

Facatativá – Cundinamarca, 09 de julio de 2024

ADENDA No. 001

PROCESO DE PROCESO DE LICITACIÓN PÚBLICA No. 070-CENACTELEMÁTICA-2024, CUYO OBJETO ES “PROVEER EQUIPOS ESPECIALIZADOS EN CIBERDEFENSA PLARAFORMA FIREWALL”.

En uso de las facultades legales consagradas en la Ley 80 de 1993, Ley 1150 de 2007, Ley 1474 de 2011, Decreto Ley 0019 de 2012, Decreto 1082 de 2015, demás normas concordantes, la Resolución de Delegación No. 4223 del 23 de junio de 2022 “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”. Por la que se delegan unas funciones y competencias relacionadas con la contratación de bienes y servicios con destino al Ejército Nacional y la Resolución No. 4130 del 16 de junio de 2022, “Manual de Contratación y de Convenios del Ministerio de Defensa Nacional, modificada parcialmente por la Resolución No. 4213 del 13 de octubre de 2023 y Decreto Reglamentario 1082 de 2015”, y

CONSIDERANDO:

Que mediante Resolución de Delegación No. 4223 del 23 de junio de 2022, el Señor Ministro de Defensa Nacional, debidamente facultado por los artículos 211, 216 y 217 de la Constitución Política; el artículo 12 de la Ley 80 de 1993; los artículos 9, 10 y 12 de la Ley 489 de 1998; el artículo 37 del Decreto 2150 de 1995; artículo 110 del Decreto 111 de 1996; y la Ley 1150 de 2007, delegó parcialmente a esta Dependencia, la celebración, modificación, adición, prórroga, liquidación y terminación de contratos, así como los demás actos inherentes a la actividad contractual, cuando la cuantía sea desde 0 hasta 10.000 S.M.L.M.V.

Que el Ministerio de Defensa Nacional- Ejército Nacional- CENACTELEMÁTICA está interesado en “**PROVEER EQUIPOS ESPECIALIZADOS EN CIBERDEFENSA PLARAFORMA FIREWALL**”

El presupuesto total asignado para el presente proceso cuyo objeto es “**PROVEER EQUIPOS ESPECIALIZADOS EN CIBERDEFENSA PLARAFORMA FIREWALL**” es por la suma **DOS MIL CIENTO TREINTA MILLONES CIENTO VEINTITRÉS MIL OCHOCIENTOS SIETE PESOS M/CTE (\$2.130.123.807,00)**, respaldado mediante Certificado Disponibilidad Presupuestal No. 13224 del 2 de mayo de 2024, expedido por el Jefe de Presupuesto del CENAC-TELEMATICA, de acuerdo a la siguiente distribución y rubros presupuestales:

ARTICULO PRESUPUESTAL (SIIF NACIÓN)	RECURSO	DESCRIPCIÓN DEL RUBRO	UNIDAD BENEFICIADA	VALOR APROXIMADO DE LA NECESIDAD EN URGENCIA FUNCIONAL
C-1502-0100-31-20107B-1502114-02	11 CSF	ADQUIS. DE BYS - SERVICIO DE CIBERDEFENSA - FORTALECIMIENTO DE LOS MEDIOS CIBERNÉTICOS DEL EJERCITO NACIONAL	BACCI	\$ 2.130.123.807,00
TOTAL				\$ 2.130.123.807,00

PATRIA HONOR LEALTAD

Calle 5 No 15 – 00 Barrio Dos caminos – Facatativá – Cundinamarca.
Conmutador 4261428 Ext. 39036
Correo electrónico de la unidad cenactel@buzonejercito.mil.co



SC8310-1

Que el día 06 de junio de 2024, la entidad CENAC DE TELEMATICA, publica en el portal único de contratación www.colombiacompra.gov.co, SECOP II el estudio previo, aviso de convocatoria, proyecto de pliego de condiciones, formularios y de más anexos que hacen parte integral del presente proceso, que tiene por objeto **"PROVEER EQUIPOS ESPECIALIZADOS EN CIBERDEFENSA PLARAFORMA FIREWALL"**

Que, hasta el día 25 de junio de 2024 fue establecido el plazo para que los interesados presentaran observaciones al proyecto de pliego de condiciones, plazo dentro del cual se recibió observaciones por parte de las empresas IT SERVICIOS DE COLOMBIA SAS y CONVIEST SAS.

Que, dentro del término de respuesta a las observaciones al proyecto de pliego de condiciones, el día 27 de junio de 2024 a través del formulario de preguntas y respuestas No. 001, el Comité estructurador realizó respuesta a la observación, debidamente publicada en la plataforma del SECOP II.

Que el día 28 de junio de 2024, la entidad CENAC DE TELEMATICA, publica en el portal único de contratación www.colombiacompra.gov.co, SECOP II Resolución de Apertura No. 152 de 28 de junio de 2024, pliego de condiciones definitivo, formularios y de más anexos que hacen parte integral del presente proceso, el cual tiene por objeto **"PROVEER EQUIPOS ESPECIALIZADOS EN CIBERDEFENSA PLARAFORMA FIREWALL"**.

Que el 27 de junio de 2024, se llevó a cabo Audiencia de asignación de riesgo del proceso LP-075-CENACTELEMATICA-2024, registrada así mediante acta No. 096, debidamente publicada en la plataforma del SECOP II.

Que dentro del término de observaciones al pliego de condiciones definitivo, se recibió observaciones por parte de la empresa IT SERVICIOS DE COLOMBIA SAS, las cuales fueron resueltas a través del formulario de preguntas y respuestas No. 002, y de las cuales el Comité Técnico Estructurador acogió parcialmente, por ello, es necesario modificar el proceso a través de la Adenda No. 01.

Que las actuaciones de quienes intervienen en la Contratación Estatal se desarrollarán con arreglo a los principios de transparencia, economía y responsabilidad (artículo 23 Ley 80/93) y conforme a los postulados que rigen la administración (artículo 209 de la Constitución Política).

