

	FICHA TÉCNICA FORTALECIMIENTO INFRAESTRUCTURA COMPOSABLE, HIPERCONVERGENTE Y ANÁLISIS TRANSACCIONAL
---	--

ANEXO No. 2. FICHA TECNICA - ESPECIFICACIONES TÉCNICAS MÍNIMAS

IDENTIFICACIÓN DE LOS BIENES Y SERVICIOS REQUERIDOS

OBJETO:

CONTRATAR LA RENOVACIÓN DEL SOPORTE Y MANTENIMIENTO DE LA PLATAFORMA HPE (SYNERGY Y SIMPLIVITY) Y DEL SERVICIO DE ANÁLISIS TRANSACCIONAL NDR DE LA PROCURADURÍA GENERAL DE LA NACIÓN.

ESPECIFICACIONES TÉCNICAS MÍNIMAS

El proponente debe comprometerse a entregar el soporte y demás servicios adquiridos y atender los requerimientos de soporte técnico tal y como se describe en las tablas siguientes, indicando para ello en la carta de presentación de la oferta que acepta, conoce y se obliga con su firma a entregar los productos y cumplir con las características de los servicios y soporte técnico según se discrimina a continuación. **Los costos que tengan estas actividades deben estar previstos en la oferta y no generarán costo adicional para la PGN.**

La entidad requiere la renovación del soporte y el fortalecimiento de la plataforma de cómputo e hiperconvergencia, los cuales se describen a continuación:

Descripción	Modelo	Serial
Servidor infraestructura de virtualización	HPE Synergy 480 Gen 10 Compute Module	MXQ01909JX
Servidor infraestructura de virtualización	HPE Synergy 480 Gen 10 Compute Module	MXQ01909JY
Servidor infraestructura de virtualización	HPE Synergy 480 Gen 10 Compute Module	MXQ01909JZ
Servidor infraestructura de virtualización	HPE Synergy 480 Gen 10 Compute Module	MXQ01909K0
Servidor infraestructura de virtualización	HPE Synergy 480 Gen 10 Compute Module	MXQ01909K1
Servidor infraestructura de virtualización	HPE Synergy 480 Gen 10 Compute Module	MXQ01909K2
Servidor infraestructura de virtualización	HPE Synergy 480 Gen 10 Compute Module	MXQ01909K3
Servidor infraestructura de virtualización	HPE Synergy 480 Gen 10 Compute Module	MXQ01909K4
Servidor infraestructura de virtualización	HPE Synergy 480 Gen 10 Compute Module	MXQ01909K5
Servidor SO Bare Metal, Tipo 1	HPE Synergy 480 Gen 10 Compute Module	MXQ01906M7
Servidor SO Bare Metal, Tipo 1	HPE Synergy 480 Gen 10 Compute Module	MXQ01906M8



FICHA TÉCNICA FORTALECIMIENTO INFRAESTRUCTURA COMPOSABLE, HIPERCONVERGENTE Y ANÁLISIS TRANSACCIONAL

Servidor SO Bare Metal, Tipo 2	HPE Synergy 480 Gen 10 Compute Module	MXQ01906M5
Servidor SO Bare Metal, Tipo 2	HPE Synergy 480 Gen 10 Compute Module	MXQ01906M6
Enclosure para servidores	HPE Synergy 12000 Frame	MXQ020073X
Enclosure para servidores	HPE Synergy 12000 Frame	MXQ020073Y
Nodos de hiperconvergencia	HPE ProLiant DL360 Gen 10 Server	2M20170J7V
Nodos de hiperconvergencia	HPE ProLiant DL360 Gen 10 Server	2M20170J7W
Nodos de hiperconvergencia	HPE ProLiant DL360 Gen 10 Server	2M20170J85
Nodos de hiperconvergencia	HPE ProLiant DL360 Gen 10 Server	2M20170J7T

Nota 1: Los servicios de soporte de la plataforma descrita debe ser hasta el 24 de junio de 2025 a partir del cumplimiento de los requisitos de perfeccionamiento del contrato. Ahora bien, si como de ello.

Nota 2: El contratista deberá entregar dentro de los 15 días calendario después del cumplimiento de los requisitos de perfeccionamiento del contrato el documento que certifique que la entidad beneficiaria de la renovación del soporte de la Infraestructura Composable e Hiperconvergente.

