ESPECIFICACIONES TÉCNICAS

ADQUISICIÓN, INSTALACIÓN Y CONFIGURACIÓN DE UNA HERRAMIENTA DE SEGURIDAD PARA LA PROTECCIÓN Y BALANCEO A LAS APLICACIONES WEB (WAF) DEL ÉJERCITO NACIONAL PARA EL FORTALECIMIENTO DE LOS MEDIOS CIBERNETICOS DEL EJÉRCITO NACIONAL.	
1	**NUMERAL 1: GENERALIDADES**
1.1	El contratista se debe comprometer a no divulgar y reproducir el software y la documentación que actualmente tiene el Ministerio de Defensa Nacional – Ejército Nacional – Batallón de Ciberdefensa que se vea obligado a conocer como producto de la ejecución del contrato. Por tanto, el contratista debe estar dispuesto a firmar los acuerdos de confidencialidad de la información suministrada en aspectos técnicos y relacionados, con la información que se maneje en el contrato, estos acuerdos deben realizarse con el acta de inicio del contrato. Así mismo, debe aceptar y permitir que Ministerio de Defensa Nacional – Ejército Nacional, efectúe un Estudio de Seguridad Personal (ESP), a los funcionarios del contratista designados para el desarrollo del contrato, a fin de comprobar datos y establecer antecedentes disciplinarios y demás que garanticen la seguridad de la infraestructura tecnológica militar e información del Ministerio de Defensa Nacional – Ejército Nacional – Batallón de Ciberdefensa.
1.2	La totalidad de la documentación y configuraciones de software, hardware y consultoría resultantes del contrato, serán de propiedad intelectual del Ministerio de Defensa Nacional – Ejército Nacional – Batallón de Ciberdefensa la cual deberá ser entregada al supervisor del contrato.
1.3	Antes de realizar una implementación el contratista debe garantizar compatibilidad con la infraestructura y arquitectura tecnológica actual del Ejército Nacional. 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.
1.4	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; Una vez finalizado el contrato, a estos elementos se les debe realizar un procedimiento de borrado seguro por parte de la Batallón de Ciberdefensa del Ejército Nacional para posteriormente ser retirados de las instalaciones del Ministerio de Defensa Nacional – Ejército Nacional – Batallón de Ciberdefensa.

<table>
<tr><td>1.5</td><td><u>El contrato debe ser tratado como un proyecto llave en mano</u>.

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 de Defensa Nacional – Ejército Nacional – Batallón de Ciberdefensa el correcto funcionamiento de acuerdo a las especificaciones técnicas requeridas.

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 Ejercito Nacional.”</td></tr>
<tr><td>1.6</td><td>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.

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.

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.

<table>
<tr><td>Cantidad</td><td>Elemento</td><td>Marca</td><td>Referencia</td><td>Detalle técnico</td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>1.7</td><td>El Contratista deberá incluir para la ejecución del contrato los patch cord OM3 multimodo o ETHERNET UTP y los módulos a 10G o Módulos RJ .5 (point five) que se requieran según la topología propuesta para la solución.

• El contratista deberá realizar las conexiones que se requieran entre racks, con tendido en fibra óptica multimodo OM3 o superior, aplicando la tecnología de cassettes MTP MPO FHD, de acuerdo a lo anterior, el contratista deberá suministrar todos los elementos pasivos que se requieran para garantizar el funcionamiento de los equipos</td></tr>
</table>

	adquiridos, conservando las buenas prácticas de instalación en centro de cómputo del Ejército Nacional (Las instalaciones de la fibra óptica deben quedar funcionales en su comunicación entre racks o dispositivos que lo requieran) • El contratista deberá realizar las conexiones que se requieran entre racks, de cableado estructurado del centro de cómputo del Ejército Nacional garantizando la correcta operatividad del sistema; Lo anterior deberá quedar claramente rotulado, organizado, certificado y documentado, conservando las buenas prácticas de instalación en el centro de cómputo del Ejército Nacional avalado por el supervisor del contrato. • Adecuación de las conexiones eléctricas (AC) si fuese necesario para la instalación y correcto funcionamiento en el centro de cómputo del Ejercito Nacional. • El contratista verificará el óptimo funcionamiento de las instalaciones eléctricas, de ser necesario se realizará la instalación, renovación o cambio de circuitos o tomas en el centro de cómputo del Ejercito Nacional. • Los equipos activos a implementar en la solución cuentan con doble fuentes de poder, teniendo en cuenta lo anterior se requiere que cada fuente se alimente de circuitos independientes, tomados desde la UPS del centro de cómputo, lo cual garantizara un respaldo eléctrico a los equipos. No se aceptan equipos con sus dos fuentes de poder conectados al mismo circuito. • El contratista debe suministrar la cantidad de puertos Ethernet y Fiber Channel LAN/SAN, gigabits, fibra óptica y demás elementos necesarios para la puesta en funcionamiento de las soluciones. • El contratista debe contemplar todos los elementos necesarios para mencionada adecuación sin que genere costos adicionales para el Ejército Nacional. • El Rackeo de las maquinas debe incluir o Instalación física en el centro de cómputo principal. o Adecuación de las conexiones eléctricas si fuese necesario. o Configuración software y demás herramientas necesarias para su correcto funcionamiento. o Configuración de red: conectividad IP. o Movimiento de los equipos que sea necesario reacomodar. o Cableado estructurado.
1.8	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.
1.9	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. 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 la que cuenta el Ejercito Nacional.
1.10	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.
1.11	Las soluciones a implementar deben ser compatibles con las plataformas actuales del Ejército Nacional y cumplir con el protocolo IPv4 e IPV6.
1.12	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.
1.13	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.
1.14	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.
	PRUEBAS DEL SISTEMA Y PUESTA EN MARCHA
1.15	Una vez realizadas las pruebas en cada una de las soluciones y si se presenta mal funcionamiento o no cumple con las especificaciones técnicas, se deberá realizar corrección y ajustes hasta asegurar su correcto funcionamiento, sin que esto genere costo adicional para el Ministerio de Defensa Nacional – Ejército Nacional – Batallón de Ciberdefensa
1.16	Se requiere realizar pruebas de funcionalidad, con el fin de garantizar que la configuración, integración e instalación sea la apropiada, en caso de alguna falla técnica en alguno de sus componentes, el contratista debe solucionar sin que esto genere costo alguno al Ministerio de Defensa Nacional – Ejército Nacional – Batallón de Ciberdefensa.
	CANAL DE COMUNICACIÓN

