PLATAFORMA SEGURIDAD INFORMÁTICA



ESPECIFICACIÓN TÉCNICA

DIRECCIÓN DE ESTRUCTURACIÓN TÉCNICA

DEPARTAMENTO DE LOGÍSTICA

CEDE 4

Fuente de Imagen: Ejército Nacional de Colombia.

ORGANIZACIÓN - DISCIPLINA - PUNTUALIDAD

CONTENIDO

1. OBJETO 3
2. DEFINICIONES Y APLICACIÓN 3
3. REQUISITOS 3
4. TOMA DE MUESTRAS Y CRITERIO DE ACEPTACIÓN O RECHAZO: 9
5. MÉTODOS DE ENSAYO 9
6. APÉNDICE 9
7. ANEXOS 10
8. CONTROL DE REVISIONES 10

Elaboró	Revisó	Aprobó
CP. Jonathan Alexander Quintero Albarracin Comité Técnico Estructurador	**TE. Carlos Gardel Martinez Hortua** Oficial de Comunicaciones del CAIMI **CT. Yudy Lorena Munoz Parra** Oficial Jurídica Militar CAIMI	**TC. Willman Javier Duran Fernandez** Jefe de Estado Mayor CAIMI

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

1. OBJETO

El presente anexo técnico tiene por objeto establecer los requisitos técnicos necesarios que permitan la realización del soporte a plataforma seguridad informática Subsistema de Inteligencia y Contrainteligencia del Ejército Nacional (SICIE).

2. DEFINICIONES Y APLICACIÓN

2.1 DEFINICIONES

NGFW: Next Generation Firewall

NGSG: Next Generation Security Gateway

HDD: Disco de dinámico.

SSD: disco de estado solido

AC: corriente alterna

DC: corriente directa

2.2 APLICACIÓN

Mantenimiento y soporte técnico de la plataforma de seguridad informática del SICIE es de suma importancia para la protección de amenazas cibernéticas internas o externas que podrían afectar la confidencialidad, integridad y disponibilidad de la información de inteligencia.

3. REQUISITOS

3.1 REQUISITOS GENERALES

Brindar soporte y actualizaciones, Upgrade, Update o parches (Software) y servicio de mantenimiento correctivo directamente con el fabricante o casa matriz, así como el soporte técnico, mantenimiento correctivo – preventivo en sitio para todos los productos y/o herramientas que hacen parte de la plataforma de seguridad informática del SICIE.

3.2 REQUISITOS ESPECÍFICOS

ÍTEM	DESCRIPCIÓN
3.2.1	SOPORTE TECNICO DEL FABRICANTE
3.2.1.1	Se deberá garantizar el servicio de soporte técnico y mantenimiento correctivo directamente con el fabricante que se tiene en la actualidad instalada y puesta en funcionamiento en el SICIE para todos los productos y/o herramientas que forman parte de la plataforma de seguridad informática, así:

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

	A) Se realizará el servicio de soporte técnico y mantenimiento correctivo para los productos y/o herramientas que forman parte de la plataforma de seguridad informática. Donde deberá cubrir los siguientes productos y herramientas: · collaborative enterprise support – standard · cpces-co-standard-add · collaborative enterprise support - standard add-on for products B) Se deberá realizar el soporte técnico para el producto Next Generation Firewall (NGFW) en relación con las características de los equipos que se encuentren en los siguientes Account ID UserCenter: 8303174, 8321551, 8007210. El soporte deberá ser proporcionado directamente ante el fabricante CHECKPOINT (checkpoint.com) y deberá cubrir todas las incidencias, mantenimiento y actualizaciones necesarias en los productos asociados a estos Account ID. Esto incluye, pero no se limita a, la resolución de fallas de software y hardware, optimización de políticas de seguridad, y gestión de licencias. C) Se deberá realizar el mantenimiento correctivo de las appliance virtuales para la gestión de seguridad de próxima generación (Next Generation Security Management) y el servicio SmartEvent en un servidor dedicado. Este servicio deberá cubrir la implementación para un total de 10 gateways bajo una licencia perpetua. El mantenimiento incluirá la resolución de problemas de rendimiento, disponibilidad y funcionalidad de estos componentes críticos de la plataforma. NOTA: Todas las actividades mencionadas en este ítem deberán de estar completamente operativas y funcionales hasta el 30 de noviembre de 2027, garantizando el cumplimiento de los estándares acordados en cuanto a seguridad y rendimiento. Se deberá presentar un plan de trabajo detallado al supervisor del contrato que incluya los hitos de implementación, mantenimiento y las métricas de rendimiento esperadas.
3.2.2	**SERVICIO DE MANTENIMIENTO PREVENTIVO**
3.2.2.1	Se deberá efectuar mantenimiento preventivo a las plataformas o equipos que forman parte de la plataforma de seguridad informática del SICIE, contemplando este mantenimiento para todos los productos y/o herramientas que están implementadas. Este servicio deberá ser proporcionado hasta el 30 de noviembre de 2027, según el cronograma acordado con el supervisor de contrato y el suboficial de seguridad informática. El servicio de soporte técnico podrá prestarse remotamente a través de herramientas web online corporativas del contratista o de manera presencial para las unidades ubicadas en la ciudad de Bogotá. Estos mantenimientos deberán incluir, como mínimo, las siguientes actividades: Actualizaciones (upgrade, update, criticas de seguridad) Revisión y solución proactiva de errores. Realización y programación de copias de seguridad. Monitoreo y Análisis de Registros Optimización de Recursos del Sistema (espacio de disco, utilización de cpu – ram, entre otros). Desinstalación Segura de Componentes Inoperativos. Hardening y Reforzamiento de la Seguridad. Gestión de vulnerabilidades Pruebas Funcionales Post-Mantenimiento Todas y cada una de las actividades de mantenimiento preventivo realizadas, incluyendo actualizaciones, revisiones, soluciones de errores, copias de seguridad, análisis de logs, optimización de recursos, desinstalaciones, procedimientos de hardening y gestión de vulnerabilidades, deben ser registradas de manera sistemática.

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

	NOTA: El mantenimiento preventivo a las plataformas o equipos que forman parte de la plataforma de seguridad informática del SICIE, así como todos los productos y/o herramientas que la integran, deberán de estar completamente operativas y funcionales hasta el 30 de noviembre de 2027, garantizando el cumplimiento de los estándares acordados en cuanto a seguridad y rendimiento. El contratista deberá presentar un plan de ventanas de mantenimiento que minimice el impacto en las operaciones del SICIE y un procedimiento de *rollback* en caso de fallas durante las actualizaciones.
3.2.3	**SERVICIO DE MANTENIMIENTO CORRECTIVO**
3.2.3.1	Se deberá realizar el mantenimiento correctivo a las plataformas o equipos que forman parte de la plataforma de seguridad informática del SICIE, cubriendo todos los productos y herramientas que forman parte de dicha plataforma. El objetivo principal de este servicio es restablecer la operación normal de los componentes afectados en el menor tiempo posible, minimizando el impacto en la confidencialidad, integridad y disponibilidad de la información de inteligencia. El mantenimiento correctivo deberá incluir, como mínimo, las siguientes actividades, así: Diagnóstico y Resolución de Fallas Instalación y/o Reparación de Software Configuración de Dispositivos y Políticas de Seguridad Sustitución de componentes de hardware por fallas técnicas o funcionales que comprometan la operatividad de los equipos Revisión Forense y Análisis de Logs y Fallos Restauración de Configuraciones Optimización de Rendimiento Post-Falla Actualización y Ajuste de Reglas de Seguridad NOTA: El mantenimiento correctivo a las plataformas o equipos que forman parte de la plataforma de seguridad informática del SICIE para todos los productos y/o herramientas que forman parte de la plataforma de seguridad informática, deberán de estar completamente operativas y funcionales hasta el 30 de noviembre de 2027, garantizando el cumplimiento de los estándares acordados en cuanto a seguridad y rendimiento. El contratista deberá adherirse estrictamente a los Tiempos de Atención y Tiempos Máximos de Restablecimiento del Servicio definidos en el ítem de Garantía
3.2.4	**OTROS REQUERIMIENTOS TECNICOS**
3.2.4.1	El contratista deberá garantizar el perfecto funcionamiento y la continuidad ininterrumpida de los procesos y servicios prestados para todos los equipos, productos y/o herramientas que forman parte de la plataforma de seguridad informática del SICIE, por el lapso total de la vigencia del contrato, desde el 01 de diciembre del 2026 al 30 de noviembre del 2027. Este compromiso implica la proactividad en la gestión de la plataforma para prevenir interrupciones y la capacidad de respuesta inmediata ante cualquier anomalía que pueda afectar la operatividad. Cuando se realice cualquier tipo de mantenimiento o soporte técnico (preventivo o correctivo), el contratista deberá ofrecer y ejecutar una transferencia tecnológica efectiva y continua sobre las plataformas o herramientas instaladas. Esta transferencia tiene como objetivo que el administrador del sistema del CAIMI, y el personal designado del SICIE, asimile las fallas presentadas, comprenda las configuraciones implementadas y adquiera el conocimiento básico necesario para solucionar problemas de primer nivel, reduciendo la dependencia externa para operaciones rutinarias y fallas menores. Se deberá proporcionar la documentación técnica pertinente como parte de esta transferencia. Una vez al mes, el contratista deberá entregar un reporte técnico integral al supervisor del contrato y al suboficial de seguridad informática del SICIE. Este reporte deberá consolidar la información de todas las actividades realizadas durante el periodo, incluyendo, como mínimo:

