

FICHA TECNICA ANTIDDoS

OBJETO: ADQUISICION DEL SISTEMA DE PROTECCIÓN Y MITIGACIÓN DE ATAQUES DE DENEGACIÓN DE SERVICIO DISTRIBUIDO (ANTI-DDoS) DE ACUERDO CON EL ANEXO TÉCNICO.

Con el fin de garantizar la continuidad operativa, disponibilidad y protección de los servicios tecnológicos institucionales expuestos a redes públicas de comunicaciones, la FAC) requiere fortalecer y mantener sus capacidades de defensa frente a ataques de Denegación de Servicio Distribuido (DDoS), preservando los niveles de protección, monitoreo y mitigación implementados sobre la infraestructura tecnológica institucional. Para tal fin, se requiere la adquisición, instalación, configuración, puesta en operación y soporte de una solución especializada de mitigación AntiDDoS, mediante el suministro de un equipo de seguridad tipo *appliance* instalado en sitio (*on-premise*), junto con la suscripción de los servicios asociados, actualización de firmas y mecanismos de protección, soporte técnico especializado, mantenimiento y demás componentes requeridos para su adecuada operación durante la vigencia contratada.

La necesidad identificada obedece a la importancia de garantizar la disponibilidad y continuidad de los servicios tecnológicos institucionales frente a amenazas cibernéticas de creciente complejidad, así como al crecimiento proyectado de la infraestructura tecnológica que soporta el cumplimiento de la misión institucional. Durante el proceso de planeación se tuvo en consideración la experiencia operativa acumulada por la Institución durante varios años en la administración de este tipo de tecnologías, la madurez alcanzada en los procesos de monitoreo, análisis, gestión y mitigación de eventos de seguridad, la evolución de las políticas y procedimientos de protección implementados, así como el conocimiento técnico y la apropiación tecnológica adquirida por la institución.

En este sentido, la solución requerida busca preservar y fortalecer las capacidades institucionales actualmente desarrolladas, mantener la continuidad de los procedimientos de protección, monitoreo y mitigación establecidos, garantizar una transición tecnológica controlada que minimice riesgos operacionales sobre la infraestructura protegida y asegurar que la Institución continúe contando con una capacidad efectiva de detección, análisis, clasificación y mitigación de tráfico malicioso asociado a ataques de Denegación de Servicio Distribuido (DDoS). De igual manera, la adquisición permitirá conservar y potenciar las capacidades técnicas, operacionales y de administración construidas durante años de experiencia institucional, garantizando que la FAC mantenga una postura de protección adecuada sobre su infraestructura tecnológica crítica, alineada con las necesidades actuales, la evolución de las amenazas y los objetivos de continuidad y resiliencia operacional requeridos para el cumplimiento de su misión institucional.

En atención a lo anterior, se establecen las siguientes especificaciones técnicas y condiciones mínimas requeridas para la prestación del servicio:

Detalle	Descripción	Cantidad AUTORIZADA PPTO
Hardware	Mitigador	1
Suscripción	Servicios asociados a la plataforma de administración, monitoreo, gestión centralizada, actualización de mecanismos de protección y soporte especializado de la solución AntiDDoS.	12 meses

ASPECTOS GENERALES DE LA SOLUCIÓN

El oferente deberá identificar expresamente en su propuesta la marca y referencia de la solución ofertada, garantizando que corresponde a una solución vigente, soportada por el fabricante y que cumple integralmente las capacidades funcionales exigidas en la presente ficha técnica, adjuntando la ficha técnica oficial vigente emitida por el fabricante y el enlace oficial (URL) donde se encuentren publicadas sus especificaciones técnicas. La documentación presentada deberá permitir a la Institución verificar el cumplimiento integral de los requisitos funcionales, de capacidad, rendimiento, administración, interfaces, mitigación y escalabilidad exigidos en la presente ficha técnica.

La solución estará orientada a la protección del tráfico perimetral de la red institucional, garantizando la disponibilidad de los servicios tecnológicos frente a ataques en capa de red (L3) y capa de transporte (L4) del modelo OSI.