1.17	El canal de comunicación será con el supervisor del contrato designado por Ministerio de Defensa Nacional – Ejército Nacional.
	CUMPLIMIENTO NORMAS TÉCNICAS
1.18	El Contratista debe cumplir o exceder en las siguientes especificaciones de instalación, documentación, componentes y sistemas de la industria según sea el caso: • 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. • 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. • 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. • 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. • Telecomunicaciones/Infraestructuras Comerciales). • 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). • ANSI/TIA/EIA-526-7 “Measurement of Optical Power Loss of Installed Single-ModeFiber Cable Plant” (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 al alcance del RETIE, para los siguientes elementos: - Tomacorrientes - Cable Eléctrico - Tableros - Tubería • Protecciones (breakers y tomas con supresor de transientes).
1.19	Para la instalación y puesta en funcionamiento de la solución, el oferente debe aportar la siguiente documentación del personal encargado de estas actividades. • 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. • Copia legible de la tarjeta profesional • Copia de cédula de ciudadanía que verifique la nacionalidad colombiana. • Certificación de fabricante de la herramienta a implementar. • Certificado de experiencia en instalación de la solución a implementar. El Contratista, durante la ejecución del contrato, acepta que el Ejército Nacional evalúe el desempeño profesional de la(s) persona(s) asignadas para el proyecto y estará(n) en facultad de solicitar su reemplazo, si esta(s) no cumple(n) con las expectativas del supervisor del contrato. Durante la ejecución del contrato, si se requiere reemplazar un funcionario por otro, éste deberá tener un perfil profesional igual o superior al que va a ser reemplazado, y cumplir con los requerimientos estipulados en esta especificación técnica. En caso de que el contratista requiera realizar un cambio de personal, este deberá informar al supervisor del contrato de tal situación con mínimo 10 días de antelación, anexando la hoja de vida del nuevo funcionario que debe cumplir con las especiaciones requeridas. 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 del contrato.
	GARANTÍA
1.20	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. El término de la garantía técnica por parte fabricante será de mínimo tres (03) años para cada elemento desde la firma del acta de recibo a satisfacción.

	El término de la garantía técnica por parte del contratista será de mínimo tres (03) años para cada elemento desde la firma del acta de recibo a satisfacción.
1.21	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: •Cambio de equipos en caso de fallas •Remplazo de equipos por otros de iguales o superiores características. •Instalación de software •Configuraciones, puesta en producción y funcionamiento
1.22	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.
SOPORTE FABRICANTE	
1.23	El horario de cobertura de soporte por parte del fabricante debe ser 24x7x365 desde la firma del contrato. El contratista deberá entregar un servicio de soporte de todos los productos a ofertar durante el periodo de la garantía de la solución de acuerdo al tem No 1.20 El fabricante deberá brindar las actualizaciones de software sin costo adicional durante el periodo de vigencia de la garantía técnica.
SOPORTE CONTRATISTA	
1.24	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 3 años que es el término de la garantía. TIPO DE ATENCIÓN: El servicio será prestado de dos formas así: • Soporte Nivel 1: De manera presencial un día a la semana con duración de 8 horas laborales (1x8) 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 • 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 1.24 . Para este soporte el contratista deberá suministrar un servicio de asistencia técnica con personal certificado para atender necesidades específicas de la plataforma.

	El horario de soporte por parte del contratista y fabricante debe ser 24x7x durante la ejecución del contrato y el periodo de la garantía de la solución, 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. **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. Tiempo máximo de respuesta dos (02) horas después de haber reportado el incidente. De ser necesario el contratista deberá enviar personal técnico especializado a sitio en un tiempo máximo de cuatro (04) horas. El tiempo máximo permitido para restablecer el servicio es de 4 horas.
1.25	Todos los equipos deberán estar embalados en las cajas de 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. De igual modo los equipos deben ser nuevos y no remanufacturados. 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.
1.26	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.
1.27	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.
1.28	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.
1.29	El contratista deberá entregar al Ejército Nacional la documentación necesaria para la Instalación, configuración, implementación y parametrización. 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: - 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. - Informe de cada visita, documentado los procedimientos realizados.
CERTIFICACION DE FABRICANTE	
1.30	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.
TRANSFERENCIA DE CONOCIMIENTO	
1.31	El Contratista debe realizar transferencia de conocimiento al personal del Batallón de Ciberdefensa del Ejercito Nacional con relación a la herramienta CLOUD WAF adquirida, administración, instalación, configuración y análisis, dictada directamente por el fabricante y /o distribuidor autorizado en la ciudad de Bogotá, en idioma español, en las

<table>
<tr><td></td><td>instalaciones adecuadas, con una duración de mínima de 40 horas, para cinco (05) funcionarios del Ejército Nacional.

Se debe expedir certificado por parte de fábrica y/o contratista.</td></tr>
<tr><td>1.32</td><td>El contratista debe realizar transferencia de conocimiento para veinte y cinco (25) funcionarios del Ejército Nacional, así mismo, debe incluir material técnico, para 25 funcionarios, con una duración mínima de 30 días hábiles en horario de 5X4 en la ciudad de Bogotá en Idioma español; se debe ofrecer una metodología teórica y práctica con laboratorios de cómputo debidamente configurados, en instalaciones dispuestas por el contratista que incluya equipos de cómputo, material impreso, digital, de software y hardware.

• El contratista debe disponer de aulas completamente dotadas que cubran todos los aspectos logísticos para la ejecución de los entrenamientos requeridos, igualmente proveer instructores idóneos, calificados y certificados, con experiencia en la ejecución de capacitación, además de un refrigerio y estación de café para cada asistente al curso.
• El Contratista debe garantizar que el entrenamiento requerido se dictará en modalidad presencial. (No se admitirá E-learning, Virtual, Sesiones pregrabadas, ni en formato video) a fin de garantizar una mejor experiencia de aprendizaje.
• El Contratista deberá entregar el material de clases necesario para desarrollar el entrenamiento de acuerdo a cada uno de los módulos. Así mismo, se deberán entregar las presentaciones utilizadas por los instructores.
• El Contratista deberá emitir un certificado a cada uno de los estudiantes que aprueben la transferencia tecnológica.
Antes del inicio de la transferencia tecnológica el contratista debe realizar una evaluación de conocimientos del personal seleccionado con el fin de articular el nivel de los temas a tratar.

<u>SE DEBEN DICTAR TEMAS:</u>

➢ Fundamentos de Infraestructura
➢ Networking
➢ Ethical Hacking
➢ computación forense
➢ sistemas operativos
➢ respuesta a incidentes
➢ análisis de malware dinámico y estático
➢ Pentesting</td></tr>
<tr><td colspan="2">LICENCIAMIENTO</td></tr>
<tr><td>1.33</td><td>La solución debe tener el modelo de licenciamiento a perpetuidad y renovación anual de la misma. El licenciamiento debe ser entregado al Ejército Nacional por un periodo de 3 AÑOS contados a partir del acta de recibo a satisfacción.

