**ANEXO ESPECIFICACIONES TECNICAS DE OBLIGATORIO CUMPLIMIENTO**

Facatativá XX de XXXXX de 2023

(El apoderado o representante legal), obrando en nombre y representación de conformidad con lo establecido en la Invitación a ofertar, 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 la FICHA TÉCNICAS "**RENOVACIÓN DEL LICENCIAMIENTO, MANTENIMIENTO Y SOPORTE DE LA PLATAFORMA DE SEGURIDAD INFORMÁTICA Y SANDBLAST DE LA UNIDAD DE CIBERDEFENSA DEL EJÉRCITO NACIONAL "No. JEMPP-CEDE4-DIETE-ET-1485/ COMUN-02**la cual contiene los parámetros técnicos que deben cumplir los oferentes en la acreditación de los servicios a prestar, así mismo, el contenido es el mismo del **ANEXO ESPECIFICACIONES TÉCNICAS** los cuales se describen a continuación:

## REQUISITOS GENERALES

Renovar el licenciamiento, realizar el mantenimiento y soporte de los productos de CheckPoint de la plataforma de seguridad informática de la Unidad de Ciberdefensa del Ejercito Nacional, de acuerdo a cada uno de los numerales de los requisitos específicos de la presente especificación técnica.

## REQUISITOS ESPECÍFICOS

<table>
<tr><th colspan="2">RENOVACION DEL LICENCIAMIENTO MANTENIMIENTO Y SOPORTE DE LA PLATAFORMA DE SEGURIDAD INFORMÁTICA Y SANDBLAST DEL BATALON DE CIBERDEFENSA Y CIBERSEGURIDAD DEL EJÉRCITO NACIONAL</th></tr>
<tr><th colspan="2">ITEM 1. RENOVACIÓN DE LICENCIAMIENTO</th></tr>
<tr><td colspan="2">La presente ítem de la especificación técnica tiene como objeto la renovación del licenciamiento, de la plataforma de seguridad informática y sandblast del Batallón de Ciberdefensa y Ciberseguridad del Ejército Nacional.</td></tr>
<tr><td colspan="2">Consiste en todas aquellas tareas de actualización de la plataforma, módulos, herramientas y servicios con los que cuenta el Ejército Nacional relativas a la plataforma de seguridad informática y su gestión, garantizando la disponibilidad 100% de la plataforma.</td></tr>
<tr><td>1.1</td><td>ALCANCE:<br>El contratista debe brindar la renovación del licenciamiento de los siguientes productos:<br><br>Collaborative Enterprise Support – Standard y renovación del licenciamiento para la plataforma Check Point.</td></tr>
<tr><td>1.2</td><td>El Contratista será el encargado de verificar y certificar al Ejército Nacional que no existirá sub-licenciamiento de la plataforma, en caso de ser así el costo deberá ser asumido por el contratista.</td></tr>
<tr><td>1.3</td><td>El Contratista deberá rendir un informe al Ejército<br><br>
<table>
<tr><th>Product Type</th><th>Device Number</th><th>Product</th></tr>
<tr><td>5600 Appliances</td><td>00:1C:7F:82:43:7D</td><td>CPAP-SG5600-NGTP</td></tr>
<tr><td>5600 Appliances</td><td>00:1C:7F:82:43:91</td><td>CPAP-SG5600-NGTP</td></tr>
</table>
</td></tr>
</table>

