

ANEXO ESPECIFICACIONES TÉCNICAS DE OBLIGATORIO CUMPLIMIENTO

Facatativá XX de XXXXX de 2026

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

Para efectos de establecer las especificaciones técnicas del presente proceso, se dará aplicación a las especificaciones técnicas para el **SOPORTE Y MANTENIMIENTO DE LA HERRAMIENTA DE CIBERSEGURIDAD PERIMETRAL CONTRA DENEGACIÓN DE SERVICIO, A EJECUTAR EN LA VIGENCIA 2026** No. **ESPECIFICACIÓN TÉCNICA No. JEMPP-CEDE6-DIPCO-ET-05732/COM-00** y a las especificaciones técnicas adicionales consignadas en el plan de necesidades Centralizado No.2026186010776933, los cuales contienen los parámetros técnicos que deben cumplir los oferentes en la acreditación de los servicios a prestar, los cuales se describen a continuación:

ESPECIFICACIÓN TÉCNICA No. JEMPP-CEDE6-DIPCO-ET-05732/COM-00





MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL FUERZAS MILITARES
EJÉRCITO NACIONAL
DEPARTAMENTO DE LOGÍSTICA

ESPECIFICACIÓN TÉCNICA

Página 2 de 11

Código: FO-JEMPP-CEDE4-890

Versión: 2

Fecha de emisión: 2022-10-12

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

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.

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.

3.1.3

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:

El Mantenimiento y Soporte para la Protección Contra Ataque de Denegación de Servicios Distribuido, deberá brindarse a los equipos que a continuación se relacionan.

3.2.1.1

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	90060000523
Standard Support for Bypass Switch chassis for 10G/40G/100G bypass modules	90800000006S
Standard Support for 10 Gigabit fiber multimode SR bypass switch module, 2 bypass segment	90800000007S
Standard Support for 10Gbps Pluggable Optics Multimode SR for Bypass Switch	90600000063S

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:

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:

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.

3.2.4.1 Estos mantenimientos deben incluir como mínimo:

- Instalación de software
- Configuraciones, puesta en producción y funcionamiento del aplicativo y/o herramienta de seguridad



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

✓



visión y/o Actualización	Modificaciones	Fecha
	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.	29/04/2025
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.	

Para efectos de establecer las especificaciones técnicas del presente proceso, la cual contiene los parámetros técnicos que deben cumplir los oferentes, así mismo, el contenido de las ESPECIFICACIONES TÉCNICAS ADICIONALES DE OBLIGATORIO CUMPLIMIENTO No. 2026574008764673, los cuales se describen a continuación:

ANEXO TÉCNICO ESPECIFICACIONES TÉCNICAS ADICIONALES DE OBLIGATORIO CUMPLIMIENTO.

REQUISITOS GENERALES

Se requiere el servicio del mantenimiento y soporte capacidad de protección contra ataque de denegación de servicio Distribuido DDoS del Batallón de Ciberdefensa y ciberseguridad del Ejército Nacional, del fabricante Radware, con el fin de proteger la Infraestructura tecnológica crítica del Ejército Nacional, fortaleciendo la compañía de Defensa Cibernética la cual tiene su administración y gestión. La plataforma consta tanto de hardware como de software el cual debe estar soportado ante cualquier falla por el fabricante, a través de compañías autorizadas; las cuales en su mayoría son empresas en Colombia prestadoras de servicios de seguridad de la información.

ESPECIFICACIONES TÉCNICAS ADICIONALES DE OBLIGATORIO CUMPLIMIENTO.


Al contestar, cite este número

Radicado N°: **2026574008764673** MDN-CQGFM-COEJC-SECEJ-JEMOP-CAOCC-
BRICG-BACGI-29.25



**ESPECIFICACIONES TECNICAS ADICIONALES DE OBLIGATORIO
CUMPLIMIENTO PARA EL PROCESO DE MANTENIMEINTO Y
SOPORTE PARA LA CAPACIDAD DE PROTECCIÓN CONTRA
ATAQUE DE DENEGACION DE SERVICIO DDOS DEL EJÉRCITO
NACIONAL.**