El contratista entregará al supervisor del contrato en documento independiente emitido por parte del fabricante de la solución certificado que indique el periodo de licenciamiento de la solución.

<table>
<tr><td>Cantidad</td><td>Descripción</td><td>Detalle de la descripción</td><td></td></tr>
</table>
</td></tr>
</table>

	1	Alteon D-5208S 6G - Upgrade to 12G - Software Option	License upgrade per unit - For Alteon D-5208S (Deliver, Perform, Secure and HPP) from 6 Gbps to 12 Gbps
	1	Alteon D-5208S 12G - Upgrade to 26G - Software Option	License upgrade per unit - For Alteon D-5208S (Deliver, Perform, Secure and HPP) from 12 Gbps to 26 Gbps
	1	Cloud WAF Enterprise - 50 Mbps - 1 Application - Managed Service - Monthly Fee	Cloud WAF Enterprise service for 1 Application. Up to 50 Mbps of actual HTTP/S traffic. Web application attack mitigation covering OWASP Top-10, protecting against Common Web attacks, Data and Access Centric attacks, and Zero Day attacks. Negative and Positive security models, Behavioral Network and Application Layer DDoS Protection with network challenge-response. Includes DDoS protection up to 1 Gbps of attack traffic for all Radware POPs. Managed service includes: 24x7 support (portal/email/phone), 30 minute response SLA via phone, onboarding assistance, asset health monitoring, proactive automatic security anomaly alerts, on-demand policy tuning and application security insights.
	1	Cloud WAF Enterprise - 10 Mbps Traffic Add-On - Monthly Fee	10 Mbps traffic add-on subscription license for Cloud WAF Enterprise service.
	1	Cloud WAF Enterprise 40 Applications Add-On - Monthly Fee	Add-on subscription license for protecting additional 40 applications.

Nota: En caso de realizarse modificaciones o adiciones al contrato, el licenciamiento empezará a contar desde el acta de recibo a satisfacción final.

CUMPLIMIENTO DE NORMATIVIDAD GUBERNAMENTAL EN MATERIA DE TICS	
1.34	Todas las soluciones deben ser compatibles con los protocoles IPV4 e IPV6

	CUMPLIMIENTO DE NORMATIVIDAD GUBERNAMENTAL EN MATERIA DE TICS 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."
ESPECIFIACIONES TECNICAS	
2.1	**REQUERIMIENTOS GENERALES DE LA HERRAMIENTA**
2.1.1	El contratista deberá proveer, instalar, configurar y poner en funcionamiento, la solución para la protección y balanceo a las aplicaciones WEB, del Ejército Nacional, garantizando la protección de los datos y la continuidad de los diferentes servicios informáticos y en general toda la infraestructura de red del Ejército Nacional. El contratista debe entregar: • La solución debe incluir 1 balanceador de carga Radware Alteon D-5208S Secure - 26G para ser implementado junto con la solución actual para armar un esquema de HA (High Availability). La entidad cuenta en la actualidad con dispositivo Radware Alteon 5208 - 6G. • La solución de Application Delivery Controller deberá estar ubicada en el cuadrante Leaders en los últimos dos informes "Gartner Magic Quadrant for Application Delivery Controllers" • Se debe garantizar incluir el licenciamiento y hardware necesario para el equipo Radware Alteon D-Line 5208 - Upgrade to 5208S (SSL Hardware Accelerators) - con el que actualmente cuenta la entidad y que ambos puedan cumplir con los requerimientos de capacidad listados a continuación: • Cada equipo de la solución debe soportar como mínimo un Throughput en L4 de 26 Gbps. • Cada equipo debe soportar como mínimo 630.000 conexiones por segundo en capa 4. • Cada equipo debe soportar como mínimo 50 Millones de conexiones concurrentes en capa 4. • Capa equipo debe soportar como mínimo 850.000 Millones de request por segundo en capa 7. • Cada equipo debe incluir las siguientes interfaces para los servicios balanceados: -2 puertos 10Gbps fibra multimodo con sus respectivos tranceivers • Cada equipo debe tener la siguiente capacidad de crecimiento en interfaces para uso futuro (no es necesario incluir los tranceivers): - 8 puertos 1GE cobre - 2 puertos 10GE fibra con múdulos SFP+ • La solución debe contar como mínimo con el siguiente desempeño de SSL: - RSA CPS (llaves de 2K): 20.500 - ECC CPS (P256): 12.000 - SSL Bulk Throughput(Gbps): 10 Gbps • La solución debe soportar FIPS 140-2 Level 3, a través del uso de un HSM integrado • La solución debe soportar HSM de red y ser compatible con SafeNet Luna Network HSM 7 de Gemalto/Thales

	• Cada equipo debe incluir al menos dos puertos de administración dedicados e independientes a las interfaces de balanceo. • Cada equipo debe incluir fuente de poder redundantes AC hot swappable • Cada equipo debe incluir un disco duro SSD de 500 GB de capacidad. • La solución debe incluir un REST API donde se provea acceso completo a la funcionalidad el equipo, incluyendo crear, leer, actualizar o borrar información. • Dejar implementado y en funcionamiento el sistema ofertado en las instalaciones del centro de Datos y Comunicaciones Provisional del Comando del Ejército ubicado en Bogotá - Carrera 54 N 26 25 CAN o donde se encuentre en el momento. • Configurar las políticas requeridas por el Ejército Nacional. • Aplicar las mejores prácticas de seguridad y ajustarlas a las políticas de seguridad informática del Ejército Nacional.
2.2	**REQUERIMIENTOS DE SWITCHING Y ROUTING**
2.2.1	La solución debe soportar como mínimo los siguientes protocolos de enrutamiento: - RIPv1 y RIPv2 - BGP - OSPF y OSPFv3
2.3	**ADMINISTRACIÓN LOCAL DE LA PLATAFORMA**
2.3.1	La solución debe permitir crear reglas de acceso a la administración a través de la definición de las IP que podrán acceder y especificando los protocolos de administración.
2.3.2	La solución debe permitir especificar límites de tasa de tráfico sobre el tráfico de administración
2.4.	**ALTA DISPONIBILIDAD**
2.4.1	La solución debe estar configurada en alta disponibilidad y debe soportar Stateful Failover.
2.4.2	La solución debe permitir forzar cambios de role de un balanceador de activo, manejando el tráfico, a modo backup.
2.4.3	La solución debe permitir forzar cambios de role de activo a backup por servicio virtual configurado.
2.4.4	La solución debe permitir sincronizar la configuración entre equipos de forma manual o automática.
2.5	**REQUERIMIENTOS DE BALANCEO LOCAL DE SERVIDORES (SLB)**
2.5.1	La solución debe balancear el tráfico enviado desde los clientes a través de la exposición de un servicio virtual y posterior entrega del tráfico a un grupo de servidores reales a balancear.