Que conforme a los anteriores considerandos, el CENAC TELEMATICA, procede a expedir la Adenda No.01 dentro del proceso LP-070-CENACTELEMATICA-2024, cuyo objeto es **"PROVEER EQUIPOS ESPECIALIZADOS EN CIBERDEFENSA PLARAFORMA FIREWALL"**

RESUELVE:

ARTÍCULO PRIMERO: Modifíquese parcialmente las especificaciones técnicas adicionales en el numeral 15.1., del Estudio Previo, Pliego de Condiciones y anexo Especificaciones Técnicas de Obligatorio Cumplimiento y adicionales, quedando así:

ESPACIO INTENCIONALMENTE EN BLANCO

PATRIA HONOR LEALTAD

Calle 5 No 15 – 00 Barrio Dos caminos – Facatativá – Cundinamarca.
Conmutador 4261428 Ext. 39036
Correo electrónico de la unidad cenactel@buzonejército.mil.co



ESPECIFICACIONES TECNICAS ADICIONALES DE OBLIGATORIO CUMPLIMIENTO

ADQUISICIÓN, INSTALACIÓN Y CONFIGURACIÓN DE UNA HERRAMIENTA DE SEGURIDAD PERIMETRAL FIREWALL PARA EL FORTALECIMIENTO DE LOS MEDIOS CIBERNETICOS DEL EJÉRCITO NACIONAL.	
1	<p><u>OBLIGACIONES GENERALES DEL CONTRATISTA:</u></p> <ul style="list-style-type: none"><u>Confidencialidad de la Información</u> <p>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”.</p> <p>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.</p> <p>A tal efecto todos los miembros del equipo prestador del servicio deberán tener un completo conocimiento del deber de secreto de la información durante la ejecución del contrato y en el supuesto de producirse algún cambio en la composición del equipo prestador del servicio, los nuevos integrantes asumirán las obligaciones contenidas en este ítem. Con esta finalidad el contratista se compromete a formar e informar al personal de tales obligaciones asumiendo, en el caso contrario, las responsabilidades que pudieran devenirse por su incumplimiento.</p> <p>Por lo anterior es indispensable que el contratista se comprometa a conocer, aceptar y ajustarse a las políticas de seguridad informática del Comando General de las Fuerzas Militares y del Ejército Nacional y firmar al inicio del contrato una promesa de reserva donde garantizan la confidencialidad de la información institucional a la cual tengan acceso directamente o por intermedio de terceros, así como la que genere, como producto de la ejecución del contrato y la de estos pliegos técnicos, y por tanto en ningún caso podrá divulgarla, copiarla, reproducirla o suministrarla a terceros.</p> <p>El contratista y los recursos humanos que formaran parte del grupo de trabajo deberán firmar al inicio de la ejecución del contrato, el acuerdo de confidencialidad donde garantizan la confidencialidad de la información institucional a la cual tengan acceso 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 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.</p>

	<ul style="list-style-type: none">• <u>Propiedad Intelectual</u> <p>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.</p> <p>_____ En particular, toda aquella documentación generada por intervenciones del personal asignado al servicio en el Ejército, será propiedad de la institución, por tanto, no podrá ser facilitada a otra persona o entidad sin consentimiento expreso del Ejército.</p> <p>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 en 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.</p> <p>Por lo anterior al finalizar la ejecución del proceso toda la información y documentos entregados por el Comando del Ejército, deberán ser retornados y no podrá quedarse con la información que se genere.</p> <ul style="list-style-type: none">• <u>Documentación</u> <p>El contratista deberá entregar al Ejército Nacional la documentación necesaria para la Instalación, configuración, implementación y parametrización.</p> <p>Esta documentación debe incluir el detalle del plan de trabajo completo para efectuar la instalación y configuración de las plataformas adquiridas, además se debe especificar:</p> <ul style="list-style-type: none">- Los recursos necesarios para la instalación.- Cada uno de los pasos que se deben efectuar.- Los tiempos de ejecución de cada uno de los pasos.- Para el desarrollo de la instalación se deberá presentar un cronograma de tareas después de firmada el acta de inicio del contrato.- Después cada configuración se debe entregar un manual de procedimiento de las configuraciones realizadas en cada una de las soluciones.- Informe final donde se describa el total de las soluciones, configuraciones y procesos realizados en la ejecución del contrato <p>Informe de cada visita, documentado los procedimientos realizados.</p> <ul style="list-style-type: none">• <u>Otros</u> <p>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.</p>
2	<p><u>El contrato debe ser tratado como un proyecto llave en mano.</u></p> <p>Para todos los efectos de funcionalidad e interoperabilidad, el contratista debe instalar, configurar, dar soporte y acompañamiento de las soluciones adquiridas y el software instalado, garantizando al Ministerio</p>