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



Al contestar, cite este número

Radicado N°: **2026574008764673** MDN-COGFM-COEJC-SECEJ-JEMOP-CAOCC-BRICC-BACCI-29.25

**ANEXO TÉCNICO ESTUDIO PREVIO
ESPECIFICACIONES TECNICAS ADICIONALES DE OBLIGATORIO CUMPLIMIENTO**

MANTENIMIENTO Y SOPORTE PARA LA CAPACIDAD DE PROTECCIÓN CONTRA ATAQUE DE DENEGACION DE SERVICIO DDOS DEL EJÉRCITO NACIONAL.	
	OBLIGACIONES GENERALES DEL CONTRATISTA: • <u>CONFIDENCIALIDAD DE LA INFORMACIÓN</u> El contratista se obliga a no suministrar ni publicar ninguna información que obtenga o conozca con ocasión de la ejecución del contrato; así como sobre los lugares a los cuales tenga acceso con ocasión de su desarrollo y sea revelada información marcada como confidencial. El contratista deberá diligenciar el formulario Anticorrupción "acuerdo de confidencialidad". La empresa adjudicataria, así como todos los miembros del equipo de trabajo objeto del proceso deberán guardar secreto profesional sobre toda la información, documentos y asuntos, independientemente de su naturaleza (técnica, comercial, financiera, operacional o de otro tipo), a los que tenga acceso o conocimiento durante la vigencia del contrato, independientemente de la forma o soporte (verbal, escrita, grabado o de cualquier otro tipo), por la que haya adquirido la información. En tal virtud, está obligado y se adoptarán todas las medidas necesarias para no hacer público, sustraer, duplicar, alterar, ocultar, ceder o enajenar cuanto dato conozca como consecuencia o con ocasión de la ejecución del contrato. Esta obligación no se limita al tiempo de ejecución del contrato, sino que deberá ser respetada aún después de su finalización. 1 A tal efecto todos los miembros del equipo prestador del servicio deberán tener un completo conocimiento del deber de secreto de la información durante la ejecución del contrato y en el supuesto de producirse algún cambio en la composición del equipo prestador del servicio, los nuevos integrantes asumirán las obligaciones contenidas en este ítem. Con esta finalidad el contratista se compromete a formar e informar al personal de tales obligaciones asumiendo, en el caso contrario, las responsabilidades que pudieran devenirle por su incumplimiento. Por lo anterior es indispensable que el contratista se comprometa a conocer, aceptar y ajustarse a las políticas de seguridad informática del Comando General de las Fuerzas Militares y del Ejército Nacional, firmar al inicio del contrato una promesa de reserva donde garanticen la confidencialidad de la información institucional a la cual tengan acceso directamente o por intermedio de terceros, así como la que genere, como producto de la ejecución del contrato y la de estos pliegos técnicos, y por tanto en ningún caso podrá divulgarla, copiarla, reproducirla o suministrarla a terceros. El contratista y los recursos humanos que formaran parte del grupo de trabajo deberán firmar al inicio de la ejecución del contrato, el acuerdo de confidencialidad donde garanticen la confidencialidad de la información institucional a la cual tengan acceso directamente o por intermedio de terceros, así como la que genere como producto de la ejecución del contrato y por tanto en ningún caso podrá divulgarla, copiarla, reproducirla o suministrarla a terceros; así mismo, en caso de un ataque cibernético relacionado con las plataformas de seguridad perimetral firewall o presentarse una situación de cualquier naturaleza



Al contestar, cite este número

Radicado N°: **2026574008764673** MDN-COGFM-COEJC-SECEJ-JEMOP-CAOCC-BRICC-BACCI-29.25

que llegue a afectar la infraestructura del Ejército Nacional dentro de los términos del contrato y sea necesario el apoyo de personal del equipo prestador de servicios tenga que apoyar en las instalaciones del Batallón de Ciberdefensa y Ciberseguridad del Ejército Nacional, deberá firmar acta de compromiso de confidencialidad, así mismo a dar cumplimiento a:

Ley 1581 de 2012 de Protección de datos personales

Ley 1712 de 2014 Acceso a la información pública

Ley 1273 de 2009 Modificación del Código Penal -bien jurídico tutelado "protección de la información y de los datos".

Ley 23 de 1982 de Derechos Autor y Ley 1915 de 2018.