Opciones para apertura de casos	<ul style="list-style-type: none">➤ Virtual: A través de un sitio web del contratista o del fabricante.➤ Automática: Los equipos conectados con esta opción deberán poder registrar incidentes automáticamente 24*7.➤ Telefónica: A través de una línea telefónica suministrada por el contratista o fabricante.
Actualizaciones	<p>El contratista debe ofrecer un esquema de acceso a las actualizaciones de software disponibles para los productos</p> <p>Se debe realizar la(s) actualización(es) de software durante la vigencia de la garantía en la plataforma del fabricante a la última versión disponible y estable relacionada en el objeto del contrato, para mejorar la funcionalidad de la seguridad, cada vez que se requiera.</p> <p>El alcance debe cubrir las actualizaciones menores (updates), mayores (upgrades) y prestar el apoyo para su instalación o configuración.</p>
	El contratista o fabricante debe contar con atención telefónica para prestar el servicio de soporte y este debe incluir atención de incidentes y consultas

	FICHA TÉCNICA FORTALECIMIENTO INFRAESTRUCTURA COMPOSABLE, HIPERCONVERGENTE Y ANÁLISIS TRANSACCIONAL
---	--

Niveles de Servicio	a través de llamadas telefónicas, correo electrónico, sesiones remotas y atención en sitio en horario Hábil y No Hábil.
	El contratista deberá contar con un software de Mesa de Servicio, donde se puedan registrar casos o incidentes de forma web, correo o teléfono, y así realizar el seguimiento correspondiente.
Soporte en sitio y/o remoto	El contratista debe atender los requerimientos de soporte técnico en sitio y/o remoto durante el período de la vigencia del contrato, en la modalidad 7*24*365*4 (Siete días a la semana, veinticuatro horas al día durante 365 días del año), con cuatro (4) horas máximo de respuesta para los bienes, relacionados con componentes de software y/o firmware, configuración de servicios, software especializado, etc.)
Soporte Telefónico	Se debe garantizar acceso al centro de soporte telefónico durante el período de la garantía, en la modalidad 7*24*365*4 (Siete días a la semana, veinticuatro horas al día durante 365 días del año), con cuatro horas máximo de respuesta.

ANALISIS TRANSACCIONAL

La entidad actualmente cuenta con una solución implementada y en operación, razón por la cual, requiere la continuidad de dicha solución de análisis transaccional para la prevención, detección e Investigación de Ciber amenazas dentro de la red de la PGN:

Generalidades	Se requiere de un sistema modular que le permita a la entidad, detectar automáticamente e investigar riesgos o amenazas que puedan existir a lo largo de su infraestructura de red de TI. El sistema deberá basar su funcionamiento en la captura permanente y pasiva de los paquetes IP que fluyan a través de la red de producción, a partir de los cuales generará información analítica que permita ejecutar flujos de trabajo de investigación para la detección, identificación, validación y respuesta a potenciales ciber amenazas. No se aceptarán soluciones que dependan de la colección de logs o flujos (p.ej. NetFlow) desde elementos aplicativos o dispositivos de la red.
	Se requiere que la solución sea presentada bajo un modelo de licenciamiento por suscripción a un año, incluyendo acceso a soporte técnico 7x24.