GARANTIA TÉCNICA

El periodo de garantía para los bienes sujetos a contratar y los servicios que se desprendan en relación del objeto contractual serán de 12 meses, iniciados a partir de la suscripción del acta de inicio.

El contratista debe garantizar una disponibilidad de servicio de mínimo el 99.9% durante la ejecución del contrato y mientras los servicios se encuentren activos. Como parte de la garantía, la FAC también recibirá soporte por parte del contratista para la gestión de problemas en el servicio que preste el equipo sujeto a contratar. Al inicio del periodo de garantía, el contratista deberá informar los datos de la persona y su información de contacto, responsable de responder por cualquier novedad que pueda presentarse sobre el funcionamiento.

DESCRIPCIÓN DEL PROCESO DE IMPLEMENTACIÓN

La ejecución del contrato se desarrollará de manera estructurada a través de las siguientes fases:

Fase 1 – Suministro del equipo

El contratista deberá realizar la entrega del equipo AntiDDoS junto con sus respectivos componentes, licencias y accesorios necesarios para su funcionamiento, en las instalaciones del Datacenter Institucional ubicado en el Comando de Transporte Militar (CATAM).

Fase 2 – Instalación

El contratista realizará la instalación física del equipo en el Data Center institucional Ubicado en las Instalaciones del Comando Aéreo de Transporte Militar Bogotá D.C, Colombia, incluyendo su integración a la infraestructura de red existente, garantizando condiciones de alta disponibilidad y operación segura.

Fase 3 – Configuración

El contratista llevará a cabo la configuración lógica de la solución, incluyendo la definición de políticas de mitigación, perfiles de protección, umbrales y parámetros de detección, acorde a la arquitectura de red de la Entidad.

Fase 4 – Pruebas de funcionamiento

Se deberán ejecutar pruebas técnicas que permitan validar el correcto funcionamiento del sistema, incluyendo pruebas de detección, mitigación y estabilidad del tráfico, sin afectar la operación normal de la infraestructura

Fase 5 – Puesta en operación

Una vez validadas las pruebas, el sistema entrará en operación formal, protegiendo el tráfico institucional en tiempo real frente a ataques DDoS.

Fase 6 – Transferencia de conocimiento

atendiendo la necesidad institucional de garantizar la adecuada apropiación y administración de la solución de protección Anti-DDoS, se considera procedente establecer como obligación del contratista que:

Durante la vigencia de la suscripción el contratista proporcionará actividades orientadas al fortalecimiento de habilidades en la administración autónoma de la solución ofrecida, impartidas por la casa matriz o fabricante, para dos (02) personas técnicas de la Dirección de Seguridad Informática y Electrónica. La actividad deberá contemplar una intensidad mínima de cuarenta (40) horas y podrá desarrollarse en modalidad virtual o presencial, de acuerdo con la oferta académica y disponibilidad definida por el fabricante, así mismo debe ser impartidas directamente por el fabricante o por instructores autorizados por el fabricante y que cuenten con certificación vigente sobre la tecnología ofrecida.

Cuando la modalidad ofrecida por el fabricante implique desplazamiento fuera de la ciudad de Bogotá D.C., el contratista deberá asumir la totalidad de los costos asociados a la participación de los funcionarios designados por la Institución, incluyendo inscripción, transportes, alojamiento y alimentación, los cuales deberán encontrarse incluidos dentro del valor ofertado, sin que ello genere costos adicionales para la Institución.

Lo anterior se justifica basado en lo expuesto en la circular No. FAC-S-2025-012565-CR del 12 de noviembre de 2025 / MDN-COGFM-FAC-COFAC-JEMFA-CODAF, cuyo asunto es el Análisis y evaluación para la inclusión de costos de comisiones al exterior dentro de la estructuración contractual de procesos, teniendo en cuenta lo anterior y en la necesidad de no afectar los recursos internos destinados a viáticos, garantizar la ejecución efectiva del componente de transferencia de conocimiento y dar cumplimiento a los lineamientos impartidos por el Comando de Apoyo de la Fuerza en materia de estructuración contractual, conforme a la normatividad vigente de contratación estatal.