2.5.2	La solución debe soportar las siguientes topologías IP - IPv4 pura, con clientes y servidores reales en IPv4. - IPv6 pura, con clientes y servidores reales en IPv6. - Clientes IPv4 y servidores en IPv6 o servidores IPv4 y clientes IPv6
2.5.3	La solución debe soportar balanceo transparente, en donde se realicé inspección del tráfico, clasificación y envío a uno o más grupos de balanceo, sin alterar el paquete original.
2.5.4	La solución debe permitir filtrar el tráfico, permitiendo aceptar o denegar el mismo, utilizando como mínimo los siguientes parámetros: - Dirección MAC. - Dirección IP. - Protocolo. - Banderas TCP. - Tipos de mensaje ICMP. - Puertos capa 4. - String en Capa 7.
2.5.5	La solución debe permitir configurar peso sobre los servidores para trabajar con algoritmos de balanceo basados en el peso otorgado.
2.5.6	La solución debe modificar los pesos asignados de forma dinámica basada en resultados de monitoreo de salud enviados vía SNMP.
2.5.7	La solución debe permitir configurar un servidor real de backup para cada servidor real definido, el cual asumirá la carga en caso de que el servidor real principal falle.
2.5.8	La solución debe soportar al menos los siguientes algoritmos de balanceo: - Hash - Persistent Hash - Tunable Hash - Weighted Hash - Highest Random Weights - Least Connections - Least Connections Per Service - Round-Robin - Response Time - Bandwidth

2.5.9	La solución debe permitir crear nuevos chequeos de salud utilizando scripts.
2.5.10	La solución debe soportar chequeos de salud para validar el estado de los servidores reales objetos de balanceo, soportando al menos los siguientes métodos predefinidos: TCP, half-open TCP, ICMP, HTTP/S, DNS (TCP & UDP based), TFTP, SNMP, FTP, POP3, SMTP, IMAP, NNTP, RADIUS, SSL, LDAP/S, WAP, ARP, DHCP, RTSP, ADFS.
2.5.11	La solución debe soportar protección de las API permitiendo importar el archivo swagger u open API. La solución debe soportar API quota management permitiendo configurar el número de llamados en un periodo de tiempo configurable, por cada método dentro de los endpoints de API definidos y debe realizar seguimiento a cada origen que realiza el llamado. La solución de protección API debe dar visibilidad del catálogo de la API mostrando al menos los endpoints, métodos y parámetros permitidos. La solución de protección API debe realizar Schema Enforcement en XML y JSON validando el método, endpoint, query parameters, header parameters, cookie parameters, path parameters. La solución de protección API debe soportar la configuración de seguridad sobre cada endpoint en modo bloqueo, solo reporte y deshabilitado. La solución de protección API debe soportar ataques embebidos y RFC compliance de HTTP en los llamados API La solución debe soportar descubrimiento de la API a través de machine learning, generando un archivo de OpenAPI que se puede descargar desde el portal del servicio. La solución debe contar con un mecanismo que permita el bloqueo temporal de direcciones IP de origen, basado en el seguimiento de los eventos de seguridad generados sobre las aplicaciones. La solución debe soportar detección y mitigación de ataques del lado del cliente, para proteger contra al menos las siguientes amenazas formjacking, Magecart, supply chain,e-skimming y DOM based XSS
2.5.12	La solución debe permitir configurar chequeos de salud compuestos de chequeos individuales, a través de expresiones lógicas.
2.5.13	La solución debe permitir definir una dirección IP específica (NAT) como el origen de los chequeos de salud.
2.5.14	La solución debe soportar balanceo por contenido HTTP de forma nativa y sin scripting adicional, utilizando al menos los siguientes elementos del protocolo HTTP para la creación de las reglas:

	- URL hostname - URL Path - URL Page name - URL page Type - Cualquier encabezado HTTP - Cookies - Texto específico en el encabezado o en el cuerpo del mensaje. - XML tags
2.5.15	La solución debe permitir controlar los códigos de respuesta HTTP enviados por los servidores reales de forma nativa y sin script adicional.
2.5.16	La solución debe permitir ocultar la información de identidad de los servidores HTTP balanceados, modificando las respuestas enviadas por los servidores reales, de forma nativa y sin script adicional.
2.5.17	La solución debe permitir modificaciones de contenido en las respuestas enviadas por los servidores o en las solicitudes realizadas por los clientes, de forma nativa, sin necesidad de script, en al menos los siguientes elementos HTTP: - HTTP Headers: Podrán ser insertados, reemplazados o removidos. - Cookies - File Type - Status Line - URL -Text
2.5.18	La solución debe soportar persistencia para cualquier protocolo TCP/UDP a través de scripting.
2.6	**REQUERIMIENTOS DE OPTIMIZACIÓN GENERAL**
2.6.1	La solución debe soportar caching conforme al RFC 2616
2.6.2	La solución debe incluir la funcionalidad de compresión HTTP
2.6.3	La solución debe soportar HTTP multiplexing incluso si el servicio virtual se encuentra configurado con SSL offloading, caché y compresión.
2.6.4	La solución debe soportar TCP pooling para mejorar el overhead que impone el establecimiento y terminación de las conexiones TCP con los servidores reales.

2.6.5	La solución debe permitir definir políticas de optimización TCP que se podrán aplicar de forma independiente a la comunicación de cara al cliente y a la comunicación de cara al servidor.
2.6.6	La solución debe soportar HTTP/2 y HTTP/3 Gateway
2.6.7	La solución debe soportar HTTP/2 Full Proxy con cliente y servidor en HTTP/2.
2.6.8	La solución debe soportar SSLv3, TLSv1, TLSv1.2, TLSv1.3
2.6.9	La solución debe soportar SNI para mantener múltiples hosts detrás de una única IP y puerto de manera nativa y sin necesidad de scripting adicional.
2.7	**REQUERIMIENTOS DE OPTIMIZACIÓN DE DESEMPEÑO EN CAPA DE APLICACIÓN WEB**
2.7.1	La optimización de desempeño WEB debe permitir trabajar en un modo aprendizaje, en donde no se apliquen las técnicas configuradas, pero si se pueda probar el sitio a través de una URL específica.
2.7.2	La solución debe soportar optimización específica por tipo de navegador.
2.7.3	La solución debe soportar Predictive Browser Caching permitiendo precargar recursos del sitio web para acelerar la carga del mismo.
2.7.4	La solución debe soportar la consolidación de los siguientes recursos dinámicos: - Consolidación de CSS. - Consolidación de Javascripts - Consolidación de Imágenes.
2.7.5	La solución debe soportar el rendering progresivo de las imágenes, permitiendo comprimir las imágenes, cargarlas en una resolución menor y luego mejorarla una vez la página haya sido cargada.
2.7.6	La solución debe soportar compresión de imagenes usando configuración específica para cada dispositivo: Desktop, Dispositivos Móviles y Tabletas.
2.8	**REQUERIMIENTOS DE BALANCEO GLOBAL**
2.8.1	La solución debe permitir el balanceo de tráfico a través de múltiples sitios físicos.
2.8.2	La solución debe permitir redirección global basada en los siguientes métodos: DNS, HTTP y Proxy (NAT de los clientes) para las aplicaciones que no usen DNS ni sean HTTP.
2.8.3	La solución debe monitorear el estado de los balanceadores en sitios remotos, como mínimo: - Tiempo de respuesta de los servidores - Uso de la CPU