	<p>de Defensa Nacional – Ejército Nacional – Batallón de Ciberdefensa y Ciberseguridad el correcto funcionamiento de acuerdo a las especificaciones técnicas requeridas.</p> <p>Nota: “Sera considerado un proyecto llave en mano, aquel que asegure el resultado final de manera satisfactoria, cumpliendo las especificaciones. La optimización de costo, logística, mejores prácticas de implementación serán potestad del contratista, siempre y cuando cumplan con el objetivo final de suministrar una solución que garantice las especificaciones técnicas requeridas; de ser necesario el oferente asumirá costos adicionales de servicios, accesorios, componentes de software, hardware, cableado y elementos adicionales requeridos para la óptima implementación de esta solución e integración con todas las soluciones tecnológicas del Ejército Nacional.”</p> <p>Se debe suministrar por parte del contratista la logística necesaria para el desarrollo del contrato como: portátiles, desplazamientos, hospedajes, alimentación, discos duros extraíbles, papelería y software para el desarrollo del contrato, sin que esto genere costo adicional para el Ministerio de Defensa Nacional – Ejército Nacional – Batallón de Ciberdefensa y Ciberseguridad; Una vez finalizado el contrato, a estos elementos se les debe realizar un procedimiento de borrado seguro por parte de la Batallón de Ciberdefensa y Ciberseguridad del Ejército Nacional para posteriormente ser retirados de las instalaciones del Ministerio de Defensa Nacional – Ejército Nacional – Batallón de Ciberdefensa y Ciberseguridad.</p>
3	<p><u>Cumplimiento de Normatividad Gubernamental en Materia de Tics</u></p> <p>Todas las soluciones deben ser compatibles con los protocolos IPV4 e IPV6 CUMPLIMIENTO DE NORMATIVIDAD GUBERNAMENTAL EN MATERIA DE TICS</p> <p>Los bienes y servicios TICS contemplados en la presente ficha técnica, 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.”</p> <p><u>Cumplimiento Normas Técnicas</u></p> <p>El Contratista debe cumplir o exceder en las siguientes especificaciones de instalación, documentación, componentes y sistemas de la industria según sea el caso:</p> <p>ANSI/TIA-568-C.0 Generic Telecommunications Cablingfor Customer Premises 2009. Norma que dicta las directrices para cableado genérico de telecomunicaciones en instalaciones de clientes.</p> <p>ANSI/TIA-568-C.1 Commercial Building Telecommunications Cabling Standard 2009. Norma internacional que estipula las condiciones del cableado de telecomunicaciones para una edificación comercial.</p> <p>ANSI/TIA-568-C.3 Optical Fiber Cabling Components 2000. Norma que crea y estipula directrices generales de los componentes de fibra óptica de un sistema de telecomunicaciones.</p> <p>ANSI/TIA-568-C.2 Commercial Building Telecommunications Cabling Standard Agosto 2009. Norma que crea y estipula directrices de los diferentes componentes de un sistema de telecomunicaciones basado en transmisión en cables de pares trenzados.Telecomunicaciones/Infraestructuras Comerciales).</p> <p>ANSI-J-STD 607 y adendos “Commercial Building Grounding and Bonding Requirements for Telecommunications” (Requisitos para Telecomunicaciones de Puesta y Unido a Tierra en Edificios Comerciales).</p> <p>ANSI/TIA/EIA-526-7 “Measurement of Optical Power Loss of Installed Single-ModeFiber Cable Plant”</p>

	<p>(Medición de la Pérdida de Potencia Óptica de la Planta Instalada de Cable de Fibra Monomodo). ANSI/TIA/EIA-526-14ª"Optical Power Loss Measurements of Installed Multimode Fiber Cable Plant" (Medición de la Pérdida de Potencia Óptica de la Planta Instalada de Cable de Fibra Multimodo). 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). ISO/IEC 11801:2000 Ed2.0 y enmiendas "Information technology – Generic cabling for customer premises" (Cableado Genérico para Propiedades de Usuario). CENELEC EN 50173:2000 y enmiendas ANSI/TIA 942 Telecommunications Infrastructure Standard for Data Centers. ISO/IEC 24764 draft Generic cabling for Data Centre premises. Código Eléctrico Nacional NEC /RETIE (NTC 2050 de 1998). ICONTEC, para la construcción y fabricación de materiales y equipos NEMA, NEC: En caso de existir vacíos en lo referente a aspectos particulares en las Normas locales. El Contratista deberá cumplir con el Reglamento Técnico de Instalaciones Eléctricas (RETIE) que se encuentra en la norma NTC 2050. El contratista deberá contar con el certificado de conformidad de los productos comprendidos en el alcance del RETIE, para los siguientes elementos:</p> <ul style="list-style-type: none">- Tomacorrientes- Cable Eléctrico- Tableros- Tubería <p>Protecciones (breakers y tomas con supresor de transientes).</p>													
4	<p>El oferente debe incluir en la oferta, un cuadro de marcas y referencias de los equipos a ofertar con su respectivo catalogo o ficha técnica y el detalle técnico.</p> <p>El oferente debe adjuntar la documentación oficial del fabricante del producto donde se evidencie el cumplimiento de las especificaciones técnicas, la cual debe estar en un sitio web público oficial del producto (fabricante) y/o mediante manuales de configuración y/o descripción del producto en los cuales se pueda evidenciar el cumplimiento de las especificaciones técnicas solicitadas.</p> <p>Dentro del sitio web y/o documentación oficial debe encontrarse los términos en idioma español (si la documentación oficial es en inglés, el oferente debe adjuntar la traducción al idioma español) que identifique fácilmente el cumplimiento de los requerimientos técnicos solicitados por la entidad, NO se aceptarán cartas firmadas como prueba de validación de especificaciones técnicas ya que deben estar públicos o en documentación oficial de los productos.</p> <table><tr><th>Cantidad</th><th>Elemento</th><th>Marca</th><th>Referencia</th><th>Detalle técnico</th></tr><tr><td></td><td></td><td></td><td></td><td></td></tr></table> <p>Los equipos deben tener un sticker adhesivo con el nombre de la empresa que suministra los equipos, el número del contrato, número telefónico y correo electrónico donde brindan soporte técnico.</p> <p>Todos los equipos deberán estar embalados en las cajas de la fábrica y deben ser totalmente nuevos. La instalación de las licencias ya debe venir incluida en cada máquina que a partir de la firma del contrato serán Propiedad del Ejército Nacional, así mismo es responsabilidad del contratista garantizar mediante certificado escrito y avalado por el fabricante y/o distribuidor autorizado que los equipos no cuentan con ningún tipo de licenciamiento adicional al que esta descrito en esta ficha, de no ser así será responsabilidad del contratista el costo del licenciamiento adicional lo que no generara costo alguno para el Ejército Nacional.</p>				Cantidad	Elemento	Marca	Referencia	Detalle técnico					
Cantidad	Elemento	Marca	Referencia	Detalle técnico										