Fase 7 – Soporte y mantenimiento y actualizaciones.

Una vez activada la suscripción de la solución, el contratista deberá garantizar durante doce (12) meses el soporte técnico especializado, la actualización de firmas y mecanismos de detección y mitigación, así como el mantenimiento requerido para la correcta operación de la plataforma, de acuerdo con la vigencia del licenciamiento contratado.

Los siguientes son los términos de respuesta del **SOPORTE TECNICO**.

PRIORIDAD		DESCRIPCIÓN	TÉRMINO DE RESPUESTA
1	CRITICA	La producción está detenida o severamente impactada de manera que no se puede continuar trabajando. La operación es de misión crítica para la entidad y/o está en situación de emergencia.	De manera remota o la indicada por el supervisor del contrato (2) horas.
2	ALTA	Experimenta perdida del servicio, algunas características importantes no pueden ser utilizadas, sin	De manera remota o la indicada por el supervisor del contrato (4) horas.

		embargo, la operación continua de manera restringida.	
3	MEDIA	Experimenta una pérdida de servicio menor, el impacto es un inconveniente.	De manera remota o la indicada por el supervisor del contrato (8) horas.
4	BAJA	No impacta la operación del programa, no se experimenta pérdida del servicio y no se impide la operación de los sistemas.	De manera remota o la indicada por el supervisor del contrato (24) horas.

CERTIFICACIÓN Y ESPECIALIZACIÓN DEL OFERENTE

El oferente deberá acreditar que se encuentra autorizado por el fabricante de la solución ofertada para comercializar, implementar, configurar, soportar y realizar actividades de puesta en funcionamiento de la plataforma propuesta.

Dicha acreditación deberá realizarse mediante certificación vigente expedida por el fabricante o su representante autorizado, en la cual conste que el oferente mantiene una relación comercial activa y cuenta con las competencias técnicas requeridas para suministrar, implementar, administrar y soportar la solución ofertada.

La certificación deberá ser presentada junto con la oferta y será objeto de verificación durante la etapa de evaluación técnica por parte de la Institución.

PERSONAL TÉCNICO PARA LA IMPLEMENTACIÓN

El contratista deberá garantizar que las actividades de instalación, configuración, implementación, puesta en funcionamiento y transferencia de conocimiento sean ejecutadas por personal profesional con experiencia comprobada en tecnologías de mitigación de ataques DDoS. Antes del inicio de las actividades técnicas, deberá presentar al supervisor del contrato la documentación que acredite la formación profesional, experiencia y certificaciones técnicas vigentes del personal que será asignado al proyecto.

Las certificaciones deberán ser emitidas por el fabricante de la solución ofertada o por entidades autorizadas por éste, y corresponder a actividades de arquitectura, instalación, implementación, configuración, administración o soporte de la tecnología propuesta. La validación de esta documentación será realizada por el supervisor de la Institución antes del inicio de la implementación. Cualquier sustitución de personal deberá contar con autorización previa y garantizar un perfil técnico igual o superior al inicialmente presentado.

TIEMPOS DE EJECUCIÓN

La implementación de la solución deberá ejecutarse dentro de los plazos establecidos a continuación, los cuales constituyen tiempos máximos de referencia para el desarrollo de cada actividad. El cumplimiento de cada fase será verificado y validado por el supervisor designado por la Institución. Los retrasos atribuibles al contratista podrán dar lugar a la aplicación de las medidas contractuales que correspondan.

- Suministro e instalación: hasta treinta (30) días calendario.
- Configuración y pruebas: hasta treinta (30) días calendario.

- Puesta en operación: posterior a la validación técnica por parte del supervisor designado por la Institución.
- Soporte técnico, actualización de firmas y servicios asociados: durante los doce (12) meses de vigencia del licenciamiento contratado.