| | | | |
|---|---|---|---|
| | Threat Emulation Appliances | 00:1C:7F:55:0B:BF | CPAP-SBTE2000X-56VM-HPP |
| | Threat Emulation Appliances | 00:1C:7F:86:B1:89 | CPAP-SBTE2000X-56VM-HPP |
| | Threat Emulation Appliances | 00:1C:7F:86:B1:8D | CPAP-SBTE2000X-56VM-HPP |
| | Smart-1 5050 Appliances | 24:6E:96:D1:45:97 | CPAP-NGSM5050 |
| | Software Products | F48458F13EE5 | CPSM-NGSM50-EVNT |
| | Nacional, dirigido al CEDE6 con Copia a la Batallón de Ciberdefensa y Ciberseguridad del Ejército Nacional, en donde certifique la funcionabilidad de la plataforma, la instalación de la renovación de las licencias y el no sub-licenciamiento con sus respectivos soportes. | | |
| 1.4 | El Contratista deberá informar al momento de la implementación de la renovación al Ejército Nacional sobre la aplicabilidad de las políticas del fabricante publicadas en Internet sobre el uso de su tecnología, de su funcionamiento y licenciamiento con el fin de no incurrir en omisión de las políticas emitidas por el fabricante, para lo cual estas deberán ser presentadas en la ejecución del contrato. | | |
| 1.5 | El Contratista deberá garantizar el normal funcionamiento de la plataforma después de la actualización e instalación del licenciamiento, de no ser así el contratista deberá cubrir los gastos (Equipos, configuraciones, horas ingenieros) que se generan hasta restablecer el funcionamiento de la plataforma en un tiempo no mayor a 24 horas. | | |
| 1.6 | EL contratista durante los primeros 5 días después de formalizado el contrato se compromete a entregar al supervisor una certificación o documento que soporte el registro de la renovación del licenciamiento para la plataforma de seguridad informática expedido por el Fabricante. | | |
| 1.7 | **CERTIFICACIONES PARTNER**<br>El oferente debe adjuntar en documento independiente en la oferta, certificado de fábrica que indique que es canal certificado en la plataforma Check Point y que está autorizado para distribuir y dar soporte de los productos relacionados en la presente especificación técnica. | | |
| 1.8 | **CUMPLIMIENTO DE NORMATIVIDAD GUBERNAMENTAL EN MATERIA DE TICS**<br>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." | | |
| 1.9 | **CONFIDENCIALIDAD DE LA INFORMACIÓN**<br>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".<br><br>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.<br><br>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.<br><br>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.<br><br>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. |
| 1.10 | **PROPIEDAD INTELECTUAL**<br>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.<br><br>En particular, toda aquella documentación generada por intervenciones del personal asignado al servicio en el Ejército, será propiedad de este, por tanto, no podrá ser facilitada a otra persona o entidad sin consentimiento expreso del Ejército.<br><br>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.<br><br>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. |
| **ITEM 2. MANTENIMIENTO PREVENTIVO , CORRECTIVO Y SOPORTE DE LA PLATAFORMA DE SEGURIDAD INFORMÁTICA Y SANDBLAST DEL BATALLÓN DE CIBERDEFENSA Y CIBERSEGURIDAD DEL EJÉRCITO NACIONAL** | |
| 2.1 | **ALCANCE SOPORTE TÉCNICO**:<br>El contratista debe brindar atención ilimitada a casos reportados por el Batallón de Ciberdefensa y Ciberseguridad del Ejército referentes a cualquier evento relacionado con el funcionamiento, administración e incidentes o eventos de seguridad de las plataformas de seguridad informática descritas en el ítem No. 1.1 de la presente especificación técnica. |

| | |
|---|---|
| 2.2 | **CERTIFICACIONES PARTNER**<br>El proponente debe adjuntar en documento independiente en la oferta, certificación expedida por el fabricante, que lo acredite como canal certificado CCSP (Certified Collaborative Support Provider) como mínimo con un nivel 2 estrellas, donde indique que se encuentra autorizado para brindar soporte y realizar la apertura de casos y escalamientos a fabrica; dicha certificación no debe ser superior a tres (3) meses, con relación a la fecha de presentación de la oferta.<br><br>El proponente deberá anexar a su oferta certificación expedida por el fabricante donde indique que cuenta con experiencia en VSX – Check Point en al menos 1 proyecto de diferente cliente final. |
| 2.3 | **MANTENIMIENTO PREVENTIVO, CORRECTIVO Y SOPORTE TÉCNICO:**<br>El contratista debe ofrecer el servicio de mantenimiento preventivo, correctivo y soporte técnico para los sistemas y/o productos y descritos en el ítem No. 1.1<br><br>**TIPO DE ATENCIÓN**: El servicio será prestado de dos formas así: |
| | • Soporte Nivel 1: De manera presencial tres días a la semana con duración de 4 horas laborales (3x4) 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<br><br>• 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, y de acuerdo con los términos y tiempos de respuesta especificados en el numeral 2.9.<br><br>Para este soporte el contratista deberá suministrar un servicio de asistencia técnica con personal certificado para atender necesidades específicas de la plataforma. |
| 2.4 | **PERSONAL REQUERIDO: PERFIL INGENIERO PARA EL SOPORTE NIVEL 1 Y 2**<br>• Formación profesional: Ingeniero en sistemas y/o electrónica y/o telecomunicaciones y/o afines según SNIES, para el cual deberá anexar a la oferta lo siguiente:<br>• Copia de diploma y/o acta de grado del ingeniero presentado en la propuesta.<br>• El ingeniero presentado en la propuesta deberá contar con conocimientos avanzados en los productos descritos en el ítem 1.1, dado que el administrador de seguridad apoyará la operación y administración de la plataforma CheckPoint.<br>• Debe adjuntar copia de certificación CCSE (Check Point Certified Security Expert) y/o certificación CCSM (Check Point Certified Security Masters)<br>• Debe adjuntar experiencia en al menos uno (1) proyecto en implementación y/o soporte de VSX<br>• El ingeniero debe ser de nacionalidad Colombiana, y pertenecer por nomina al proponente<br>• Cantidad: Mínimo dos (2) ingenieros. Uno de los dos debe contar con certificación Check Point Certified VSX Specialist<br><br>• HOJA DE VIDA: El oferente deberá allegar en la propuesta, la hoja de vida del personal requerido incluyendo datos de contacto (teléfonos, correos y cada una de las certificaciones anteriormente relacionadas). |

