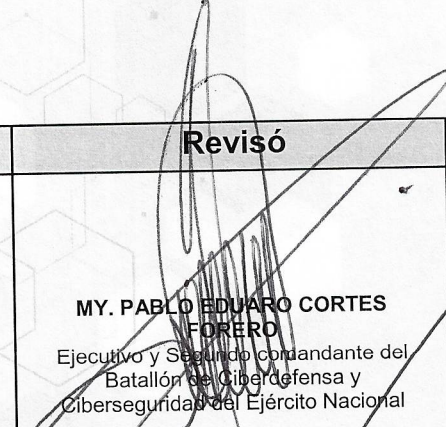
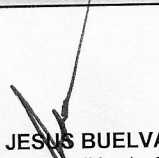
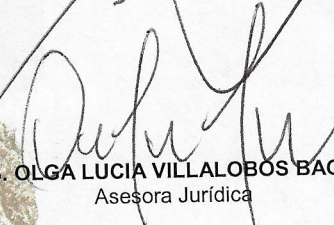
ORGANIZACIÓN - DISCIPLINA - PUNTUALIDAD

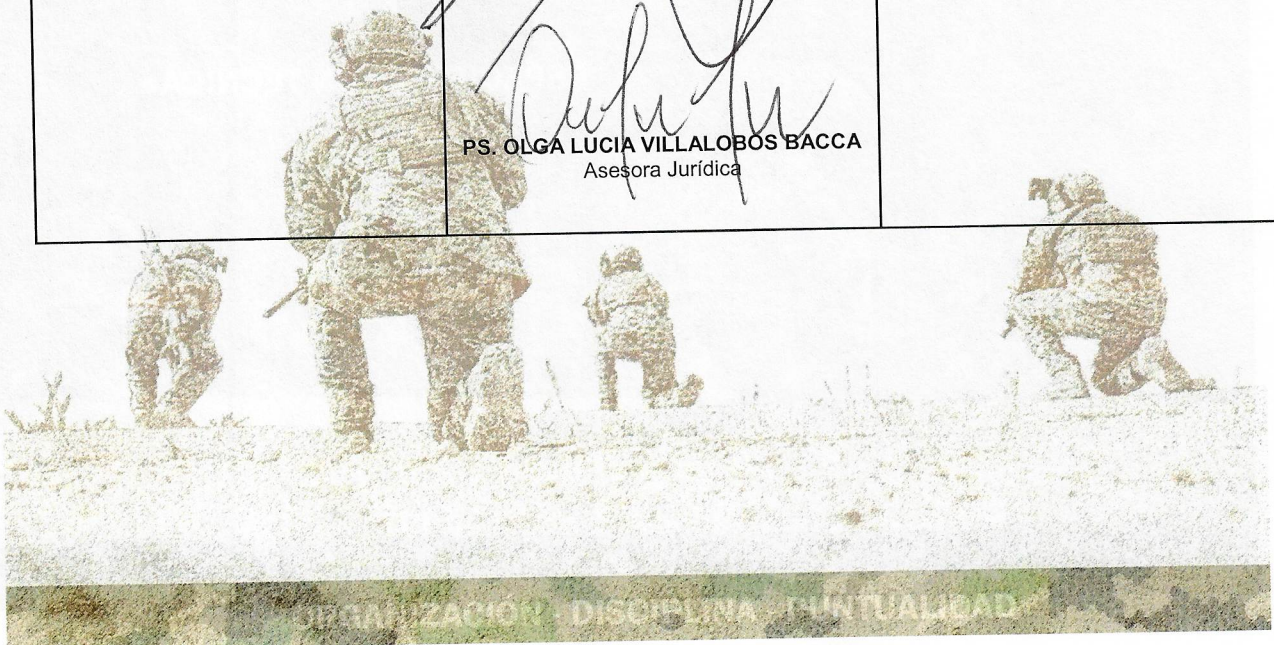


CONTENIDO

1. OBJETO	3
2. DEFINICIONES Y APLICACIÓN	3
5. MÉTODOS DE ENSAYO	8
6. APÉNDICE	9
7. ANEXOS	10
8. CONTROL DE REVISIONES.....	10



Elaboró	Revisó	Aprobó
 SS. JORGE IVAN NEGRETE ANAYA Analista Seguridad Perimetral	 MY. PABLO EDUARDO CORTES FORERO Ejecutivo y Segundo comandante del Batallón de Ciberdefensa y Ciberseguridad del Ejército Nacional	 TC. ROGER JESUS BUELVAS NARVAEZ Comandante del Batallón de Ciberdefensa y Ciberseguridad del Ejército Nacional.
	 PS. OLGA LUCIA VILLALOBOS BACCA Asesora Jurídica	





1. OBJETO

La presente especificación técnica tiene por objeto establecer los requisitos técnicos para el mantenimiento y soporte para la capacidad de protección contra ataque de denegación de servicio Distribuido DDoS del Ejército Nacional para el fortalecimiento de los medios cibernéticos.