ENTREGABLES

El contratista deberá entregar como mínimo:

- Equipo AntiDDoS instalado y operando
- Configuración de políticas de seguridad implementadas
- Documento de arquitectura e integración
- Informe de pruebas realizadas
- Acta de puesta en operación
- Evidencia de capacitación y transferencia de conocimiento
- Documentación técnica de la solución implementada

INTERACCIÓN CON LA ENTIDAD

La ejecución del contrato se realizará en coordinación con el personal técnico de la Institución, quien validará las actividades desarrolladas en cada fase y emitirá el respectivo concepto de cumplimiento para la puesta en operación del sistema.

El contratista deberá garantizar que todas las actividades se ejecuten sin afectar la disponibilidad de los servicios tecnológicos institucionales.

REQUERIMIENTOS DE HARDWARE Y SOTWARE

ARQUITECTURA:

Cantidad de equipos solicitados: **01 junto con el licenciamiento que se requiera para su funcionamiento.**

- La solución de mitigación de ataques DDoS se debe integrar a la red de forma transparente en capa 2.

La solución de mitigación de ataques DDoS debe tener la siguiente configuración de interfaces para su integración a la red:

- La solución deberá incluir como mínimo cuatro (4) interfaces de fibra óptica 10 Gigabit Ethernet (10GE) multimodo, con sus respectivos transceptores ópticos SFP+ de 10 Gbps multimodo, requeridos para su integración y operación. Así mismo, deberá incluir mecanismo de bypass asociado a dichas interfaces, que garantice la continuidad del tráfico ante falla del equipo o pérdida de energía.
- El dispositivo debe incluir al menos dos interfaces de gestión (Management Ports) y administración por consola RJ45.

- La solución debe soportar bypass por software para pares de puertos individuales.
- La solución de mitigación de ataques DDoS debe soportar la inspección de los encabezados internos o externos de tuneles L2TP, GRE, GTP, IPinIP.
- La solución debe poder monitorear y alertar sobre el uso de CPU de cada política definida de forma independiente.
- La solución de mitigación de ataques DDoS debe soportar IPv4 e IPv6.
- La solución de mitigación de ataques DDoS debe soportar un número ilimitado de sesiones concurrentes de ataque.
- La solución de mitigación de ataques DDoS debe incluir doble fuente de poder hot swappable.

CAPACIDAD:

- La solución de mitigación de ataques DDoS debe estar licenciada para un throughput de tráfico legítimo de al menos 10 Gbps por equipo.
- La solución de mitigación de ataques DDoS debe soportar crecimiento de throughput por licenciamiento sobre el mismo hardware de hasta 40 Gbps por equipo.
- La solución de mitigación de ataques DDoS debe estar licenciada para soportar una capacidad de mitigación mínima de 50 Gbps por equipo
- La solución de mitigación de ataques DDoS debe estar licenciada para soportar una capacidad de mitigación mínima de 45 MPPS por equipo.
- La solución de mitigación de ataques DDoS debe tener una latencia menor a 60 microsegundos.

FUNCIONALIDADES DE DETECCION Y MITIGACION DE ATAQUES:

- La solución debe proteger contra al menos las siguientes anomalías de tráfico:

Checksum incorrecto de IPV4.

Encabezado IPv4 o longitud total invalido.

Tamaño de Encabezado Capa 4 invalido.

TTL igual a 0.

Cabecera IPV6 inconsistente.

Límites de salto IPV6 alcanzados.

Protocolo Capa 4 no soportado.

TCP flags invalido.

Dirección de origen o destino igual al Local Host.

Dirección de origen igual a la dirección de destino.

Puerto capa 4 de origen o destino igual a cero.

Cabecera de GRE invalida

Versión GRE Incorrecta

- La solución debe operar a través de políticas de seguridad con distintas configuraciones de detección y mitigación de acuerdo con los objetos protegidos.
- La solución debe soportar la configuración de dos modos de operación, modo reporte y modo bloqueo. Estos se podrán configurar por política de seguridad y por tipo de protección específica dentro de la política de seguridad.
- El mitigador debe contar con análisis de comportamiento, aprendiendo del tráfico de la red para detectar anomalías de tráfico y prevenir ataques de día cero incluyendo al menos las siguientes inundaciones de tráfico:

Inundación de red UDP.