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

	Actividades Realizadas Recomendaciones Análisis de Tendencias Nivel de Servicio Uso de Recursos Fundamentación
3.2.4.2	El Oferente debe anexar a la propuesta, como parte integral de los requisitos de idoneidad, los siguientes documentos vigentes a la fecha de presentación de la oferta: Certificaciones oficiales emitidas directamente por el fabricante Check Point Software Technologies Ltda. donde se demuestre, de manera inequívoca, que el oferente es, como mínimo, un distribuidor autorizado o socio de negocios (partner) de Check Point. Esta certificación debe evidenciar explícitamente la especialización en soporte (CCSP - Check Point Certified Security Professional) y una categorización por parte de Check Point de, como mínimo, dos estrellas. Una carta de respaldo formal del fabricante Check Point, dirigida al Ejército Nacional de Colombia, en la que se confirme el apoyo técnico al oferente para la prestación de los servicios objeto de este contrato y se garantice el acceso a las actualizaciones, parches y soporte de segundo y tercer nivel del fabricante para los Account IDs mencionados (8303174, 8321551, 8007210). Mínimo una (01) hoja de vida de un profesional en Ingeniería de Sistemas o afines, de acuerdo al Sistema Nacional de Información de la Educación Superior (SNIES), quien deberá estar certificado como CCSE R82 (Check Point Certified Security Expert R82) o una versión superior y vigente a la fecha de presentación de la oferta.
3.2.5	**ACUERDOS DE CONFIDENCIALIDAD**
3.2.5.1	El contratista y todo el personal vinculado directa o indirectamente a la ejecución del proyecto deberán suscribir, de manera previa e indispensable al inicio de las actividades, el Acuerdo de Confidencialidad y Protección de Información Clasificada (Código: FO-JEMPP-CEDE6-1736). Mediante dicho instrumento se obligan formal y expresamente a preservar bajo estricta reserva legal, integridad, custodia y confidencialidad toda la información institucional, técnica, operativa, estratégica, de infraestructura tecnológica o de inteligencia a la que tengan acceso o generen en desarrollo del objeto contractual, incluyendo aquella clasificada conforme a los niveles y reservas previstos en la Ley Estatutaria 1621 de 2013 y sus normas reglamentarias. En virtud de lo anterior, queda terminantemente prohibida la divulgación, reproducción, almacenamiento, extracción, transmisión, procesamiento, análisis, comercialización o uso para fines distintos al estricto cumplimiento contractual de cualquier información clasificada, estratégica o de inteligencia y contrainteligencia, a través de cualquier medio físico, óptico, digital, electrónico u oral, sin la autorización previa, formal y expresa del Comando de Apoyo de Inteligencia Militar – CAIMI. Lo anterior, en observancia y cumplimiento de lo establecido en los artículos 1, 2, 4, 5, 6, 7 y 13 de la Ley 1621 de 2013, que determinan los fines, principios, límites, tratamiento, clasificación de reserva legal y protocolos de protección de la información de seguridad y defensa del Estado. Como condiciones indispensables y obligaciones especiales, el contratista deberá: Pruebas y Estudios de Confiabilidad Obligatorios: Atendiendo a la naturaleza de la entidad contratante y a que las plataformas, equipos y datos objeto de intervención constituyen activos y bienes estratégicos esenciales para la defensa y seguridad nacional, el contratista deberá permitir, coordinar y garantizar que el personal asignado al proyecto se someta y apruebe las