	<p>De igual modo los equipos deben ser nuevos y no remanufacturados.</p> <p>Cada uno de los equipos será entregado con sus respectivas cajas individuales y manuales técnicos, manuales de operación, cargador, interfaces de conexión, software de configuración (drivers) en medios digitales originales, para cada uno de los componentes del equipo que garanticen su pleno funcionamiento. Los manuales deben contener idioma ingles y/o español.</p> <p>El contratista deberá adjuntar en archivo digital e impreso en Excel el listado de los seriales, referencias, periodo de garantía, licenciamiento, de todos los equipos a entregar con el fin de verificar de una forma rápida el material.</p> <p>Los equipos deben tener un sticker adhesivo con el nombre de la empresa que suministra los equipos, el número del contrato, número telefónico y correo electrónico donde brindan soporte técnico.</p>
5	<p>El contratista debe garantizar que toda representación gráfica debe cumplir normas fijas y preestablecidas para poder describir de forma exacta y clara; equipos, asignación de recursos físicos y licencias, al igual que dimensiones y características que permitan identificar la plataforma adquirida y habilitar la construcción del nuevo diseño elaborado.</p> <p>Al finalizar la implementación el contratista debe entregar un diagrama técnico detallado donde sea representado gráficamente cada uno de los componentes de Hardware y Software con sus correspondientes conexiones de red (datos y de potencia), con el propósito de proporcionar información suficiente para facilitar su análisis, mantenimiento e integración con las demás herramientas con las que cuenta el Ejército Nacional.</p>
	<p>El contratista debe garantizar que los dispositivos de hardware ofertados como appliance deben tener las características y elementos para montaje en rack estándar, e incluir sus cables de alimentación eléctrica, cables para datos tipo RJ45, conversores RJ45 a RJ .5 y cables de fibra óptica necesarios para su correcta operación y funcionalidad de acuerdo al diseño lógico y físico ofrecido. Así mismo deben ser instalados y configurados todos los elementos de las soluciones, lo cual no incurrirá en costos adicionales para el Ejército Nacional.</p>
6	<p>Las soluciones a implementar deben ser compatibles con las plataformas actuales del Ejército Nacional y cumplir con el protocolo IPv4 e IPV6.</p>
7	<p>Para la implementación y conectorización eléctrica no se podrán realizar apagados del centro de datos, por lo cual toda la actividad de implementación se debe realizar en producción sin afectar los servicios del centro de cómputo previa coordinación con el supervisor del contrato. De ser necesario un apagado programado, este debe ser coordinado con el supervisor del contrato.</p>
8	<p>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.</p>
9	<p>Soporte Fabricante</p> <p>Según las especificaciones proporcionadas, el horario de cobertura de soporte por parte del fabricante debe ser 24x7x365, lo que significa que debe estar disponible los 365 días del año, las 24 horas del día, incluyendo días festivos. Esto garantiza que el Ministerio de Defensa Nacional - Ejército Nacional - Batallón de Ciberdefensa y Ciberseguridad pueda recibir asistencia técnica y soporte en cualquier momento, incluso fuera del horario laboral regular.</p> <p>En cuanto a las actualizaciones de software, el fabricante debe proporcionarlas sin costo adicional durante el periodo de vigencia del contrato. Esto garantiza que el software utilizado en la solución se mantenga actualizado y cuente con las últimas mejoras y correcciones de seguridad sin incurrir en costos adicionales.</p>

	<p>Es importante tener en cuenta que estos aspectos relacionados con el soporte, la cobertura horaria y las actualizaciones de software deben ser detallados y especificados tanto en el contrato como en los términos de garantía, para asegurar que ambas partes, el Ministerio de Defensa Nacional - Ejército Nacional - Batallón de Ciberdefensa y Ciberdefensa el contratista, estén de acuerdo y cumplan con estas condiciones durante la ejecución del contrato.</p> <p>El término de la garantía técnica por parte fabricante será de mínimo dos (02) años para cada elemento desde la firma del acta de recibo a satisfacción.</p> <p>El Fabricante a través del contratista debe incluir los servicios de revisión y validación del estado de salud de la plataforma generando informes para optimización y verificación de casos específicos solicitados por el supervisor del contrato.</p>
10	<p><u>Soporte Contratista</u></p> <p>El contratista debe ofrecer el servicio de soporte técnico de la garantía para los sistemas y/o productos descritos en las Especificaciones Técnicas, durante la ejecución del contrato, es decir por un periodo de 2 años que es el término de la garantía.</p> <p>El horario de soporte por parte del contratista debe ser 24x7x365 remoto o presencial según lo solicite la entidad a partir de la firma del contrato, en caso de requerir cambios de equipos o partes por el fabricante, el contratista debe asumir todos los costos por desplazamiento, instalaciones, configuraciones y demás que sean necesarios en sitio y esto no incurrirá en ningún costo para la entidad.</p> <p>TIPO DE ATENCIÓN: El servicio será prestado de dos formas así:</p> <ul style="list-style-type: none"> • Soporte Nivel 1: De manera presencial tres días a la semana con duración de 8 horas laborales (3x8) en las instalaciones Ejército del Cantón Militar "Caldas" Cra 46 # 20c -01 Bogotá o donde se encuentre el sistema, el horario de trabajo será de acuerdo al requerimiento del supervisor del contrato, durante la vigencia de contrato. <p>Para prestar este servicio el ingeniero de soporte debe contactar con equipo de cómputo suministrado por el contratista el cual se dejará en las Instalaciones del Batallón de Ciberdefensa y Seguridad durante la vigencia del contrato.</p> <ul style="list-style-type: none"> • Soporte Nivel 2: Cuando se requiera remotamente a través de herramientas web online; en horario 7x24 (7 días a la semana las 24 horas del día) durante la vigencia de ejecución del contrato <p>Para este soporte el contratista deberá suministrar un servicio de asistencia técnica con personal certificado para atender necesidades específicas de la plataforma.</p> <p>Tiempos de respuesta: El servicio de soporte debe ser atendido de manera inmediata de acuerdo a lo solicitado por el Batallón de Ciberdefensa y Ciberseguridad del Ejército Nacional durante la duración del periodo de garantía.</p> <p>Tiempo máximo de respuesta dos (02) horas después de haber reportado el incidente.</p> <p>De ser necesario el contratista deberá enviar personal técnico especializado a sitio en un tiempo máximo de cuatro (04) horas.</p> <p>El tiempo máximo permitido para restablecer el servicio es de 4 horas.</p>
11	<p><u>Garantía</u></p> <p>El Contratista durante los primeros 15 días posteriores a la reunión de inicio deberá indicar el</p>