Inundación de red ICMP.

Inundación de red IGMP.

Inundación de red TCP con flag SYN.

Inundación de red TCP con flag RST.

Inundación de red TCP con flag SYN y ACK.

Inundación de red TCP con flag Fin y ACK.

Inundación de red TCP Frag

Inundación de red UDP Frag

- La solución debe incluir un mecanismo preciso de detección de inundaciones UDP que tenga en cuenta parámetros que varíen con la tasa de tráfico y parámetros que no varíen con la tasa de tráfico, incluyendo:

Ancho de banda UDP.

Tasa de paquetes por segundo.

Tasa de conexiones por segundo

- La solución debe permitir configurar un umbral de ancho de banda de supresión de aprendizaje, para evitar que las líneas bases se distorsionen en bajo tráfico.
- La solución debe generar de forma automática firmas descriptivas para bloquear el tráfico o la actividad de red potencialmente maliciosos, creados de forma dinámica, automática y en tiempo real. Estas firmas deben ser adaptativas en base al tipo de ataque.
- La solución debe proteger contra ataques de tipo ráfaga (burst attacks) identificando que una nueva ráfaga de tráfico pertenece a una firma en tiempo real previamente creada.
- La solución debe incluir un mecanismo de prevención de overblocking de tráfico el cual valide y refresque la firma, si se está bloqueando más tráfico del debido.
- La solución debe permitir especificar un límite de tasa de tráfico que servirá como un método alternativo automático a la firma en tiempo real de red.
- La solución de mitigación de ataques DDoS debe incluir un mecanismo de límite de conexiones TCP y sesiones UDP que cumpla con las siguientes características:

La solución debe contar el número de conexiones TCP o sesiones UDP abiertas por cliente, por servidor, o por la combinación de cliente y servidor.

La solución debe permitir descartar los paquetes que pasen el límite establecido.

La solución debe permitir suspender el tráfico por un tiempo determinado si este pasa del límite establecido.

- La solución de mitigación de ataques debe incluir un mecanismo que haga seguimiento y bloquee paquetes que superen una tasa de PPS en sesiones definidas.
- La solución debe incluir protección contra ataques DDoS de inundación de paquetes fuera de estado.
- La solución debe incluir protección contra ataques DDoS de tipo SYN Flood.
- La protección de SYN Flood debe prevenir contra ataques de tipo Spoofed-SYN-flood que vayan dirigidos a múltiples puertos destinos, a través del seguimiento de paquetes SYN enviados a toda la red configurada en la política.

- La protección de SYN Flood debe contar con al menos dos métodos de autenticación TCP: ACK Fuera de Secuencia y Proxy Transparente.

Los filtros de tráfico deben permitir como mínimo seleccionar los siguientes criterios para hacer match al tráfico:

Red de Origen

Red de Destino

Puerto Origen

Puerto Destino

Protocolo

Tamaño del Paquete

Flags TCP

Time to Live (TTL)

Número de Secuencia TCP

Type of Service (ToS) / DSCP

Fragment Offset

Fragment ID

Expresiones Regulares de Payload3

Los filtros de tráfico deben permitir configurar límites de tráfico en PPS o bps, sobre el tráfico que haga match con los criterios definidos.

- La solución debe soportar verificaciones de cumplimiento RFC para todo el tráfico DNS inspeccionado.
- La solución debe soportar la configuración de listas blancas DNS para fuentes y/o registros (DNS records) confiables.
- La solución debe soportar limitación de tasa (rate-limit) basada en QPS (queris por segundo) para el tráfico DNS.
- La solución debe detectar y mitigar automáticamente inundaciones de bajo volumen (micro-inundaciones o carpet bombing) dirigidas a hosts, subredes o servicios individuales dentro de una política, aunque el tráfico total de la política no supere sus umbrales. Debe hacerlo mediante detección granular por objeto protegido o un mecanismo equivalente.