	- Disponibilidad y uso de sesiones
2.8.4	La solución debe soportar como mínimo las siguientes reglas de balanceo global: - Red o redes de origen. - Ubicación geográfica. - Menor número de conexiones. - Roundrobin - Weighted Roundrobin - Menor tiempo de repuesta - Combinación de tiempo de respuesta y menor número de conexiones. - Ancho de banda - Proximidad, midiendo el tiempo de respuesta entre cada datacenter y el cliente - Persistencia - Hash de la IP de origen y el nombre del dominio
2.8.5	La solución debe permitir la configuración de balanceo global, aun estando detrás de un dispositivo que realice un NAT de las direcciones IP públicas como un Firewall y no debe requerir hardware adicional para realizar esto.
2.9	**REQUERIMIENTOS DE BALANCEO DE ENLACES**
2.9.1	La solución debe soportar balanceo de enlaces para tráfico entrante y para tráfico saliente.
2.9.2	El balanceo de enlaces debe contar con al menos las siguientes opciones de despliegue: - Capa 3 o modo ruteo - Capa 2 o modo bridge
2.9.3	La solución debe permitir definir los enlaces a balancear especificando: - Dirección IP del router de upstream. - Chequeo de salud por enlace. - NAT a configurar para el balanceo de salida
2.9.4	El balanceo de enlaces de salida debe permitir clasificar el tráfico con al menos los siguientes parámetros: - Vlan - Dirección IP Origen/destino

	- Puerto Origen/Destino - Protocolo - Contenido a capa 7 - Estático definiendo los grupos por donde se debe enviar el tráfico
2.9.5	La solución debe contar con al menos las siguientes métricas en el balanceo de salida para determinar el mejor enlace: - Least Connections - Round-Robin - Response Time - Bandwidth
2.9.6	La solución debe soportar al menos los siguientes tipos de conversiones de direcciones de red (NAT): - No NAT: que el tráfico se reenvíe de forma transparente - NAT dinámico - NAT estático - NAT de prefijos de IPv6
2.9.7	La solución debe soportar al menos las siguientes métricas para el balanceo de enlaces entrante: - Red o redes de origen. - Ubicación geográfica. - Menor número de conexiones. - Roundrobin - Weighted Roundrobin - Menor tiempo de repuesta - Combinación de tiempo de respuesta y menor número de conexiones. - Ancho de banda - Persistencia - Hash de la IP de origen y el nombre del dominio

2.9.8	La solución debe incluir una métrica por proximidad que correlacione la latencia y el número de saltos hacia un origen determinado, para el balanceo de salida y desde un origen determinado para el balanceo entrante.
3	**REQUERIMIENTOS DE VIRTUALIZACIÓN**
3.1	La solución debe soportar instancias virtuales de balanceo que se ejecuten sobre un hypervisor de balanceo especializado.
3.1.1	La solución debe incluir 5 balanceadores virtuales, con posibilidad de crecimiento hasta 32, sin necesidad de modificar el hardware.
3.1.2	La solución debe permitir asignar recursos físicos independientes, CPU, memoria, sobre cada instancia virtual y los recursos físicos asignados no debe compartirse entre las instancias virtuales de balanceo.
3.1.3	La solución debe permitir que cada balanceador virtual maneje su propia infraestructura de red independiente, tanto en capa 2 como en capa 3, incluyendo protocolos de enrutamiento dinámicos.
3.1.4	La solución soporta múltiples imágenes de software por cada balanceador virtual. Cada balanceador podrá correr una imagen de software distinta.
3.1.5	La solución debe permitir asignar recursos físicos independientes para la funcionalidad de Optimización de desempeño Web.
3.1.6	La solución debe permitir asignar recursos físicos independientes para la funcionalidad de Web Application Firewall, para evitar que el balanceador y el WAF compartan los mismos recursos.
3.2	**REQUERIMIENTOS DE SEGURIDAD**
3.2.1	La solución debe soportar ACL (listas de control de acceso) para controlar el acceso a los dispositivos que conforman la solución y a los servidores balanceados desde la interfaz gráfica.
3.2.2	La solución debe incluir IP reputation, con configuración de acciones, Alertar, Permitir y bloquear, de acuerdo con: - La región (ubicación) - La categoría: Tor Exit Nodes e IP Maliciosas - El nivel de riesgo. -El servicio de cloud WAF debe permitir crear excepciones de IP que se encuentren incluidas dentro del bloqueo por geografía

	El balanceador debe contar con integración nativa con un servicio de administración de bots (Bot Manager) del mismo fabricante, con las siguientes características mínimas: - Activación del BOT Manager por servicio virtual. - Activación del BOT Manager por reglas de contenido. - Soportar aplicaciones WEB, aplicaciones móviles y API. - Soportar análisis de comportamiento profundo para determinar la intención de la conexión, inteligencia colectivida de bots, fingreprinting de browsers y de máquinas. - Permitir desde el balanceador, configurar al menos las siguientes respuestas ante ataques detectados: Permitir, Captcha, Bloqueo.
3.2	**REQUERIMIENTOS DE INSPECCIÓN SSL**
3.2.1	La solución debe proveer visibilidad SSL/TLS para ambos, el tráfico hacia el Datacenter y el tráfico saliente a Internet, permitiendo a la solución ser la responsible de la orquestación y distribución dinámica de tráfico entre dispositivos de seguridad.
3.2.2	La solución de inspección SSL debe soportar al menos los siguientes tipos de despliegue: - Solución transparente en capa 2. - Dispositivo en modo ruteo en capa 3.
3.2.3	La solución debe ser agnóstica a los dispositivos de seguridad conectados y debe soportar como mínimo, los siguientes tipos de dispositivos de acuerdo a su tipo de despliegue de red: - Dispositivos en capa 3, que pueden estar conectados en one-leg o two-legs. Ejemplos: Antimalware, Firewalls. - Dispositivos en capa 2 conectados en two-legs. Ejemplo: ATP, IPS. - Dispositivos pasivos en donde solo se copie el tráfico, como DLPs e IDS. Conectados en one-leg. - La solución debe soportar dispositivos tipo ICAP, como DLP activos y anti-virus.
3.2.4	La solución, para la inspección SSL de salida, debe soportar Proxy Transparente y Proxy Explícito.
3.2.5	La solución, para la inspección SSL de salida, debe soportar bypass de la inspección SSL la cual podrá definirse a través de como mínimo: - Dirección IP origen o destino.