2. DEFINICIONES Y APLICACIÓN

2.1 DEFINICIONES

- **Aplicación Web:** Aplicación o herramienta informática accesible desde cualquier navegador, bien sea a través de internet (lo habitual) o bien a través de una red local.
- **APTs:** Una amenaza persistente avanzada, también conocida por sus siglas en inglés, APT (por Advanced Persistent Threat), es un conjunto de procesos informáticos sigilosos y continuos, a menudo orquestados por humanos, dirigidos a penetrar la seguridad informática de una entidad específica. Una APT, generalmente, fija sus objetivos en organizaciones o naciones por motivos de negocios o políticos.
- **Ataque de denegación de servicios:** También llamado ataque DoS (de las siglas en inglés Denial of Service) o DDoS (de Distributed Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.
- **Botnets:** es un término que hace referencia a un conjunto o red de robots informáticos o bots, que se ejecutan de manera autónoma y automática. El artífice de la botnet puede controlar todos los ordenadores/servidores infectados de forma remota.
- **Ciberterrorismo:** Es el uso de medios de tecnologías de información, comunicación, informática, electrónica o similar con el propósito de generar terror o miedo generalizado en una población, clase dirigente o gobierno, causando con ello una violación a la libre voluntad de las personas.
- **Filtrado de contenido:** Es un equipo que nos permite bloquear el contenido no deseado de páginas Web, restringe el acceso a páginas de entretenimiento, compras, y páginas de chat entre otras, también bloquea los mensajeros instantáneos (programas para chatear o comunicarse con los amigos o la familia en línea) y por último también deniega y evita los programas de descarga, inclusive llamados p2p como por ejemplo: música, videos, la mayoría con contenido pornográfico, programas pirata y un alto contenido de virus.
- **Hacktivismo:** (un acrónimo de hacker y activismo) se entiende normalmente "la utilización no-violenta de herramientas digitales ilegales o legalmente ambiguas persiguiendo fines políticos.



MANTENIMIENTO Y SOPORTE PARA LA CAPACIDAD DE PROTECCIÓN CONTRA ATAQUE DE DENEGACIÓN DE SERVICIO
DDOS No. JEMPP-CEDE6-DIPCO-ET-05732/COM-00

- **Sistema de protección de intrusos (IPS):** Control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.
- **Update:** hace referencia al cambio de un hardware, software, firmware para una versión mejor o más reciente con el fin de obtener más funciones útiles o mejorar los sistemas existentes.
- **Upgrade:** hace referencia al cambio de un hardware, software, firmware para una versión mejor o más reciente con el fin de obtener más funciones útiles o mejorar los sistemas existentes.

2.2 APLICACIÓN

El Ejército Nacional a través de su Red Nacional de Datos brinda servicios Informáticos desde el Comando de la Institución de forma centralizada, los cuales se encuentran públicos en la web, pueden ser consultados desde cualquier dispositivo tecnológico con acceso a internet; por tal razón es fundamental garantizar la operatividad de las herramientas y plataformas que brindan protección ante intrusos, con el fin de evitar denegación de servicios distribuidos y así evitar caídas en los servicios críticos a nivel web del Ejército Nacional y a nivel nacional para todas las Unidades Militares conectadas en la Red institucional.

3. REQUISITOS

Fortalecer el área de Ciberdefensa, manteniendo la operatividad de la plataforma garantizando la continuidad de los servicios con el fin de Proteger la infraestructura tecnológica del Ejército Nacional, contra ataques de denegación de servicios evitando caídas a nivel de red en el Comando del Ejército y a nivel nacional para todas las Unidades Militares conectadas en la red institucional, garantizando el cumplimiento de la misión institucional y el cumplimiento de la Resolución 7870 de 2022 del Ministerio de Defensa Nacional, la cual propende por la seguridad, disponibilidad y confidencialidad de la información del sector Defensa.