Ante este tipo de ataque, la solución debe aplicar de forma escalonada al menos dos mecanismos de mitigación dentro de las capacidades nativas de la plataforma, tales como filtrado dinámico, bloqueo de las fuentes de mayor volumen o limitación de tasa.

La sensibilidad de detección y los parámetros de mitigación deberán ser configurables por el operador.

La funcionalidad deberá encontrarse soportada directamente por el fabricante dentro de la versión de software ofertada, sin requerir componentes adicionales de terceros para su operación.

La solución debe permitir crear reglas de listas de bloqueo y listas permitidas (allow list / block list), incluyendo al menos los siguientes parámetros de clasificación:

Red Origen

Puerto Origen

Red Destino

Puerto Destino

Protocolo

- La solución de mitigación de ataques DDoS debe incluir un mecanismo de protección contra escaneos de puertos TCP, UDP e ICMP.
- La protección contra escaneos debe generar una firma en tiempo real para bloquear el escaneo de puertos realizado.
- La solución de mitigación de ataques DDoS debe incluir una protección basada en firmas de ataques conocidos que permita al menos mitigar los siguientes tipos de ataques:

Inundaciones TCP, UDP e ICMP lanzados desde herramientas conocidas.

Vulnerabilidades a nivel de servidores: Web, e-mail, FTP, SQL, DNS, SIP

- La protección basada en firmas de ataques conocidos debe incluir grupos de firmas preconfigurados para ser aplicados en las políticas.
- La protección basada en firmas de ataques conocidos debe permitir crear grupos de firmas por elementos comunes y aplicar los grupos de firmas en las políticas.
- La protección basada en firmas debe permitir a los operados crear sus propias firmas.
- La solución de mitigación de ataques DDoS debe incluir una suscripción para actualización de la protección basada en firmas.

- La solución de mitigación de ataques DDoS debe incluir una suscripción que permita el bloqueo por geolocalización, debe poder habilitarse a una política de seguridad particular, sin que se afecte el tráfico que haga match con otras políticas. Dentro de dicho perfil se podrán definir al menos las siguientes acciones:

Bloquear las geografías seleccionadas.

Permitir las geografías seleccionadas.

Permitir las geografías hasta que se supere un umbral determinado por el operador (en PPS o kbps/Mbps)

- La solución de mitigación de ataques DDoS debe incluir una lista de IP de mala reputación productos del centro de investigación del fabricante, que será actualizada periódicamente.

- La lista de IP debe incluir al menos las siguientes categorías:

Atacantes Activos: Direcciones IP que han sido correlacionados y se han determinado como maliciosas.

Tor Exit Nodes: Una IP que es un Tor Exit Node, sin importar si ha participado o no en actividades de ataques.

Web Attacks: Una IP que ha hecho intentos de violaciones Web.

Scanners

- La lista de IP maliciosas, en conjunto con las acciones configuradas por categorías, debe aplicarse sobre cada política de seguridad.
- La solución debe ofrecer una funcionalidad de Protección Basada en Sistemas Autónomos (ASN) para permitir el control del tráfico en función del origen de la red.
- La solución debe actuar como un punto de control de feeds, lo que permite gestionar varios feeds y fuentes de datos en un solo lugar. Esto incluye feeds de terceros, listas de bloqueo regulatorias, listas de inteligencia de alta capacidad entre otros. Estas listas pueden ser cargadas usando la interfaz gráfica o de forma automatizada vía API.

CONSOLA DE ADMINISTRACION:

- La solución debe incluir un elemento de gestión y control centralizado que soporte la administración y monitoreo de todos los mitigadores que hacen parte de la propuesta.

- El elemento de gestión y control centralizado debe incluir un panel que permita el monitoreo de toda la solución en tiempo real.

- El panel de monitoreo en tiempo real debe mostrar el estado general de la solución:

Situación general, si estamos o no bajo ataque.

Resumen de tráfico actual, incluyendo tráfico de descartado y tráfico autenticado.