	- Sitios específicos o categorías. Todo el licenciamiento necesario debe ser incluido.
3.2.6	La solución debe permitir agrupar los dispositivos de seguridad y balancear el tráfico hacia los dispositivos definidos en los grupos.
3.2.7	La solución debe permitir crear políticas de inspección que definan a que grupos de dispositivos de seguridad se debe enviar el tráfico a ser inspeccionado.
3.2.8	La solución debe permitir crear políticas que permitan manejar el tráfico que NO debe ser inspeccionado, por ejemplo, el tráfico en texto plano.
3.3	**REQUERIMIENTOS SEGURIDAD WEB Y APIs**
3.3.1	La solución debe incluir un servicio en nube para protección contra ataques en capa de aplicación web, Cloud Waf El servicio de Cloud WAF debe soportar despliegues siempre activos, a través de modificación de DNS y que no requieran modificación alguna de Hardware o Sofware del lado de los servidores a proteger. El servicio de Cloud WAF debe soportar un modelo de integración basado en API que no requiera cambios de DNS o BGP para proteger las aplicaciones y que cuente tenga las siguientes características: La arquitectura basada en API no requiere compartir el certificado digital. La arquitectura basada en API los requerimientos van directamente a la aplicación. El servicio de Cloud WAF debe proveer una cobertura completa de ataques en capa de aplicación WEB incluyendo todos los ataques descritos en el OWASP TOP 10 El servicio de Cloud WAF debe estar basado en un WAF con certificación ICSA Labs El servicio de Cloud WAF debe permitir integración con el SIEM local de la entidad El servicio de Cloud WAF soporta modificaciones programáticas sobre el servicio vía RESTful API El servicio de Cloud WAF debe proteger un total de 41 aplicaciones con ancho de banda máximo de 60 Mbps El servicio de cloud Waf debe soportar TLS versión 1.3 El servicio de Cloud WAF debe soportat IPv6 end to end, es decir, desde el cliente hasta los servidores de origen. El servicio de cloud WAF debe generar las políticas de seguridad de cada aplicación aprovisionada de forma automática a través de algoritmos de machine learning. El servicio de cloud WAF debe bloquear conexiones que no sean HTTP RFC Compliance

	El servicio de cloud Waf debe incluir protección contra ataques de tipo cookie poisoning, permitiendo el cifrado de las cookies importantes para garantizar que estas no sean modificadas del lado del cliente. El servicio de cloud Waf debe incluir un mecanismo de Fingerprinting que permita identificar de forma única el dispositivo que está ingresando a la aplicación web sin necesidad de conocer su dirección IP El servicio debe permitir limitar la tasa de tráfico con las siguientes funcionalidades: - Limitar la tasa de tráfico hacia todo el sitio. - Limitar la tasa de tráfico hacia un path específico. - Permitir configurar el tiempo de bloqueo para la IP origen que sobrepase la tasa de tráfico definida. El servicio de cloud WAF debe permitir la configuración de listas blancas de IP desde el portal de servicios, por cada aplicación aprovisionada. El servicio de cloud WAF debe permitir la configuración de bloqueo por geografía desde el portal de servicios, por cada aplicación aprovisionada. El servicio de cloud WAF, a través del portal, debe permitir crear reglas de control de acceso por IP a las aplicaciones protegidas. El servicio de cloud WAF, a través del portal, y por cada aplicación, debe permitir la redirección de trafico en base al contenido del mismo, como mínimo considerando: - Encabezados - Métodos - IP/CIDR - País de Origen - URI El servicio de cloud WAF, a través del portal, y por cada aplicación, debe permitir la creación de reglas para, remover y reescribir los encabezados en el request, como mínimo considerando: - Encabezados - Métodos - IP/CIDR - País de Origen - URI

	El servicio de cloud WAF, a través del portal, y por cada aplicación, debe permitir la creación de reglas para, remover, reescribir e insertar encabezados en el response.
3.3.2	La solución propuesta debe proteger contra ataques conocidos y ataques de día cero, soportando modelos de seguridad positivos y modelos de seguridad negativos Las aplicaciones aprovisionadas se podrán configurar en modo activo, bloqueando los paquetes de ataques de forma proactiva o en modo monitoreo, simplemente reportando eventos, pero no bloqueándolos. La política de seguridad no debe ser genérica, ni basada en políticas por defecto o mejores prácticas. Debe ser una política a la medida, ajustada a cada aplicación aprovisionada. Las políticas de seguridad generadas deben adaptarse a cambios en la aplicación optimizándose y actualizándose automáticamente, aunque la aplicación aprovisionada se encuentre en modo bloqueo de tráfico.
3.3.3	La solución propuesta debe proteger contra mínimo los siguientes ataques en capa de aplicación WEB: - XSS - SQL injections OS and LDAP - OS command injections - LDAP injections - SSI injections - XPath injections - Sensitive information leakage - Application DoS - CSRF - Parameter tampering - From field manipulation - Session hijacking - Cookie Manipulation & Poisoning - Application buffer overflows - Brute Force attacks - Access to predictable resource locations - Unauthorized navigation

	- Web server reconnaissance - Directory/path traversal - Forceful browsing - Hotlink - HTTP response splitting & protocol manipulation - Evasion and illegal encoding - XML and Web Services Attacks - Web services method restrictions and validation - HTTP RFC violations - HTTP request format and limitation violations - Use of revoked or expired client certificates - File upload violations - Clickjacking - Cross Site Scripting - Cross Site Request Forgery - Predictable Resource Location - Remote File Inclusions - Buffer overflow - Information leakage - Improper output Handling - Directory indexing - Access Control (White & Black list, Geolocation, anonymous proxies) - Known Vulnerabilities & Custom Rules - Anti-scrapping"
3.3.4	La solución debe incluir una suscripción que permita actualizar las firmas de ataques conocidos, base de datos de geolocalización e IP de proxies anónimos.
3.3.5	La solución debe permitir configurar un periodo de tiempo en el cual las nuevas firmas descargadas estarán aplicadas en modo reporte únicamente sin causar bloqueos. Luego de que el periodo expire, las firmas entrarán en modo bloqueo.