3.1 REQUISITOS GENERALES

La presente especificación técnica tiene como objetivo el mantenimiento y soporte capacidad de protección contra ataque de denegación de servicio Distribuido DDoS del Ejército Nacional, con el fin de realizar el servicio de soporte técnico, monitoreo, administración y operación, para la totalidad de los equipos activos.

ITEM	DESCRIPCION
3.1.1	Soporte Nivel 1: Mantenimiento y Soporte Técnico de la Capacidad de Protección Contra Ataque de Denegación De Servicio Distribuido DDoS del Ejército Nacional de manera presencial.



MANTENIMIENTO Y SOPORTE PARA LA CAPACIDAD DE PROTECCIÓN CONTRA ATAQUE DE DENEGACIÓN DE SERVICIO
DDoS No. JEMPP-CEDE6-DIPCO-ET-05732/COM-00

3.1.2	Soporte Nivel 2: Mantenimiento y Soporte Técnico de la Capacidad de Protección Contra Ataque de Denegación De Servicio Distribuido DDoS del Ejército Nacional de manera Remota.
3.1.3	SOPORTE TÉCNICO: El soporte técnico se debe brindar con una atención ilimitada a casos reportados por el Ejército Nacional, referentes a cualquier evento relacionado con el funcionamiento, administración e incidentes o eventos de seguridad de la capacidad de Protección Contra Ataque de Denegación De Servicio Distribuido DDoS. SOPORTE PROGRAMADO: El Soporte programado son aquellas tareas previamente planificadas y que el Batallón de Ciberdefensa y Ciberseguridad haya considerado necesario llevar a cabo fuera del horario establecido con el “SOPORTE DELEGADO PARA VISITAS”; por lo tanto, el proveedor debe adaptarse a los criterios y horarios (nocturnos, domingos y festivos) fijados por el Batallón de Ciberdefensa y Ciberseguridad. SOPORTE NO PROGRAMADO: Soporte no programado son todas aquellas tareas no planificadas (incidentes y/o eventos de seguridad) y fuera del horario establecido con el “SOPORTE DELEGADO PARA VISITAS”, por lo tanto, el proveedor debe adaptarse a los criterios y horarios (nocturnos, domingos y festivos) fijados por el Batallón de Ciberdefensa y Ciberseguridad.

3.2 REQUISITOS ESPECÍFICOS

3.2.1	SERVICIO DE MANTENIMIENTO:										
3.2.1.1	El Mantenimiento y Soporte para la Protección Contra Ataque de Denegación de Servicios Distribuido, deberá brindarse a los equipos que a continuación se relacionan. <table><tr><th>NOMBRE DE PRODUCTO</th><th>CODIGO PRODUCTO</th></tr><tr><td>DefensePro X40 - 20G/ODS-HT2p/96GB/DUAL</td><td>32408048</td></tr><tr><td>10Gbps Pluggable Optics Multimode SR for DefensePro</td><td>PQ8U030004 PQ8U030114 PQ8U030003 PQ8U030005</td></tr><tr><td>10Gbps Pluggable Optics Multimode SR for Bypass Switch</td><td>N5CAJTX N5CBOW0</td></tr><tr><td>Bypass Switch chassis for 10G/40G/100G bypass modules (12.5.2.2.0)</td><td>22A0A133240017</td></tr></table>	NOMBRE DE PRODUCTO	CODIGO PRODUCTO	DefensePro X40 - 20G/ODS-HT2p/96GB/DUAL	32408048	10Gbps Pluggable Optics Multimode SR for DefensePro	PQ8U030004 PQ8U030114 PQ8U030003 PQ8U030005	10Gbps Pluggable Optics Multimode SR for Bypass Switch	N5CAJTX N5CBOW0	Bypass Switch chassis for 10G/40G/100G bypass modules (12.5.2.2.0)	22A0A133240017
NOMBRE DE PRODUCTO	CODIGO PRODUCTO										
DefensePro X40 - 20G/ODS-HT2p/96GB/DUAL	32408048										
10Gbps Pluggable Optics Multimode SR for DefensePro	PQ8U030004 PQ8U030114 PQ8U030003 PQ8U030005										
10Gbps Pluggable Optics Multimode SR for Bypass Switch	N5CAJTX N5CBOW0										
Bypass Switch chassis for 10G/40G/100G bypass modules (12.5.2.2.0)	22A0A133240017										



MANTENIMIENTO Y SOPORTE PARA LA CAPACIDAD DE PROTECCIÓN CONTRA ATAQUE DE DENEGACIÓN DE SERVICIO
DDoS No. JEMPP-CEDE6-DIPCO-ET-05732/COM-00