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

	pruebas de confiabilidad técnica, verificación de antecedentes y estudios integrales de seguridad que la entidad estime convenientes e instruya a través de la IMI-CAIMI. La presentación de estas pruebas es de estricto y obligatorio cumplimiento para autorizar el ingreso, permanencia y asignación de credenciales a las plataformas; su aplicación se ceñirá a los estándares institucionales de seguridad militar, guardando absoluta proporcionalidad y garantizando el respeto integral a los derechos fundamentales, la dignidad humana y el núcleo esencial de la intimidad personal de los colaboradores. Acreditación de Idoneidad: Facilitar oportunamente la documentación, consientes y autorizaciones exigidas por la IMI-CAIMI para certificar la idoneidad moral, disciplinaria y técnica del personal, así como para validar los niveles de acceso y acreditación a áreas o consolas de administración restringidas. En caso de que un funcionario no supere las valoraciones de confiabilidad, el contratista estará obligado a sustituirlo de forma inmediata por un perfil de iguales o superiores calidades que cumpla con los filtros de seguridad institucionales. Conocimiento y Cumplimiento Normativo: Comprometerse formalmente a conocer, acatar y cumplir en su totalidad la Ley 1621 de 2013, su reglamentación y las directivas de seguridad de la información del Ministerio de Defensa Nacional, el Comando General de las Fuerzas Militares, el Ejército Nacional y el CAIMI, en especial lo ateniente a manejo, custodia, almacenamiento y destrucción segura de datos. Medidas Preventivas de Seguridad: Adoptar e implementar todas las medidas técnicas, operacionales, físicas, de cifrado y ciberseguridad que impidan la fuga, interceptación, alteración o compromiso no autorizado de los activos de información, aplicando de forma rigurosa los principios rectores de «necesidad de conocer» y «mínimo privilegio». Entornos y Dispositivos Restringidos: Abstenerse de procesar, almacenar o manipular datos institucionales o clasificados en entornos informáticos, servicios cloud personales, medios extraíbles o equipos no homologados y expresamente autorizados por la IMI-CAIMI. Prohibición en Canales No Autorizados: Abstenerse de divulgar, registrar fotográficamente, comentar o compartir aspectos técnicos, arquitecturas de red o material clasificado en redes sociales, foros, aplicaciones de mensajería comercial o cualquier canal externo no corporativo ni institucional. Disposición Final de la Información: Al término de la ejecución del contrato, el contratista deberá entregar a satisfacción y en su totalidad, mediante Acta Formal de Entrega-Recepción, todas las configuraciones, soportes, modelos, copias y documentos técnicos suministrados o elaborados para el CAIMI. El contratista y sus colaboradores certifican que no conservarán en su poder respaldos, copias directas o indirectas ni registros en ningún soporte digital o físico, en acatamiento de las disposiciones legales de reserva. Cualquier inobservancia, vulneración a la reserva legal o negativa a cumplir con los protocolos y pruebas de confiabilidad aquí establecidos configurará incumplimiento grave del contrato, facultando a la entidad para la imposición de multas, declaratoria de caducidad o terminación unilateral, sin perjuicio de las acciones penales que correspondan bajo el Código Penal Colombiano (delitos contra la seguridad de la información, espionaje o violación de reserva legal) y las responsabilidades disciplinarias y administrativas pertinentes.
3.2.6	**GARANTÍA**
3.2.6.1	El Contratista debe garantizar el perfecto funcionamiento y la continuidad operativa de cada uno de los elementos de software y de los appliance del SISTEMA DE SEGURIDAD, incluyendo todos los equipos, productos y/o herramientas que forman parte de la plataforma de seguridad informática del SICIE, como mínimo, durante todo el tiempo de ejecución del contrato. Durante este período, el contratista se obliga a reemplazar cualquier elemento de