- El panel de monitoreo en tiempo real debe incluir un campo de búsqueda que permita filtrar la información desplegada utilizando al menos los siguientes criterios:

Filtro a través de una IP específica.

Filtro por el mitigador.

Filtro por política.

- El panel de monitoreo en tiempo real debe mostrar los siguientes gráficos de uso:

Gráficos del tráfico manejado por los mitigadores en bps y pps.

Gráficos de nuevas conexiones y conexiones concurrentes.

Gráficos de tráfico por mitigación en curso.

- El panel de monitoreo en tiempo real debe mostrar un listado de todas las políticas que incluya el estado de cada uno de ellos, indicando al menos:

Si la política se encuentra bajo ataque.

Nombre de la política.

Ancho de banda entrante hacia la política.

Tráfico siendo descartado sobre la política.

Tráfico siendo autenticación.

- El panel de monitoreo en tiempo real debe mostrar un listado de todos los mitigadores, agrupando las métricas de ancho de banda, tráfico descartado y autenticado u número de políticas por cada mitigador.
- El panel de monitoreo en tiempo real debe mostrar un listado con los eventos de detección de ataques asociados a las políticas, tanto los que ocurren en tiempo real, como los históricos, aquellos que han ocurrido previamente.
- El listado de los eventos de detección se debe indicar el mitigador, la política de seguridad, nombre del evento, la acción tomada por el mitigador, la categoría del ataque, la duración y la hora de inicio del ataque.

- Para los ataques detectados la solución debe mostrar el detalle de los mismos incluyendo permitiendo ver muestras de los paquetes que hacen parte del ataque y también descargar PCAPs de los ataques en caso de que aplique.
- La solución debe permitir realizar capturas en tiempo real con el fin de obtener visibilidad del tráfico tanto en tiempo de paz como durante un ataque.
- La solución debe incluir un panel de analítica de red que permita el monitoreo de tráfico en tiempo de paz, permitiendo filtrar el tráfico por mitigador o por política.

- La analítica de red debe incluir como mínimo la siguiente información para cada activo protegido:

Gráficos de Tráfico.

TOP IP Origen.

TOP IP Destino.

TOP Aplicaciones.

TOP Protocolos.

TOP Países

Tendencias de la última semana.

- El panel de analítica de red debe permitir exportar la información mostrada en un rango de tiempo determinado en formato PDF.
- La solución debe proporcionar una visualización completa de los detalles del ataque para los eventos de detección que lo ameriten, incluyendo ID del ataque, objeto protegido, hora de inicio, duración, nombre del ataque, firmas asociadas y atributos contextuales como IPs de origen/destino, puertos y protocolos. La descarga directa de archivos de captura de paquetes (PCAP) desde la misma vista del evento.
- La plataforma debe ofrecer un panel de Analítica del Ataque que visualice los principales orígenes y destinos del tráfico malicioso (por dirección IP de origen, país, puerto, protocolo y SNI) mediante widgets interactivos. Debe mostrar tanto el volumen de tráfico (bps/pps) como la duración del evento, permitir alternar entre métricas y soportar hasta los 100 principales valores por cada parámetro.
- La solución de gestión centralizada debe incluir un módulo capaz de realizar reportes con al menos las siguientes características:

Capacidad de generar reportes por dispositivo y política de seguridad.

Programar los reportes y enviarlos vía correo electrónico.

Los reportes deben estar disponibles en formatos PDF, HTML o CSV.

- Los reportes deben ser personalizables y deben permitir elegir la información a incluir en los reportes entre al menos la siguiente información:

Ataques recibidos en el periodo de tiempo seleccionado.

Top ataques por geolocalización.

Gráficos de tráfico (bps y pps), Conexiones por Segundo y Conexiones concurrentes.

TOP Ataques por duración.

TOP Ataques por volumen.

TOP Ataques por acción del mitigador.

TOP Ataques por categoría de amenaza.

TOP IP Destinos atacados.

TOP IP orígenes que atacan.

Ataques por política.