		10 Gigabit fiber multimode SR bypass switch module, 2 bypass segments	20031B245230071
		Standard Support for DefensePro X40 - 20G	1920070285S
		Standard Support for 10Gbps Pluggable Optics Multimode SR for DefensePro	9060000042S
		Cyber Controller X 40 Gbps attack capacity	9000000322Y1
		Network Protection Gold Subscription for DefensePro X40 - 20G	9006000523
		Standard Support for Bypass Switch chassis for 10G/40G/100G bypass modules	9080000006S
		Standard Support for 10 Gigabit fiber multimode SR bypass switch module, 2 bypass segment	9080000007S
		Standard Support for 10Gbps Pluggable Optics Multimode SR for Bypass Switch	9060000063S
3.2.2	SERVICIO DE SOPORTE		
3.2.2.1	Se requiere que el servicio de soporte realice la administración de la plataforma DDoS, el cual será responsable de las tareas de comprobación de funcionamiento, administración, gestión y control. El servicio de soporte tendrá que monitorear el funcionamiento de la plataforma, con el fin de identificar comportamientos anormales dentro del sistema, lo cual será informado al funcionario designado por el Ejército Nacional. El soporte se encargará de hacer la revisión, control y mantenimiento de la estabilidad y operación de la plataforma. El soporte incluirá la configuración de políticas, evaluación y ajuste de la configuración de políticas de seguridad, implantadas en la plataforma, bajo la supervisión del personal designado por el Ejército Nacional. El soporte estará encargado de atender las solicitudes donde evaluará y ejecutará nuevos requerimientos de configuración sobre la plataforma con la finalidad de blindar la infraestructura tecnológica institucional ante cualquier intento de intrusión. El administrador de DDoS e IPS será el responsable de verificar que las herramientas descritas en el ítem 3.2.1.1 de este documento se encuentren en regla y actualizadas con los correspondientes soportes y mantenimientos ejecutados por el proveedor del contrato de soporte y mantenimiento. El soporte incluirá el seguimiento de Backups con el fin de Gestionar y efectuar las copias de resguardo (back-up) de la información de las herramientas de seguridad DDoS. El soporte deberá efectuar la generación de reportes periódicos sobre las actividades realizadas de acuerdo a la necesidades del funcionario designado por el Ejército Nacional y realizará la entrega de los informes correspondientes. El soporte realizará la instalación de nuevas versiones y/o parches de seguridad de la solución DDoS, avalados por el fabricante. El soporte brindará el Apoyo técnico en la implementación de IPV6 en caso de requerirse para la solución durante la ejecución del contrato.		



MANTENIMIENTO Y SOPORTE PARA LA CAPACIDAD DE PROTECCIÓN CONTRA ATAQUE DE DENEGACIÓN DE SERVICIO
DDOS No. JEMPP-CEDE6-DIPCO-ET-05732/COM-00

	En caso de presentarse una falla en la herramienta de seguridad DDoS e IPS fuera del horario del personal en sitio, el soporte deberá prestarse de forma remota y/o en sitio, en cualquier horario, fines de semana y festivos o desplazarse al sitio si este así se requiere, donde se encuentre la herramienta de seguridad, en los tiempos de respuesta indicados, así mismo dar solución al inconveniente, hasta dejar en correcto funcionamiento la misma.
	El soporte debe brindar atención ilimitada a casos reportados por el Ejército Nacional referentes a cualquier evento y/o incidente de seguridad relacionado con el funcionamiento, administración de la plataforma de seguridad DDoS e IPS fuera del horario del soporte del personal en sitio, para prestar el soporte de forma remota en cualquier horario fines de semana y festivos o desplazarse al sitio si este así lo requiere, donde se encuentre la herramienta de seguridad, en los tiempos de respuesta indicados, así mismo dar solución al inconveniente, hasta dejar en correcto funcionamiento la misma.
3.2.3	ALCANCE MANTENIMIENTO PREVENTIVO:
3.2.3.1	El mantenimiento se debe efectuar mínimo un (01) vez de forma preventiva durante la ejecución del contrato según cronograma acordado entre las partes a las plataformas de seguridad informática descritas en el punto 3.2.1.1. Este mantenimiento debe incluir como mínimo las siguientes actividades: • Actualizaciones de software (Upgrade, Update, críticas de seguridad). • Revisiones del funcionamiento de las plataformas y solución de errores. • Realización y programación de copias de seguridad. • Revisión de los logs de eventos registrados en los sistemas. • Revisión y mejoramiento de espacio de disco, utilización de CPU – RAM y afinamiento de servidores. • Evaluación de los sistemas de seguridad instalados. • Configuración de funcionalidades inoperativas. • Emisión de recomendaciones de las plataformas a través de un informe técnico, al supervisor del contrato. Nota: El contratista deberá suministrar el recurso de este mantenimiento en sitio o donde se requiera, así mismo con previa coordinación se podrán realizar de manera remota, pero si algo falla y no se puede subsanar el contratista desplazará al personal especializado hasta el sitio hasta su correcto funcionamiento.
3.2.4	ALCANCE MANTENIMIENTO CORRECTIVO:
3.2.4.1	En caso de presentarse fallas en los sistemas de seguridad descritos en el ítem 3.2.1.1, el contratista deberá efectuar los mantenimientos correctivos todas las veces que se requiera. Estos mantenimientos deben incluir como mínimo: • Instalación de software • Configuraciones, puesta en producción y funcionamiento del aplicativo y/o herramienta de seguridad