| | |
|---|---|
| 2.5 | **ACTIVIDADES DEL SERVICIO DE SOPORTE**:<br>Se debe desarrollar como mínimo las siguientes actividades durante la vigencia del contrato:<br>• Administración de plataformas de seguridad: responsable de las tareas de comprobación de funcionamiento, administración, gestión, control y aplicación de las plataformas de seguridad informática descritas<br>• El administrador de seguridad apoyará la operación y administración de la plataforma de seguridad informática Check Point.<br>• Monitorizar el funcionamiento de la plataforma de seguridad informática.<br>• Revisión, control y mantenimiento de la estabilidad y operación de las plataformas de seguridad informática descritas<br>• Apoyo a la actualización de las plataformas de seguridad informática descritas |
| | • Configuración de políticas, evaluación y ajuste de la configuración de las políticas de seguridad implantadas en todas las plataformas de seguridad informática descritas, bajo la supervisión del administrador de Seguridad del Ejército Nacional.<br>• Atención a solicitudes: Para ello evaluará y ejecutará nuevos requerimientos de configuración sobre las plataformas de seguridad informática<br>• 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.<br>• 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.<br>• 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.<br>• Afinamiento a la infraestructura de seguridad actual.<br>• Nuevas configuraciones o activaciones de nuevas funcionalidades del producto, previa coordinación con el supervisor del contrato.<br>• Pruebas de puesta en funcionamiento de nuevos servicios<br>• El contratista debe brindar 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 Check Point. |

| | |
|---|---|
| 2.6 | **OBLIGACIONES GENERALES DEL CONTRATISTA:**<br>• En caso de un ataque cibernético relacionado con las plataformas de seguridad descritas en el ítem 1.1, el contratista debe proveer en las instalaciones del Ejército Nacional, un ingeniero certificado en la plataforma, para que verifique la situación en un plazo no mayor a tres (3) horas y dejar solucionado el problema en un lapso no mayor a veinticuatro (24) horas, a menos de que se trate de un ataque de día cero en donde no se conoce ni una causa ni una solución al inconveniente presentado. En el caso de que el ataque deje rastro o daños en los servidores o máquinas de usuario, el contratista deberá apoyar en la puesta en marcha y funcionalidad de los equipos.<br>• De presentarse una situación de cualquier naturaleza que llegue a afectar la infraestructura del Ejército Nacional, el contratista deberá proporcionar todo el recurso humano y tecnológico necesario, hasta la restauración del servicio objeto del alcance de la presente especificación técnica.<br>• El contratista atenderá de manera ilimitada requerimientos en cuanto a configuraciones, administración, validaciones con el fin de descartar ataques no conocidos, dudas y demás solicitudes por parte del Ejército Nacional, los cuales podrán ser asistidos de manera remota a menos de que se presente una situación en la que después de agotar el recurso remoto se requiera personal en sitio. |
| 2.7 | **ALCANCE MANTENIMIENTO PREVENTIVO:**<br>El contratista debe efectuar un (01) mantenimiento preventivo durante la ejecución del contrato según cronograma acordado entre el contratista y el supervisor del contrato a las plataformas de seguridad informática descritas en el ítem 1.1.<br>Este mantenimiento debe incluir como mínimo las siguientes actividades:<br>• Actualizaciones de software (Upgrade, Update, criticas de seguridad)<br>• Revisiones del funcionamiento de las plataformas y solución de errores<br>• Realización y programación de copias de seguridad<br>• Revisión de los logs de eventos registrados en los sistemas<br>• Revisión y mejoramiento de espacio de disco, utilización de CPU – RAM y afinamiento de servidores.<br>• Evaluación de los sistemas de seguridad instalados<br>• Configuración de funcionalidades inoperativas.<br>• Emisión de recomendaciones de las plataformas a través de un informe técnico, al supervisor del contrato.<br>**Nota:** 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**.** |