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

	software o appliance que presente falla o mal funcionamiento, sin costo adicional para la entidad. Al finalizar la vigencia del contrato, el contratista se obliga a que no quedará ningún servicio sin atender. Esto asegura una transición limpia y que la plataforma quede en un estado operativo óptimo para la siguiente fase o gestión interna. Todos los appliance deben tener una garantía que cubra, como mínimo, el tiempo restante de la ejecución del contrato. El contratista deberá suministrar asistencia inmediata a través de un Centro de Atención de Llamadas (CAL) o Service Desk, disponible las veinticuatro (24) horas del día, los siete (7) días a la semana, todo el año (24x7x365). Este servicio debe incluir soporte local y ofrecer un Acuerdo de Nivel de Servicio (SLA) 7x24x365. La prestación del servicio de atención a casos reportados tendrá un horario base de 5x8 (cinco días a la semana, ocho horas al día), adicionando un mínimo de dieciséis (16) horas mensuales de atención que podrán ser utilizadas para casos reportados fuera de este horario base. Estas horas adicionales deberán ser gestionadas de común acuerdo con el supervisor del contrato. Los soportes técnicos deben ser atendidos por medio telefónico o remoto de forma inmediata. Si en el lapso de dos (02) horas después de haber reportado un incidente (independientemente de su categorización inicial) no se ha dado una solución definitiva o una mitigación temporal efectiva al mismo, se deberá enviar personal técnico especializado a sitio en un tiempo máximo de dos (02) horas. Los anteriores tiempos de respuesta también aplican para las unidades ubicadas fuera de la ciudad de Bogotá y podrá ser prestado remotamente desde el CAIMI, siempre y cuando las condiciones técnicas lo permitan. El tiempo máximo permitido para restablecer el servicio luego de realizada la llamada solicitando el soporte técnico es de veinticuatro (24) horas. En caso de que sea necesario el reemplazo de un equipo appliance, el contratista deberá incluir la reposición de cualquiera de sus partes por un modelo igual o de características superiores, cuando así se requiera. El plazo máximo para dicho reemplazo es de cuatro (04) días, ya sea por daño de hardware o software. Esto también aplica si alguna parte no es compatible con la última versión liberada y estable del sistema operativo o firmware lanzado por el fabricante para sus dispositivos, sin que esto genere costos adicionales para la entidad. El contratista debe coordinar con el supervisor del contrato la salida del equipo defectuoso y, a su vez, suministrará el reemplazo de la parte o elemento necesario para garantizar el normal funcionamiento del sistema VICIOS OCULTOS: Cuando el bien reemplazado presente problemas no detectados por el supervisor o el comité técnico evaluador al momento del recibo de los mismos, por defectos de fabricación, ensamble o calidad de sus componentes, que afecten la funcionabilidad del bien, el contratista cambiará la parte y/o solucionará el reporte técnico objeto de la reclamación. Esto durante el término de la presente garantía técnica El contratista debe garantizar la calidad de todos los servicios de soporte y mantenimiento prestados.

3.3 REQUISITOS DE EMPAQUE Y ROTULADO

3.3.1 Empaque.

Omitido

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

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

Omitido.

6. APÉNDICE

6.1 NORMAS QUE DEBEN CONSULTARSE

- Constitución Política de Colombia
- Código Civil
- Código General del Proceso
- Código de Comercio
- Código de Procedimiento Administrativo y de lo Contencioso Administrativo
- Ley 80 de 1993 (Estatuto General de Contratación de la Administración Pública)
- Ley 1150 de 2007 (Modifica la Ley 80 de 1993 sobre contratación pública)
- Ley 816 de 2003 (En el caso de no limitarse a MIPYMES nacionales)
- Ley 1952 de 2019 (Estatuto Anticorrupción)

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

- Ley 1978 de 2019 (Norma que reglamenta las Tecnologías de la Información y las Comunicaciones – TIC)
- Decreto-Ley 019 de 2012 (Medidas para la simplificación de trámites)
- Decreto 1082 de 2015 (Por el cual se expide el Decreto Único Reglamentario del Sector Administrativo de la Función Pública)
- Decreto 1263 de 2022 (Lineamientos para la transformación digital de la Administración Pública)
- Resolución de Delegación 1549 del 6 de marzo de 2015
- Directiva Permanente 09 de 2014 emitida por el Ministerio de Defensa Nacional
- Resolución No. 6302 del 31 de julio de 2014 (Manual de Contratación del Ministerio de Defensa Nacional)
- Cartilla de Formatos de Contratación, Tomo I (Jefatura de Logística – Dirección de Contratación, en lo que aplique)
- Manuales y Circulares de Colombia Compra Eficiente y sus respectivas actualizaciones
- Ley Estatutaria 1621 de 2013 (Ley de Inteligencia y Contrainteligencia)
- Manuales y circulares de Colombia Compra Eficiente y sus respectivas actualizaciones Y demás normas concordantes y pertinentes.

6.2 ANTECEDENTES

Omitido.

7. ANEXOS

Omitido.

8. CONTROL DE REVISIONES

Revisión y/o Actualización	Modificaciones	Fecha
00	Creación del Anexo Técnico MANTENIMIENTO Y SOPORTEPLATAFORMA SEGURIDAD INFORMATICA	26/02/2025
01	Cambio de nombre a Creación del Anexo Técnico PLATAFORMA SEGURIDAD INFORMATICA	09/09/2026

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