	<p>procedimiento que se deberá seguir para solicitar el servicio de garantía, tanto del hardware como de software de los servicios implementados.</p> <p>El término de la garantía técnica por parte fabricante será de mínimo dos (02) años para cada elemento</p> <p>El término de la garantía técnica por parte del contratista será de mínimo dos (02) años para cada elemento desde la firma del acta de recibo a satisfacción.</p> <p>NOTA: El Oferente deberá incluir con la oferta el procedimiento que se deberá seguir para solicitar el servicio de garantía, tanto del hardware como de software de los servicios implementados.</p>
12	<p><u>Certificación de Fabricante</u></p> <p>El oferente debe adjuntar en documento independiente en la oferta, certificado de fábrica que indique que es canal certificado en la herramienta y que está autorizado para distribuir y dar soporte de los productos adquiridos.</p> <p>El oferente debe adjuntar en documento independiente en la oferta, certificado de fábrica que indique que es canal certificado Check Point Certified Support Provider (CSP/CCSP) y que está autorizado para distribuir con un nivel de experiencia profesional o superior y dar soporte de los productos relacionados en la presente especificación técnica.</p> <p>El oferente deberá presentar carta del fabricante de la solución propuesta la cual avale la solución ofertada para el cumplimiento de todas las características técnicas.</p> <p>El contratista durante los primeros 5 días después de formalizado el contrato se compromete a entregar al supervisor una certificación o documento que soporte la compra de la solución propuesta expedido por el fabricante.</p>
13	<p>SERVICIO DE MIGRACIÓN E IMPLEMENTACIÓN:</p>
13.1	<p><u>Implementación del Proyecto</u></p> <p>El contratista junto con el supervisor debe realizar un plan de trabajo de la propuesta de implementación del proyecto garantizando la integración de cada una de las capacidades y herramientas que se deben integrar con la seguridad perimetral.</p> <p>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.</p> <p>Antes de realizar una implementación el contratista debe garantizar compatibilidad con la infraestructura y arquitectura tecnológica actual e indicar que el presente proceso es para fortalecer e integrar la seguridad perimetral con la que cuenta actualmente el Ejército Nacional.</p> <p>El contratista asumirá los costos que genere las integraciones con las tecnologías que posee el Ejército Nacional que sean necesarias para el óptimo funcionamiento de todas las tecnologías.</p> <p>El contratista debe entregar un diagrama técnico detallado donde sea representado gráficamente cada uno de los componentes de Hardware y Software con sus correspondientes conexiones de red (datos y de potencia), con el propósito de proporcionar información suficiente para facilitar su análisis, mantenimiento e integración con las demás herramientas con las que cuenta el Ejército Nacional.</p> <p>El contratista debe garantizar que los dispositivos de hardware ofertados como appliance deben tener las características y elementos para montaje en rack estándar, e incluir sus cables de alimentación eléctrica, cables para datos tipo RJ45, convertidores RJ45 a RJ .5 y cables de fibra óptica necesarios para su correcta operación y funcionalidad de acuerdo al diseño lógico y físico ofrecido. Así mismo deben ser instalados y configurados todos los elementos de las soluciones, lo cual no incurrirá en costos adicionales para el</p>

	<p>Ejército Nacional.</p> <p>Las soluciones a implementar deben ser compatibles con las plataformas actuales del Ejército Nacional y cumplir con el protocolo IPv4 e IPV6.</p> <p>Para la implementación y conectorización eléctrica no se podrán realizar apagados del centro de datos, por lo cual toda la actividad de implementación se debe realizar en producción sin afectar los servicios del centro de cómputo previa coordinación con el supervisor del contrato. De ser necesario un apagado programado, este debe ser coordinado con el supervisor del contrato.</p>
13.2	<p><u>Caso de Fallas</u></p> <p>Los daños ocasionados por la implementación, desarrollo y puesta en marcha del contrato a cualquier elemento o sistema existente en la entidad serán asumidos por el contratista sin costo alguno para la entidad.</p> <p>El Contratista en caso de que al momento de las pruebas o instalación de las soluciones si algún equipo sale defectuoso el contratista está en la obligación de reemplazar los equipos por uno de las mismas características y/o superiores en un plazo no mayor a 30 días. El equipo no puede ser remanufacturado o reparado debe ser totalmente nuevo y deberá enviar los números de seriales para realizar los cambios pertinentes administrativos en el Ejército Nacional.</p> <p>En caso de presentarse fallas en cualquiera de los elementos que componen el sistema, se deberán efectuar los soportes todas las veces que se requiera; estos soportes deben incluir como mínimo:</p> <ul style="list-style-type: none"> Cambio de equipos en caso de fallas. Remplazo de equipos por otros de iguales o superiores características. Instalación de software. <p>Configuraciones, puesta en producción y funcionamiento</p> <p>En caso de falla de alguno de los equipos, el fabricante deberá proporcionar los materiales y/o piezas para su reparación o reemplazo de características iguales o superiores.</p> <p>En el caso de un reemplazo o adquisición de un nuevo appliance para el arreglo, la solución debe incorporarlo al Clúster en menos de 10 minutos, minimizando la intervención humana dentro del proceso.</p>
13.3	<p><u>Migración:</u></p> <p>El contratista deberá realizar una reunión inicial para el levantamiento de información y planificación para la implementación de la solución.</p> <p>El contratista deberá entregar un plan de trabajo y cronograma de trabajo donde se evidencien los recursos, tiempos, requisitos, factores críticos de éxito y responsables del proceso de implementación</p> <p>El contratista aplicara las mejoras prácticas de seguridad y ajustarlas a las políticas de seguridad informática de seguridad informática del Ejército Nacional.</p> <p>El contratista deberá integrar los equipos a la red y configurará el enrutamiento y la dirección IP.</p>