| | |
|---|---|
| 2.8 | **ALCANCE MANTENIMIENTO CORRECTIVO:**<br>En caso de presentarse fallas en los sistemas de seguridad descritos en el ítem 1.1, el contratista deberá efectuar los mantenimientos correctivos todas las veces que se requiera.<br><br>Estos mantenimientos deben incluir como mínimo:<br><br>• Instalación de software<br>• Configuraciones, puesta en producción y funcionamiento<br>• Remplazo de equipos por otro de iguales características de forma temporal hasta que la falla sea solucionada. |
| 2.9 | **TERMINOS Y TIEMPOS DE RESPUESTA:**<br><br>**Horario del servicio**: En disponibilidad de horario 7x24 (7 días a la semana las 24 horas del día) durante la vigencia de ejecución del contrato.<br><br>**Tipo de atención**: El servicio será en la ciudad de Bogotá y remotamente a través de herramientas WEB online; de acuerdo con los tiempos de respuesta.<br><br>**Tiempos de respuesta**: El servicio de soporte debe ser atendido de manera inmediata a través de una línea telefónica gratuita, servicio de correo electrónico o en forma remota de acuerdo a los niveles de servicio. Para las Unidades Militares de la ciudad de Bogotá, si en el lapso de cuatro (04) horas después de haber reportado el incidente no se da solución al mismo, el contratista deberá enviar personal técnico especializado a sitio en un tiempo máximo de dos (02) horas. |
| | El tiempo máximo permitido para restablecer el servicio en las unidades de Bogotá es de ocho (08) horas, una vez el recurso haya llegado al sitio.<br><br>El tiempo máximo permitido para el reemplazo temporal de equipos estipulado en el ítem 2.8 es de tres (03) días.<br><br>**Nota**: El tipo de atención y tiempos de respuesta será asignado según las anteriores clasificaciones por el funcionario de la unidad de Ciberseguridad y Ciberdefensa que reporta el incidente. |
| 2.10 | **EVALUACIÓN DEL RECURSO HUMANO:**<br>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 en facultad de solicitar su reemplazo, si esta(s) no cumple(n) con las expectativas del Batallón de Ciberdefensa y Ciberseguridad del Ejército Nacional.<br>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 un tiempo no mayor a 5 días calendarios**.** |

| | |
|---|---|
| 2.11 | **DOCUMENTACIÓN:**<br>• INFORME DE MANTENIMIENTOS Y SOPORTE TÉCNICO: Una vez realizados los soportes técnicos y mantenimientos tanto correctivos como preventivos (remotos o en sitio) el contratista deberá hacer entrega de un informe técnico donde se indique las actividades realizadas, observaciones y pendientes, donde se indique como mínimo:<br><br>o Actividades realizadas<br>o Actualizaciones aplicadas<br>o Procedimientos preventivos y/o correctivos aplicados<br>o Recomendaciones<br>o Registro fotográfico y/o pantallazos de las herramientas<br><br>Este informe deberá entregarse al supervisor del contrato por cada mantenimiento realizado el día hábil siguiente a la realización del mantenimiento o soporte técnico.<br><br>**INFORME MENSUAL DE ACTIVIDADES**: El contratista debe entregar informe mensual (último día hábil del mes) al supervisor del contrato con las actividades realizadas tanto en los mantenimientos como de los soportes técnicos realizados, así como de las actividades de apoyo en la administración y operación de las plataformas objeto de la presente especificación técnica.<br>Si el supervisor del contrato requiere un informe adicional, el contratista estará en la obligación de entregar mencionado informe.<br>**Nota**: cada informe entregado debe ser firmado por el ingeniero o líder del proyecto o representante legal de la empresa y debe incluir fecha de elaboración. |
| 2.12 | **ACTUALIZACIÓN GRUPO DE TRABAJO**:<br>El contratista brindara servicio de actualización al grupo de trabajo en la plataforma Check Point con la que cuenta el Batallón de Ciberdefensa y Ciberseguridad del Ejército Nacional, en sitio acordado entre el supervisor y el contratista para los administradores de la herramienta con una duración de 20 horas. Esto no generara costo adicional al Ejercito Nacional |
| 2.13 | **FUNCIONAMIENTO Y CONTINUIDAD**:<br>Garantizar el perfecto funcionamiento y la continuidad de la plataforma, los procesos y servicios prestados en la misma, así mismo si las fallas presentadas son ocasionadas por las actividades efectuadas por el soporte o mantenimiento producto del contrato, por parte del proveedor, durante la vigencia del contrato. |
| 2.14 | **CUMPLIMIENTO DE NORMATIVIDAD GUBERNAMENTAL EN MATERIA DE TICS**:<br>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." |

El OFERENTE

_____

REPRESENTANTE LEGAL O APODERADO
Nombre
Identificación Razón social
C.C. / NIT XXXXXXX