3.3.6	La solución debe soportar modo bypass configurable en cada aplicación. En este modo no se realiza ni inspección ni reportes de eventos de seguridad lo cual permite hacer debug de la solución de seguridad de forma rápida y sin cambios mayores a la configuración del servicio.
3.3.7	La solución debe incluir un mecanismo que permita priorizar los recursos de procesamiento otorgados a las aplicaciones más críticas.
3.3.8	La solución debe controlar el tiempo timeout de conexión de los clientes a nivel HTTP, definiendo para cada aplicación protegida: - El tiempo que espera por datos de request del cliente. - El tiempo que espera por una respuesta por parte del servidor.
3.3.9	La solución debe proteger contra ataques de denegación de servicio de tipo low and slow a través de análisis de comportamiento.
3.3.10	La solución debe aprovisionar de forma automática los tamaños de mensajes permitidos para los requerimientos del cliente y las respuestas enviadas por el servidor, definiendo como mínimo: - El tamaño del cuerpo del mensaje - El tamaño total de los encabezados - El tamaño total de un solo encabezado - El tamaño total de headers individuales.
3.3.11	La solución debe contar con un mecanismo de bloqueo por origen que cuente con las siguientes características mínimas: - Debe hacer seguimiento a los ataques generados por una dirección IP en particular. - Debe hacer seguimiento a los ataques generados por un fingerprinting de dispositivo particular. - Dependiendo al nivel de ataque, la IP o el Fingerprinting serán bloqueados por un tiempo en minutos configurable. - Las IP o los fingerprinting de los dispositivos se podrán desbloquear desde el WBI de la solución.
3.3.12	La solución debe enviar las IP bloqueadas por el mecanismo de source blocking a un mitigador de ataques DDoS del mismo fabricante, para que este efectúe el bloqueo en el perímetro.
3.3.13	La solución debe incluir un mecanismo de generación automática de política basado en el auto descubrimiento y en un análisis de amenazas realizado sobre los paths descubiertos.

3.3.14	El mecanismo de generación automática de políticas debe realizar como mínimo las siguientes acciones sin intervención humana: - Generar automáticamente los paths de cada aplicación - Configurar las protecciones para cada path configurado - Refinar las protecciones - Cambiar las protecciones de modo monitoreo a modo bloqueo
3.3.15	La solución debe continuar auto descrubriendo el sitio, modificando la política de seguridad y refinando las protecciones, aun estando sus protecciones en modo bloqueo.
3.3.16	La solución debe contar con una protección que evalué las solicitudes de los clientes y bloqueé aquellas que no hagan match con las expresiones definidas, las cuales deben contar como mínimo con las siguientes opciones de configuración - host - Path dentro de la aplicación - Método HTTP - Página - Expresión Regular
3.3.17	La solución debe contar con una protección contra ataques de fuerza bruta que bloquee intentos de atacantes de hallar el usuario y password de un usuario autorizado. La protección del lado del cliente debe tener la capacidad de bloquear automáticamente dominios sospechosos según su nivel de amenaza y permitir dominios legítimos con excepciones. El servicio de cloud WAF debe incluir un portal desde donde se aprovisionen los certificados digitales, aplicaciones y que incluya dashboards, eventos, analítica, alertas y reportes
3.3.18	La solución debe usar un motor de análisis de consulta de base de datos para detectar comandos de tipo SQL que los hackers puedan usar para realizar una manipulación de datos.
3.3.19	La solución debe aplicar múltiples heurísticas en valores de parámetros para detectar valores codificados en Base64. Los parámetros códificados, deben decodificarse y luego se debe aplicar la política de seguridad sobre los mismos.
3.3.20	La solución debe permitir crear reglas para controlar el upload de archivos con al menos los siguientes parámetros:

	- Path de la aplicación. - Extensión del archivo - Método HTTTP - Permitir descarga de los archivos
3.3.21	La solución debe evaluar las respuestas de los servidores para determinar si estas están exponiendo información sensible, con al menos las siguientes características: - Debe redirigir a página de bloqueo u ocultar los caracteres, si la respuesta del servidor incluye información de tarjetas de crédito. - Debe redirigir a página de bloqueo u ocultar los caracteres, si la respuesta del servidor incluye un parámetro personalizado por el administrador a través de expresiones regulares.
3.3.22	La solución debe permitir evaluar parámetros dentro de una solicitud de usuario detectando y bloqueando aquellas que no sean válidas de acuerdo a los siguientes criterios que podrán ser configurados: - Tipo de parámetro: Long, Float, Número, Letra, Alfa numérico, Expresión, Cadena, Null Parameter. - Longitud mínima. - Longitud máxima. - Si permite o no valores nulos.
3.3.23	La solución debe permitir cifrar la información de cookies para mitigar ataques que busquen manipular el estado de la sesión.
3.3.24	La solución debe permitir cifrar la información en parámetros de tipo form, path y query para bloquear ataques que busquen manipular el estado de la sesión.
3.3.25	La solución debe incluir una base de datos de firmas de vulnerabilidades conocida.
3.3.26	La solución debe permitir crear patrones personalizados para que sean validados junto con los incluidos en la base de datos de firmas de ataques conocidos. El portal debe soportar doble factor de autenticación. El portal debe soportar FiM (Federated Identity Management) para autenticación y autorización. El portal debe permitir visualizar los cambios realizados por los administradores y debe conservar la información por al menos 3 meses.
3.3.27	La solución debe permitir configurar protección contra ataques de tipo Directory Listing para un grupo de hosts o para un host en particular.