	<p>El contratista deberá contemplar dentro de su oferta todo el costo asociado al cableado estructurado, patch cord de cobre, fibra ópticas y demás elementos que se requiera para la implementación y puesta en funcionamiento de la solución la integración con Dos y el SW CORE que cuenta el Ejército Nacional</p> <p><u>Integración:</u> <u>Realizar una correcta instalación:</u> Es importante realizar una correcta instalación de la solución, siguiendo las instrucciones proporcionadas por el fabricante y verificando que se cumplan los requisitos de hardware y software.</p> <p><u>Configuración adecuada:</u> La configuración de la solución debe realizarse de manera adecuada, considerando las políticas de seguridad existentes en la organización y las necesidades de la red.</p> <p><u>Pruebas de integración:</u> El contratista en conjunto con el supervisor del contrato debe realizar pruebas de integración para comprobar la eficacia de la solución en la infraestructura existente y asegurarse de que la solución esté proporcionando el servicio esperado.</p>
14	TRANSFERENCIA DE CONOCIMIENTO
14.1	<p>El Contratista debe realizar transferencia de conocimiento para 02 personas, del Batallón de Ciberdefensa y Ciberseguridad del Ejército Nacional curso CCSE, dictado directamente por el canal implementador en las instalaciones adecuadas por mínimo 40 horas. Se debe expedir certificado por parte de fábrica.</p>
15	RECURSOS HUMANOS
15.1	<ul style="list-style-type: none"> Implementación: La implementación debe ser realizada por el contratista de acuerdo a los siguientes perfiles, de la cual el oferente deberá presentar junto con la oferta los siguientes requerimientos: <p><u>Líder o gerente del Proyecto:</u> Profesional responsable de coordinar y supervisar la ejecución del contrato, así como de comunicarse con el supervisor del contrato para garantizar el cumplimiento de los objetivos y las obligaciones establecidas, encargado de la implementación de la tecnología a adquirir y con quien se gestionarán el cumplimiento del objeto del contrato, debe cumplir con los siguientes requisitos:</p> <ul style="list-style-type: none"> ✓ Se requiere que el rol del líder o gerente del proyecto, la realice como mínimo un (01) ingeniero con el siguiente perfil: Ingeniero electrónico y/o de sistemas y/o telecomunicaciones o afines, con fecha de expedición en tarjeta profesional superior a cuatro (04) años. ✓ Debe haber sido líder técnico de proyectos de seguridad. ✓ Debe acreditar al menos tres (3) certificaciones o más de experiencia relacionada con la implementación o soporte u operación o administración de la solución adquirir <p><u>Implementación:</u> Profesional operativo que se encargará de la implementación y despliegue de la solución a adquirir, generación de reglas y políticas, configuración de reglas y generación de estándares para la clasificación sensible de activos de información, aplicación de buenas prácticas de seguridad.</p> <ul style="list-style-type: none"> ✓ Se requiere que la implementación de la solución, la realice como mínimo uno (01) ingenieros con el siguiente perfil: Ingeniero electrónico y/o de sistemas y/o telecomunicaciones o afines, con fecha de expedición en tarjeta profesional superior a tres (03) años.

	<ul style="list-style-type: none"> ✓ Debe acreditar al menos tres (3) certificaciones o más de experiencia relacionada con la implementación o soporte u operación o administración de redes o seguridad de informática o implementación de la solución. ✓ Deberá contar con las siguientes certificaciones: <ul style="list-style-type: none"> ○ Debe contar con la certificación nivel experto CCSE y CCTE (vigentes a la fecha de cierre del proyecto) ○ Debe haber participado en mínimo un proyecto de implementación o soporte de firewalls virtuales ○ Certificación CCNP. ○ Certificación o constancia de entrenamiento en la solución ofertada emitido por el fabricante o por un ente certificador autorizado por el fabricante <p><u>Soporte:</u> Profesional operativo que se encargará posterior a la implantación, de las labores de mantenimiento de la solución instalada, garantizando el correcto funcionamiento y velando por que las políticas y configuraciones de acuerdo a requerimientos del Supervisor, durante la vigencia de ejecución del contrato hasta el término de la garantía, y de acuerdo con los términos y tiempos de respuesta especificados en el ítem 3.2.16.2 en el documento de Especificaciones técnicas.</p> <ul style="list-style-type: none"> ✓ Se requiere que el ingeniero soporte de la solución, la realice como mínimo un (01) ingeniero con el siguiente perfil: Ingeniero electrónico y/o de sistemas y/o telecomunicaciones o afines, con fecha de expedición en tarjeta profesional superior a dos (02) años. ✓ Debe adjuntar certificación CCSE (Check Point Certified Security Expert) y/o certificación CCSA (Check Point Security Administrator y/o CCTE (Check Point Certified Troubleshooting Expert y/o CCSM (Check Point Certified Security Masters). ✓ Debe acreditar al menos dos (2) certificaciones o más de experiencia relacionada con la implementación o soporte u operación o administración de soluciones de redes o seguridad de informática o implementación de seguridad perimetral. <p><u>ALCANCE SOPORTE</u></p> <p>Se debe desarrollar como mínimo las siguientes actividades durante la vigencia del contrato preveía autorización y aprobación del supervisor del contrato:</p> <ul style="list-style-type: none"> • Administración de plataformas de seguridad perimetral firewalls: responsable de las tareas de comprobación de funcionamiento, administración, gestión, control y aplicación de las plataformas de seguridad perimetral firewall. • Generar recomendaciones para las buenas prácticas de administración de políticas en las plataformas de seguridad perimetral firewall. • Monitorizar el funcionamiento de la plataforma de seguridad perimetral firewalls. • Revisión, control y mantenimiento de la estabilidad y operación de las plataformas de seguridad informática descritas. • Generar recomendaciones para la actualización de las plataformas de seguridad perimetral firewalls del Ejército Nacional. • Configuración de políticas, realizar evaluación y ajuste de la configuración de las políticas de seguridad implantadas en todas las plataformas de seguridad perimetral firewalls, bajo la supervisión del administrador de Seguridad del Ejército Nacional.
--	--