V



MANTENIMIENTO Y SOPORTE PARA LA CAPACIDAD DE PROTECCIÓN CONTRA ATAQUE DE DENEGACIÓN DE SERVICIO
DDOS No. JEMPP-CEDE6-DIPCO-ET-05732/COM-00

- Reemplazo de equipos por otro de iguales o superiores características de forma temporal hasta que la falla sea solucionada.

3.3 REQUISITOS DE EMPAQUE Y ROTULADO

3.3.1 Empaque.

OMITIDO

3.3.2 Rotulado.

OMITIDO

4. TOMA DE MUESTRAS Y CRITERIO DE ACEPTACIÓN O RECHAZO:

4.1 TOMA DE MUESTRAS Y CRITERIO DE ACEPTACIÓN O RECHAZO PARA EVALUAR LOS REQUISITOS GENERALES Y REQUISITOS DE EMPAQUE Y ROTULADO

OMITIDO.

4.1.1 Muestreo.

OMITIDO

4.1.2 Criterios de aceptación o rechazo para requisitos generales y requisitos de empaque y rotulado.

OMITIDO

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

OMITIDO

4.2.1 Muestreo.

OMITIDO

4.2.2 Criterio de aceptación o rechazo para evaluar requisitos específicos.

OMITIDO

5. MÉTODOS DE ENSAYO

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



OMITIDO

6. APÉNDICE

6.1 NORMAS QUE DEBEN CONSULTARSE

1. Constitución Política de Colombia.
2. Código Civil.
3. Código General del Proceso.
4. Código de Comercio.
5. Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
6. Ley 80 de 1993 "Por la cual se expide el Estatuto General de Contratación de la Administración Pública" y las demás normas que la modifiquen o aclaren.
7. Ley 1150 de 2007 "Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos" y las demás normas que la modifiquen o aclaren.
8. Ley 816 de 2003 "Por medio de la cual se apoya a la industria nacional a través de la contratación pública" y las demás normas que la modifiquen o aclaren.
9. Ley 1474 de 2011 "Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública" y las demás normas que la modifiquen o aclaren.
10. Ley 1341 de 2009 "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones" y las demás normas que la modifiquen o aclaren.
11. Decreto Ley 19 de 2012 "Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública" y las demás normas que lo modifiquen o aclaren.
12. Ley 1712 de 2014 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones" y las demás normas que la modifiquen o aclaren.
13. Decreto 1082 de 2015 "por medio del cual se expide el Decreto Único Reglamentario del sector Administrativo de Planeación Nacional" y las demás normas que lo modifiquen o aclaren.



MANTENIMIENTO Y SOPORTE PARA LA CAPACIDAD DE PROTECCIÓN CONTRA ATAQUE DE DENEGACIÓN DE SERVICIO
DDOS No. JEMPP-CEDE6-DIPCO-ET-05732/COM-00