- **PROPIEDAD INTELECTUAL**

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

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

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

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

- **DOCUMENTACIÓN**

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

PLAN DE TRABAJO:

Una vez firmada el acta de inicio y/o reunión de inicio del contrato, el contratista en coordinación con el supervisor deberá realizar un diagnóstico del estado de aseguramiento, entrevistas con el personal de ingenieros a desarrollar los soportes y mantenimientos de la Herramienta Contra ataques de denegación de servicios (DDoS) del Ejército Nacional, con el fin de identificar los principales requerimientos críticos de la Fuerza generando prioridades, Esta actividad no podrá exceder 5 días hábiles para su ejecución. Con base en el levantamiento de información, el contratista deberá presentar al supervisor un plan de trabajo inicial con su respectiva asignación de recursos requeridos para el desarrollo de las actividades priorizadas.



Al contestar, cite este número

Radicado N°: **2026574008764673** MDN-COGFM-COEJC-SECEJ-JEMOP-CAOCC-BRICC-BACCI-29.25

	Los tiempos generados en el desarrollo del levantamiento de información y la elaboración del plan de trabajo no serán descontados de las horas contratadas, ni generará costo adicional para Ministerio de Defensa - Ejército Nacional. El plan de Trabajo deberá ser entregado a el supervisor del contrato para su aprobación final dentro de los tres días (3) hábiles siguientes al término del levantamiento de información, dicho documento deberá estar firmado por la empresa adjudicataria y el supervisor del contrato. Este plan de trabajo deberá ser revisado mes a mes con el objeto de realizar seguimiento a estas tareas por parte del supervisor del contrato. Si el Ejército Nacional por intermedio del supervisor desea efectuar cualquier cambio en el plan de trabajo aprobado, este podrá realizar según acuerdo y aprobación por escrito de las partes. Funcionario idóneo por parte de la firma adjudicataria y Ejército Nacional a través del supervisor del contrato. - Después cada configuración se debe entregar un manual de procedimiento de las configuraciones realizadas en cada una de las actividades de soporte y mantenimiento requeridas por parte del Ejército Nacional. - Informe final donde se describa el total de las soluciones, configuraciones y procesos realizados en la ejecución del contrato. Informe de cada visita, documentado los procedimientos realizados. • <u>OTROS</u> El contratista se debe comprometer a conocer, aceptar y ajustarse a las políticas de seguridad de la Directiva de Seguridad Informática del Ministerio de Defensa - Comando General de las Fuerzas Militares Directivas Permanentes de Ciberdefensa y Seguridad de la Información.
2	<u>REQUERIMIENTO</u> El Ejército Nacional requiere efectuar el Mantenimiento y Soporte de la Plataforma Contra ataques de denegación de Servicios (DDoS), garantizando la operatividad y el funcionamiento, de la infraestructura tecnológica del Ejército Nacional, que se encuentran en producción relacionados en la presente especificación técnica y sin que este genere costos adicionales para la institución, con el fin de contribuir a una mejor operatividad del sistema.
3	<u>MODALIDAD DEL SERVICIO:</u> La ejecución del contrato que se derive de la presente especificación técnica se realizará mediante la modalidad de bolsa de horas a disposición del supervisor
4	<u>SOPORTE TÉCNICO:</u> El contratista debe atender los equipos y sus componentes desde la fecha de inicio del contrato y brindar soporte técnico de acuerdo al ítem 3 numerales 3.1.1 al 3.1.3 de la Especificación Técnica de obligatorio cumplimiento para el presente proyecto teniendo en cuenta los siguientes niveles:



Al contestar, cite este número

Radicado N°: **2026574008764673** MDN-COGFM-COEJC-SECEJ-JEMOP-CAOCC-BRICC-BACCI-29.25

	Nivel 1: Se denomina Nivel 1 cuando el sistema presenta bloqueo o caída total crítica, el contratista debe atender el requerimiento en sitio y dar solución en un tiempo máximo de 02 horas a partir del momento de que se realiza el requerimiento. Si el problema reportado requiere realizar cambios y/o actualización a software y/o firmware; en este caso la entrega será en un plazo máximo de 12 horas, sin costo alguno para el Ejército Nacional. Nivel 2: Se denomina Nivel 2 cuando el sistema presenta fallas parciales que no afectan el funcionamiento total del sistema, el contratista debe atender el requerimiento en los sitios definidos en el objeto de este contrato, en un tiempo no mayor a 04 horas. El contratista deberá garantizar la disponibilidad del servicio de soporte en modalidad 7x24 (siete días a la semana, veinticuatro horas al día) durante toda la vigencia del contrato, permitiendo el reporte y escalamiento de incidentes o requerimientos a través de los canales definidos (teléfono, correo electrónico o acceso remoto). La disponibilidad del servicio no implica la dedicación exclusiva ni la asignación permanente de recursos por parte del contratista. "La sola existencia de la disponibilidad 7x24 no constituye tiempo facturable ni consumible de la bolsa de horas; únicamente serán descontadas las horas efectivamente ejecutadas y registradas para la atención de actividades previamente requeridas o autorizadas por el Supervisor del Contrato." Los costos derivados de la solución al requerimiento efectuado en alguno de los niveles de soporte técnico, deberán asumirse en su totalidad por el contratista. Una vez evaluado el requerimiento y solucionado, este debe quedar documentado en un acta firmada por el contratista y supervisor del contrato.
5	<u>Cumplimiento de Normatividad Gubernamental en Materia de Tics</u> Los bienes y servicios TICS contemplados en el presente anexo técnico, deben brindar soporte al protocolo de internet versión seis (IPv6) de conformidad con la Resolución 2710 del 03 de octubre de 2017 de MINTIC, que en su Artículo 5. "Contratación", estipula: "A partir de la entrada en vigencia de la presente resolución, todos los procesos de selección que inicien las entidades públicas deberán, desde los mismos pliegos de condiciones o lo que haga sus veces, exigir soporte IPv6 nativo en coexistencia con IPv4, en la contratación de bienes y servicios relacionados con las TICS."
6	<u>Garantía</u> Contratista durante los primeros 5 días hábiles posteriores a la reunión de inicio deberá indicar el procedimiento que se deberá seguir para solicitar el servicio de garantía del servicio de soporte prestados durante la vigencia del contrato o hasta finalizar las horas de soporte pactadas, y seis (6) meses más después de la entrega a satisfacción del mismo. La garantía cubre como mínimo la calidad y correcto funcionamiento del sistema de denegación de servicios DDOS. Este servicio no será contemplado dentro de las horas contratadas y no generará costo adicional para Ejército Nacional.



Al contestar, cite este número

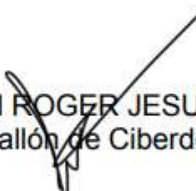
Radicado N°: **2026574008764673** MDN-COGFM-COEJC-SECEJ-JEMOP-CAOCC-BRICC-BACCI-29.25

	El Contratista, durante la ejecución del contrato, acepta que el Ejército Nacional evalúe el desempeño profesional de la(s) persona(s) asignadas para el proyecto y estará(n) en facultad de solicitar su reemplazo, si esta(s) no cumple(n) con las expectativas del supervisor del contrato. Durante la ejecución del contrato, si se requiere reemplazar un funcionario por otro, éste deberá tener un perfil profesional igual o superior al que va a ser reemplazado, y cumplir con los requerimientos estipulados en esta especificación técnica. En caso de que el contratista requiera realizar un cambio de personal, este deberá informar al supervisor del contrato de tal situación con mínimo 10 días de antelación, anexando la hoja de vida del nuevo funcionario que debe cumplir con las especificaciones requeridas. El supervisor evaluará el desempeño laboral del profesional asignado para el soporte y estará en facultad de solicitar su reemplazo si lo considera necesario, en dado caso el oferente adjudicatario deberá reemplazarlo en un tiempo no mayor a cinco (5) días luego de la solicitud formal por parte del supervisor del contrato. El Contratista deberá garantizar el normal funcionamiento de la solución después de los mantenimientos preventivos y/o correctivos. La garantía deberá ser aportados en documento independiente debidamente suscrito por el oferente.
7	<u>Término de Respuesta de la Garantía Técnica</u> Para el presente proceso de selección, el proponente junto con la oferta deberá presentar el termino de respuesta de la garantía técnica, el cual cubrirá lo siguiente: - o El Contratista deberá garantizar el normal funcionamiento de la solución después de los mantenimientos preventivos y/o correctivos, de no ser así el contratista deberá cubrir los gastos (configuraciones, horas ingenieros) que se generan hasta restablecer el funcionamiento de la solución en un tiempo no mayor a 24 horas. - o Estarán a cargo del contratista todos los costos en que deba incurrir en el cumplimiento de su deber de garantía. NOTA: Los términos de respuesta de la garantía técnica, deberán ser aportados en documento independiente debidamente suscrito por el oferente.
8	<u>Caso de Fallas</u> El contratista será responsable por la calidad de las actividades ejecutadas durante la prestación del servicio de soporte y mantenimiento. En caso de presentarse incidentes, errores, afectaciones o fallas atribuibles a las actividades realizadas por el contratista, este deberá efectuar las correcciones necesarias para restablecer el correcto funcionamiento de los servicios y componentes intervenidos, sin costo adicional para la entidad. Las actividades de corrección derivadas de errores o fallas imputables al contratista no generarán consumo de horas de la bolsa contratada y deberán ser atendidas hasta su solución definitiva.