	<ul style="list-style-type: none"> • Atención a solicitudes: Para ello evaluará y ejecutará nuevos requerimientos de configuración sobre las plataformas de seguridad perimetral firewalls. • Seguimiento de backups: Gestionar y efectuar las copias de resguardo (back-up) de la información de las herramientas de seguridad del sistema y de completar la documentación correspondiente a esta tarea. • Integración del Directorio Activo con las plataformas de Seguridad Perimetral Firewalls del Ejército Nacional. • Revisión y seguimiento de políticas de passwords: El administrador de seguridad deberá realizar periódicamente un seguimiento de la implementación de las políticas de passwords, con el propósito de verificar que las mismas se encuentran en fase con lo definido. • Seguimiento de la actualización de herramientas de seguridad: el administrador de seguridad será el responsable de verificar que las herramientas de seguridad descritas en este documento, se encuentren en regla y actualizados con los correspondientes soportes y mantenimientos ejecutados por el proveedor del contrato de soporte y mantenimiento. • Afinamiento a la infraestructura de seguridad perimetral Firewalls actual. • Nuevas configuraciones o activaciones de nuevas funcionalidades del producto, previa coordinación con el personal técnico y el supervisor del contrato. • Pruebas de puesta en funcionamiento de nuevos servicios de seguridad perimetral firewall. • Realizar levantamiento de la topología de red de la infraestructura de seguridad perimetral Firewalls del Ejército Nacional. • Sugerir recomendaciones en coordinación con la administración de seguridad perimetral y el supervisor del contrato para implementar nuevas políticas de firewalls, mejoramiento IPS y control de aplicaciones. • Atención ilimitada a casos reportados por el Batallón de Ciberdefensa y Ciberseguridad (BACCI) del Ejército Nacional referentes a cualquier evento relacionado con el funcionamiento, administración e incidentes o eventos de seguridad de la plataforma de seguridad informática. <p>ALCANCE MANTENIMIENTO PREVENTIVO:</p> <p>El contratista debe efectuar dos (02) mantenimiento preventivo durante la ejecución del contrato según cronograma acordado entre el contratista y el supervisor del contrato a las plataformas de seguridad perimetral Firewalls del Ejército Nacional.</p> <p>Este mantenimiento debe incluir como mínimo las siguientes actividades:</p> <ul style="list-style-type: none"> • 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. • El contratista deberá suministrar el recurso en sitio donde se requiera realizar este mantenimiento se podrán realizar de manera remota, pero si algo falla y no se puede subsanar el contratista desplazará al personal especializado hasta el sitio.
--	--

<p>ALCANCE MANTENIMIENTO CORRECTIVO:</p> <p>En caso de presentarse fallas en los sistemas de seguridad perimetral firewall del Ejército Nacional, el contratista deberá efectuar los mantenimientos correctivos todas las veces que se requiera.</p> <p>Estos mantenimientos deben incluir como mínimo:</p> <ul style="list-style-type: none"> • Instalación de software • Configuraciones, puesta en producción y funcionamiento • Remplazo de equipos por otro de iguales características de forma temporal hasta que la falla sea solucionada. <p>Nota1: Los ingenieros deben ser de nacionalidad colombiana</p> <p>Nota2: El oferente deberá presentar junto con la oferta las hojas de vida con sus respectivas certificaciones académicas y de experiencia laboral en las funciones requeridas para los anteriores perfiles:</p> <p><u>Para realizar la validación correspondiente del personal requerido, el oferente debe aportar la siguiente documentación del personal encargado de estas actividades.</u></p> <p>Copia legible del diploma de pregrado como ingeniero de sistemas, o electrónico, o de telemática, o comunicaciones y/o afines conforme al SNIES a estas profesiones.</p> <ul style="list-style-type: none"> • Copia legible de la tarjeta profesional • Copia de cédula de ciudadanía que verifique la nacionalidad colombiana. • Carta de compromiso de participación del personal firmada por la profesional dirigida al proceso. • La experiencia se deberá certificar considerando los siguientes aspectos que se relacionan a continuación: <ul style="list-style-type: none"> ▪ Nombre o razón social del contratante ▪ Descripción de las actividades realizadas ▪ Fecha de iniciación del contrato ▪ Fecha de terminación del contrato ▪ Dirección y teléfono de quién expide la certificación <p>Otras obligaciones del contratista:</p> <p>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.</p> <p>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.</p> <p>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 especiaciones requeridas.</p> <p>El supervisor evaluará el desempeño laboral del profesional asignado para el soporte y estará en facultad de solicitar su remplazo 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</p>
--

	del contrato.
--	---------------

ARTÍCULO SEGUNDO: Modifíquese el cronograma del proceso, así:

ETAPA	FECHA	LUGAR
PUBLICACIÓN ESTUDIO PREVIOS, PROYECTO PLIEGO DE CONDICIONES Y AVISO DE CONVOCATORIA 1	06 DE JUNIO DE 2024	En el portal del Sistema Electrónico para la contratación Pública II (SECOPII): www.colombiacompra.gov.co
OBSERVACIONES PRESENTADAS AL PROYECTO PLIEGO DE CONDICIONES	25 DE JUNIO DE 2024 DE HASTA las 19.00 HORAS	En el portal del Sistema Electrónico para la contratación Pública II (SECOPII): www.colombiacompra.gov.co
RESPUESTA A LAS OBSERVACIONES PRESENTADAS AL PROYECTO DE PLIEGO DE CONDICIONES ESTUDIOS PREVIOS	27 DE JUNIO DE 2024	En el portal del Sistema Electrónico para la contratación Pública II (SECOPII): www.colombiacompra.gov.co
PUBLICACIÓN RESOLUCIÓN DE APERTURA Y PLIEGOS DEFINITIVOS	28 DE JUNIO DE 2024	En el portal del Sistema Electrónico para la contratación Pública II (SECOPII): www.colombiacompra.gov.co
AUDIENCIA DE ASIGNACIÓN DE RIESGOS	04 DE JULIO DE 2024 a las 08:00 am	En las instalaciones del CENAC DE TELEMATICA Carrera 15 No. 05-00 cantón De comunicaciones ciudad de Facatativá Cundinamarca
PLAZO PARA PRESENTAR OBSERVACIONES AL PLIEGO DE CONDICIONES DEFINITIVO	04 DE JULIO DE 2024 HASTA LAS 19:00 HORAS	En el portal del Sistema Electrónico para la contratación Pública II (SECOPII): www.colombiacompra.gov.co
RESPUESTA A LAS OBSERVACIONES PRESENTADAS PLIEGO DE CONDICIONES DEFINITIVOS	08 DE JULIO DE 2024 HASTA LAS 18:00 HORAS	En el portal del Sistema Electrónico para la contratación Pública II (SECOPII): www.colombiacompra.gov.co
PLAZO PARA EXPEDIR ADENDAS	09 DE JULIO DE 2024 A LAS 11:00 HORAS	En el portal del Sistema Electrónico para la contratación Pública II (SECOPII): www.colombiacompra.gov.co
PLAZO PARA LA ENTREGA DE PROPUESTAS (CIERRE DEL PROCESO)	15 DE JULIO DE 2024 A LAS 11:00 HORAS	En el portal del Sistema Electrónico para la contratación Pública II (SECOPII): www.colombiacompra.gov.co
PUBLICACION EVALUACIÓN DE OFERTAS	19 DE JULIO DE 2024 A LAS 19:00 HORAS	Procedimiento interno de la Unidad.
TRASLADO DEL INFORME DE EVALUACIÓN, OBJECIONES AL INFORME DE EVALUACIÓN Y PLAZO PARA SUBSANAR	DESDE EL 22 DE JULIO DE 2024 HASTA EL 26 DE JULIO DE 2024 a las 19:00 HORAS	En el portal del Sistema Electrónico para la contratación Pública II (SECOPII): www.colombiacompra.gov.co
AUDIENCIA DE ADJUDICACIÓN O DECLARATORIA DE DESIERTO.	30 DE JULIO DE 2024 A LAS 10:00 HORAS	En las instalaciones del CENAC DE TELEMATICA Carrera 15 No. 05-00 cantón De comunicaciones ciudad de Facatativá Cundinamarca.
RESOLUCIÓN DE ADJUDICACIÓN	30 DE JULIO DE 2024 HASTA LAS 19:00 HORAS	
SUSCRIPCIÓN DEL CONTRATO	05 DE AGOSTO DE 2024	SUSCRIPCIÓN DEL CONTRATO
SUSCRIPCIÓN DE LA GARANTÍA ÚNICA DE CUMPLIMIENTO	12 DE AGOSTO DE 2024	SUSCRIPCION DE LA GARANTIA UNICA DE CUMPLIMIENTO

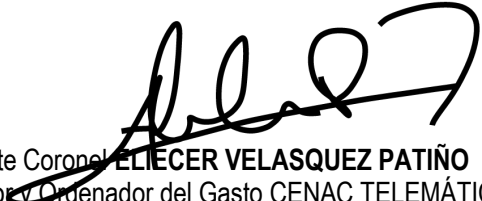
PATRIA HONOR LEALTAD

Calle 5 No 15 – 00 Barrio Dos caminos – Facatativá – Cundinamarca.
Conmutador 4261428 Ext. 39036
Correo electrónico de la unidad cenactel@buzonejercito.mil.co



ARTÍCULO TERCERO: Los demás numerales, parágrafos y párrafos contenidos en los documentos del proceso que no se modifiquen en esta adenda, continúan vigentes y sin modificaciones.

Dada en Facatativá, a los 09 días del mes de julio de 2024


Teniente Coronel **ELIECER VELASQUEZ PATIÑO**
Director y Ordenador del Gasto CENAC TELEMÁTICA


Teniente Coronel **RAMIRO ESTEBAN SILVA GUTIERREZ**
Gerente de Proyecto.


PD06. **JOSÉ EDINSON ROJAS CALDON**
Comité Técnico estructurador


AS. **LEIDY OLAYA GALDERON**
Comité Jurídico Estructurador

Martha lucia ramos Gonzalez
AS. **MARTHA LUCIA RAMOS GONZALEZ**
Comité Económico Estructurador

Vo.Bo.


MY. **EDWIN ANDRES RINCON CEPEDA**
Oficial de Contratación CENAC TELEMÁTICA

PATRIA HONOR LEALTAD

Calle 5 No 15 – 00 Barrio Dos caminos – Facatativá – Cundinamarca.
Conmutador 4261428 Ext. 39036
Correo electrónico de la unidad cenactel@buzonejercito.mil.co