14. Decreto 103 del 20 de enero de 2015 “Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones” y las demás normas que lo modifiquen o aclaren.
15. Resolución de delegación 4519 del 27 de mayo de 2016 “Por la cual se delegan unas funciones y competencias relacionadas con la contratación de bienes y servicios con destino al Ministerio de Defensa Nacional, a las Fuerzas Militares y la Policía Nacional y se dictan otras disposiciones” y las demás normas que la modifiquen o aclaren.
16. Resolución No. 4130 del 16 de junio de 2022 “MANUAL DE CONTRATACIÓN Y DE CONVENIOS” del Ministerio de Defensa Nacional y las demás normas que la modifiquen o aclaren.
17. Resolución 2710 del 03 de octubre de 2017 del Ministerio de Tecnologías de la Información y las Comunicaciones “Por la cual se establecen lineamientos para la adopción del protocolo IPv6” y las demás normas que la modifiquen o aclaren.
18. Directiva de Seguridad de la Información del Ministerio de Defensa 2014-18 “Lineamiento de seguridad de la información para sector defensa” y las demás normas que la modifiquen o aclaren.
19. Directiva permanente 00201 de 2017 “Lineamiento de ciberseguridad y Ciberdefensa para el Ejército Nacional” y las demás normas que la modifiquen o aclaren.
20. Directiva permanente 00221 de 2017 “Seguridad de la información para el Ejército Nacional” y las demás normas que la modifiquen o aclaren.

6.2 ANTECEDENTES

MANTENIMIENTO Y SOPORTE TECNICO DE LA PLATAFORMA DDOS E IPS – BACCI No. JEMPP-CEDE6-BACCI-ET-01487/ COMUN-02, con oficio 2025574003742973 se solicitó su derogación.

7. ANEXOS

OMITIDO

8. CONTROL DE REVISIONES

Debe contener un cuadro de control de revisiones Cada Especificación Técnica debe llevar un registro denominado control de revisiones el cual permite asegurar que se identifiquen los cambios realizados y el estado de revisión actual del documento.

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

10/10/22

V



visión y/o Actualización	Modificaciones	Fecha
00	Creación de la especificación técnica mantenimiento y soporte para la capacidad de protección contra ataque de denegación de servicio DDOS No. JEMPP-CEDE6-DIPCO-ET-05732/COM-00. Creación de la especificación técnica mantenimiento y soporte para la capacidad de protección contra ataque de denegación de servicio DDOS No. JEMPP-CEDE6-DIPCO-ET-05732/COM-00 con base a estudio de mercado con oficio 2025574000698653 – radicado N° 2025574003742973 solicitud de derogación de las siguientes Especificaciones Técnicas: MANTENIMIENTO Y SOPORTE TECNICO DE LA PLATAFORMA DDOS E IPS –BACCI No. JEMPP-CEDE6-BACCI-ET-01487/ COMUN-02. El Batallón de Ciberdefensa y Ciberseguridad BACCI, en la presente especificación técnica garantiza la pluralidad de oferentes. El Batallón de Ciberdefensa y Ciberseguridad BACCI, en la presente especificación técnica garantiza los requisitos generales y específicos, los cuales fueron revisados técnicamente y satisfacen las necesidades del Ejército Nacional. El Batallón de Ciberdefensa y Ciberseguridad BACCI en la presente especificación técnica garantiza que fue elaborada de manera profesional, con la mayor transparencia, siempre buscando dejar en alto el nombre del Ejército Nacional.	29/04/2025



MINISTERIO DE DEFENSA NACIONAL
COMANDO EN JEFE FUERZAS ARMADAS
REPUBLICANAS
DEPARTAMENTO DE LOGÍSTICA

ESPECIFICACIÓN
TÉCNICA

Fecha de emisión: 1975-10-15
Versión: 1.0
Código: 10-10-15-1.0

REVISIÓN

Descripción de la especificación técnica: Se trata de la especificación técnica para la construcción de un sistema de control de tráfico aéreo (CTA) que permita el control de los vuelos de los aviones en el espacio aéreo.

Descripción de la especificación técnica: Se trata de la especificación técnica para la construcción de un sistema de control de tráfico aéreo (CTA) que permita el control de los vuelos de los aviones en el espacio aéreo.

El Batallón de Comunicaciones y Enlace (BCE) en la presente especificación técnica para la construcción de un sistema de control de tráfico aéreo (CTA) que permita el control de los vuelos de los aviones en el espacio aéreo.

El Batallón de Comunicaciones y Enlace (BCE) en la presente especificación técnica para la construcción de un sistema de control de tráfico aéreo (CTA) que permita el control de los vuelos de los aviones en el espacio aéreo.

El Batallón de Comunicaciones y Enlace (BCE) en la presente especificación técnica para la construcción de un sistema de control de tráfico aéreo (CTA) que permita el control de los vuelos de los aviones en el espacio aéreo.

✓