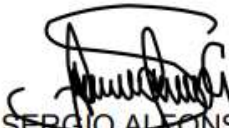
9	RECURSOS HUMANOS El Contratista debe contar con personal técnico especializado, capacitado y certificado en cada una de las herramientas relacionadas en la presente especificación técnica para atender y solucionar los incidentes reportados durante la ejecución del contrato y el tiempo de soporte de todas las soluciones, de acuerdo al siguiente perfil, de la cual el oferente deberá presentar junto con la oferta los siguientes requerimientos: Profesional en Ingeniería electrónica o telemática o de sistemas o telecomunicaciones o Seguridad de la Información, que cuente con experiencia mínima de tres (3) años, contados a partir de la fecha de expedición de la tarjeta profesional, y deberá contar con las siguientes certificaciones: • Certificación o constancia vigente de entrenamiento nivel 1 o superior en la solución ofertada emitido por el fabricante o por un ente certificador autorizado por el fabricante. • Certificado o curso IPV6. • Certificación de experiencia técnica en instalación y/o soporte de los productos de la plataforma DDoS e IPS ofertadas. • Debe contar con al menos una (1) certificación en la plataforma de ciberseguridad descrita en la Especificación Técnica N°. JEMPP-CEDE6-DIPCO-ET-08732/COM-00, la cual debe estar orientada a permitir ejecutar tareas de configuración, administración y monitoreo de alto nivel. • Certificado de vigencia y/o antecedentes profesionales donde certifique que no tiene antecedentes ético-profesionales o sanciones vigentes que impidan el ejercicio de la profesión. Nota 1: Deberá anexar con la oferta Hoja de vida completa con los respectivos datos personales, experiencia y formación profesional. Nota 2: No se aceptan certificaciones con enmendaduras y que no contengan como mínimo la información solicitada o que presenten inconsistencias. Nota 3: La Central Administrativa Contable y Especializada Telemática, se reserva el derecho de verificar la veracidad de la información suministrada por el oferente. Nota 4: No se acepta ningún otro documento para acreditar la experiencia. NO SE ACEPTAN AUTO CERTIFICACIONES. Nota 5: Las copias de los documentos presentadas deben ser completamente legibles. Nota 6: La información suministrada se entiende bajo la gravedad de juramento y debe ser correlativa a la documentación aportada. Nota 7: El objeto del contrato debe haber sido ejecutada a satisfacción y en su desarrollo no debe haberse presentado ningún tipo de sanción y/o observación.
---	--

Nota 8: El personal dispuesto por el contratista debe ser de nacionalidad colombiana.

La entidad evaluará la información suministrada y de acuerdo con ella determinará si resulta suficiente para acreditar la experiencia


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


CS. SENA BOLIVAR SERGIO LUIS
Comité Técnico Estructurador


PD02: SERGIO ALFONSO GOMEZ
Comité Técnico Estructurador

EI OFERENTE

REPRESENTANTE LEGAL O APODERADO

Nombre Identificación Razón social

C.C. / NIT XXXXXX