Ataques por Firma de seguridad.

- El módulo de reportes debe incluir un reporte de los ataques generados por la lista de IPs de mala reputación, presentando al menos:

TOP de los ataques por geolocalización.

TOP de los ataques por IP

TOP de los ataques por actividad maliciosa.

Total, hits recibidos desde las IP maliciosas.

- La solución debe permitir extraer reportes forenses para analizar ataques, los métodos y tendencias.

- La solución debe permitir escoger los criterios para generar el reporte forense, con al menos:

Categoría de la amenaza

Nombre del ataque.

Tasa del ataque en bps y pps.

IP Origen / IP Destino.

Duración del Ataque.

- La solución debe incluir un módulo de alertas que permita definir el impacto y severidad de cada alerta creada y que permita enviarlas via e-mail.
- El alcance de las alertas generadas debe ser por políticas, permitiendo configurar una o varias políticas por alerta.
- La solución debe permitir escoger los criterios para generar el reporte forense, con al menos:
Categoría de la amenaza
Nombre del ataque.
Tasa del ataque en bps y pps.
IP Origen / IP Destino.
Duración del Ataque.
Riesgo.

SERVICIOS POSTVENTA
El contratista deberá realizar sesiones periódicas con el fin de validar el correcto funcionamiento del producto contratado y realizar sugerencias de mejoras
El contratista deberá brindar soporte técnico para incidentes y requerimientos relacionados con el buen funcionamiento las suscripciones adquiridas.
El contratista deberá garantizar que se puedan escalar casos de soporte técnico a la casa fabricante de la solución durante toda la vigencia de la suscripción de la solución contratada.
El fabricante debe permitir la apertura de casos por medio del su portal de contacto, chat o vía telefónica.

 T1. HERNANDEZ HERNANDEZ LUSBIN Comité Estructurador Técnico	 MY. LUIS MAURICIO LEON PINZON Gerente del Proyecto
--	---

GLOSARIO DE TÉRMINOS

AntiDDoS: Solución tecnológica orientada a la detección, mitigación y prevención de ataques de denegación de servicio distribuido.

DDoS (Distributed Denial of Service): Tipo de ataque que busca afectar la disponibilidad de un servicio mediante el envío masivo de tráfico desde múltiples fuentes.

Throughput: Capacidad máxima de procesamiento de tráfico que puede manejar un sistema, generalmente expresada en Gbps.

PPS (Packets Per Second): Métrica que indica la cantidad de paquetes que un dispositivo puede procesar por segundo.

Latencia: Tiempo que tarda un paquete de datos en atravesar un sistema o red.

Bypass: Mecanismo que permite el paso del tráfico en caso de falla del equipo, evitando la interrupción del servicio.

Modo Transparente (Capa 2): Forma de operación en la cual el equipo se integra sin modificar direcciones IP, actuando como un puente.

Política de Seguridad: Conjunto de reglas configuradas para la detección y mitigación de tráfico malicioso.

Rate Limit: Mecanismo que permite limitar la cantidad de tráfico permitido en un periodo de tiempo.

Firma de Ataque: Patrón de tráfico identificado como comportamiento malicioso utilizado para bloquear ataques.

Baseline (Línea Base): Comportamiento normal del tráfico de red utilizado como referencia para detectar anomalías.

Burst Attack: Ataque de corta duración, pero alta intensidad.

Top Talkers: Identificación de las direcciones IP que generan mayor volumen de tráfico.

ASN (Autonomous System Number): Identificador único asignado a una red en Internet.

Geo-localización: Técnica que permite identificar el origen geográfico de una dirección IP

PCAP: Archivo que contiene capturas de tráfico de red para análisis forense.

QPS (Queries Per Second): Métrica utilizada para medir consultas por segundo, comúnmente en servicios DNS.

Lista Blanca (Allow List): Conjunto de direcciones o entidades permitidas.

Lista Negra (Block List): Conjunto de direcciones o entidades bloqueadas

Overblocking: Bloqueo excesivo de tráfico legítimo durante la mitigación de ataques.