3.3.28	La solución debe permitir ofuscar la estructura real de la aplicación de un atacante potencial a través de la configuración de reescritura de la URL (URL Rewrite)
3.3.29	La disponibilidad mínima del servicio debe ser de 99.999%, de la siguiente manera: El servicio de Cloud WAF debe ser un servicio de seguridad administrado por el fabricante con disponibilidad 7x24x365 y durante el periodo de garantía es decir a 3 años. El servicio administrado debe contar con los siguientes mecanismos de contacto: Portal Web de Soporte Soporte vía e-mail Soporte Telefónico El servicio debe monitorear constantemente el estado de salud de las aplicaciones configuradas El servicio administrado debe proporcionar asistencia durante la fase de onboarding de las aplicaciones El servicio administrado debe generar alertas proactivas automáticas de seguridad El servicio debe contar, como mínimo, con los siguientes estándares de seguridad y calidad PCI-DSS v3.1 (Payment Card Industry Data Security Standard) ISO/IEC 27001:2013 (Information Security Management Systems) ISO/IEC 27032:2012 (Security Techniques -- Guidelines for Cybersecurity) ISO 27017:2015 (Information Security for Cloud Services) ISO 27018:2014 (Information Security Protection of Personally identifiable information (PII) in public clouds) ISO 28000:2007 (Specification for Security Management Systems for the Supply Chain) US SSAE16 SOC-1 Type II, SOC-2 Type II
3.3.30	La solución debe soportar device fingerprinting para realizar seguimiento a las actividades utilizando un identificador de dispositivo y no la dirección IP origen.
3.3.31	La solución debe soportar protección contra ataques LFI (Local File Inclusión), RFI (Remote File Inclusion), y SSRF (Server Side Request Forgery).
3.3.32	La solución debe soportar seguridad sobre websockets incluyendo ataques DDoS de tipo low and slow.
3.3.33	La solución debe registrar al menos los siguientes eventos de auditoría:

	- Modificaciones de configuración. - Intentos de acceso no autorizados. - Reinicios de la solución o servicios.
3.3.34	La solución debe registrar los eventos de seguridad detectados o bloqueados incluyendo como mínimo la siguiente información: - Severidad del evento - Fecha - Descripción corta del evento - El tipo de ataque. - Dirección IP origen - Geolocalización - Puerto Origen - Host - Path de la aplicación - URI - Nombre del Parámetro - Valor del Parámetro - Tipo de Parámetro
3.3.35	La solución debe permitir refinar las políticas desde la vista de los eventos de seguridad.
3.3.36	La solución debe permitir visualizar, para cada evento registrado, el header HTTP de la solicitud.
3.3.37	La solución debe permitir visualizar, para cada evento registrado el header HTTP de la respuesta del servidor, cuando la política se encuentre en modo monitoreo
3.4	**SEGURIDAD DE LAS API**
3.4.1	La solución debe soportar protección a Restful API
3.4.2	La solución debe permitir importar el archivo de Open API en versiones 2 y 3 en formatos json y yaml.
3.4.3	La solución debe soportar el “merge” de dos archivos Open API permitiendo configurar el comportamiento del “merge” sobre los endpoints y métodos.

3.4.4	La protección de API debe soportar manejo de cuotas, definiendo el número de llamados de API en un rango de tiempo configurable por cada endpoint.
3.4.5	La solución debe soportar schema enforcement sobre los métodos, endpoints, parámetros de path, query, header y body requests.
3.4.6	La solución debe soportar las siguientes acciones en el Schema Enforcement: Bloquear, Schema enforcement, Pasivo y Bypass
3.4.7	La solución debe soportar que después de validar el requerimiento API, estos sean inspeccionados por los otros módulos del WAF para detectar ataques embebidos.
4.	**OBLIGACIONES GENERALES DEL CONTRATISTA Y FABRICANTE**
	En caso de un ataque cibernético relacionado con la solución, el contratista en acompañamiento del fabricante debe proveer en las instalaciones del comando 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 al 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. • 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. • 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 durante el periodo de garantia.es decir por tres años.
5	**EXPERIENCIA Y CERTIFICACIONES POR FABRICANTE**
	• Implementación: La implementación debe ser realizada directamente por ingenieros del fabricante garantizando la implementación, en compañía por oferente adjudicatorio. ✓ El fabricante debe indicar mediante documento independiente el alcance del servicio Silver Shield Package. y los servicios de soporte especializados ofrecidos durante los tres años de garantía. ✓ El fabricante debe indicar mediante documento independiente el alcance del SLA (Service Level Agreement), para los casos que se presenten. Líder del Proyecto o Se requiere que la implementación 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 tres (03) años. ✓ Debe contar con capacitación o certificaciones de proyectos ✓ Debe haber sido líder técnico de proyectos de seguridad.

	✓ Con más de 5 años o más de experiencia apoyando, diseñando, implementando y manteniendo soluciones de redes y seguridad de informática e implementación de Cloud WAF. ✓ Debe ser Personal certificado directo del fabricante para garantizar la implementación de la solución y con las siguientes certificaciones: - RADWARE CERTIFIED APPLICATION SPECIALIST - RADWARE CERTIFIED APPLICATION SECURITY SPECIALIST Implementación o Se requiere que la implementación de la solución, la realice como mínimo dos (02) 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 tres (03) años. ✓ Debe haber participado en al menos un proyecto de implementación CLOUD WAF ✓ Debe ser Personal certificado directo del fabricante para garantizar la implementación de la solución y con las siguientes certificaciones: - RADWARE CERTIFIED APPLICATION SPECIALIST - RADWARE CERTIFIED APPLICATION SECURITY SPECIALIST Nota: Se debe anexar hoja de vida completamente diligenciada y anexar certificado solicitado al momento de presentar la oferta cada uno de los ingenieros, este requerimiento debe ser directamente solicitado al fabricante.
5.1	**EXPERIENCIA Y CERTIFICACIONES POR PARTE DEL CONTRATISTA**
	PERSONAL REQUERIDO: PERFIL INGENIERO PARA EL SOPORTE NIVEL 1 Y 2 Se requiere que lo servicio de soporte especializado, la realice como mínimo un (01) ingeniero con el siguiente perfil: • 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: • Copia de diploma y/o acta de grado del ingeniero presentado en la propuesta. • El ingeniero presentado en la propuesta deberá contar con conocimientos avanzados en los productos descritos en las especificaciones técnicas, dado que el administrador de seguridad apoyará la operación y administración de la solución • Debe adjuntar copia de certificación RADWARE CERTIFIED APPLICATION SPECIALIST y/o RADWARE CERTIFIED APPLICATION SECURITY SPECIALIST • Debe haber participado en al menos un proyecto de implementación CLOUD WAF

	• El ingeniero debe ser de nacionalidad colombiana, y pertenecer por nomina al proponente 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).
5.1.1	ALCANCE SOPORTE GARANTÍA ESPECIALIZADO POR CONTRATISTA
	El contratista debe efectuar durante la ejecución del contrato según cronograma acordado entre el contratista y el supervisor del contrato deben incluir como mínimo las siguientes actividades: • Actualizaciones de software (Upgrade, Update, criticas 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. • Ante nuevas versiones y/o parches que la entidad considere necesarios para la operación, el contratista estará en disposición y capacidad de instalarlos previa presentación de un plan de trabajo • 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. • Emisión de recomendaciones de las plataformas a través de un informe técnico, al supervisor del contrato. En caso de presentarse fallas en la solución el contratista deberá efectuar correctivos todas las veces que se requiera deben incluir como mínimo: • 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 Y cumplir con lo descrito en el ítem 1.24