FICHA TÉCNICA FORTALECIMIENTO INFRAESTRUCTURA COMPOSABLE, HIPERCONVERGENTE Y ANÁLISIS TRANSACCIONAL

	<p>Se requiere que la solución permita al menos las siguientes funcionalidades para cualquier servicio IP de la entidad:</p> <ul style="list-style-type: none">➤ Alertas tempranas, basadas en el análisis de tráfico de la red, para la detección de las primeras fases de un ataque.➤ Monitoreo continuo de la superficie de ataque: Proporcionar información consistente y en tiempo real de los cambios de comportamiento en la comunicación de red, tanto en su perímetro, como dentro de la red institucional.➤ Seguimiento de contactos: Identificación de todos los sistemas afectados por una amenaza o una posible infracción, analizando la interacción transaccional entre cada uno de ellos.➤ Investigación forense de las comunicaciones de red: Visibilidad retrospectiva de comunicaciones y sesiones de los distintos servicios IP de la entidad, para hacer investigación de la evolución de comunicaciones anómalas detectadas en el tráfico de red.
Captura y Análisis de Paquetes.	<p>La funcionalidad de captura, almacenamiento y análisis de paquetes IP en tiempo real, deberá contar con los siguientes elementos:</p> <ol style="list-style-type: none">1. La solución deberá tener la capacidad de capturar y analizar de manera continua los paquetes IP que fluyen por los switches virtuales definidos por la entidad, desde los cuales se configurará copia del tráfico relevante.2. La solución deberá contar con la capacidad de capturar y analizar el tráfico que fluye a través de switches virtuales en hipervisores, mediante la instalación de sondas virtuales sobre cada host físico, que realizarán la función de instrumentación del switch virtual.3. Se requiere la instalación de una sonda virtual, con capacidad de análisis de tráfico de hasta 1Gbps cada una.4. La solución se deberá implementar de manera pasiva, sin la instalación de agentes o recolección de logs.5. Las máquinas virtuales instaladas para la captura y análisis de tráfico de los switches virtuales se deben soportar para las siguientes versiones de hipervisores: VMware vSphere ESXi 7.0, 6.7, o 6.5.6. La solución deberá permitir escalabilidad a futuro para la decodificación y análisis de tráfico circulante por switches físicos o TAPS, mediante la implementación de appliances en hardware del mismo fabricante, especializados para tal fin.7. En caso de requerirse escalabilidad para decodificación y análisis de tráfico circulante por switches físicos o TAPS, la solución deberá poder incluir a futuro dispositivos de colección y administración de tráfico tipo packet broker del mismo fabricante (con funcionalidades de agregación, replicación,



FICHA TÉCNICA FORTALECIMIENTO INFRAESTRUCTURA COMPOSABLE, HIPERCONVERGENTE Y ANÁLISIS TRANSACCIONAL

	<p>filtrado y balanceo de tráfico definido por criterios de sesión, para optimización del tráfico a analizar). Estos dispositivos deben permitir conectarse a varios puertos espejo en los switches de la entidad que hayan sido configurados para entregar una copia del tráfico o a los dispositivos de copia pasiva tipo TAPs, y orquestar el flujo de tráfico hacia el componente que cumpla la función de captura y almacenamiento de paquetes, mediante funciones como agregación y filtrado.</p> <p>8. En caso de requerirse escalabilidad para decodificación y análisis de tráfico circulante por switches físicos o TAPS, la solución deberá permitir la inclusión de dispositivos de análisis y almacenamiento de paquetes tipo appliance del mismo fabricante, que permitan generar métricas de forma constante y en tiempo real, utilizando técnicas de inspección profunda de paquetes.</p>
	<p>Los dispositivos de captura y análisis de paquetes deberán cumplir al menos con las siguientes características:</p> <ul style="list-style-type: none">a) Tener la capacidad de captura de manera continua y pasiva los paquetes IP que fluyen por los switches virtuales definidos por la entidad.b) Deberá analizar los paquetes capturados para generar información analítica de seguridad.c) Deberá tener la capacidad de almacenar los paquetes capturados, permitiendo seleccionar los protocolos deseados, así como el tamaño de paquete a ser almacenado, así como poder capturar, indexar y almacenar paquetes para realizar actividades de análisis forense
Consola central para detección, prevención e investigación de amenazas en el tráfico de red.	<p>La información analítica generada por las sondas de captura de tráfico deberá ser colectada, almacenada y explotada en una consola central, accesible vía Web, donde estarán disponibles diferentes módulos de análisis y configuración de la solución.</p>
	<p>La comunicación entre esta consola y las sondas de captura y análisis de tráfico deberá hacerse vía HTTP, HTTPS o SNMP.</p>
	<p>Deberá incluir el licenciamiento de una fuente de información de ciber inteligencia propietaria, la cual inyecte indicadores de compromiso (IoCs) al sistema, permitiendo detectar tráfico hacia entidades maliciosas a partir de direcciones IP, dominios y/o URLs.</p>
	<p>Deberá soportar al menos las siguientes opciones de integración hacia herramientas de terceros, existentes en el stack de seguridad:</p>



FICHA TÉCNICA FORTALECIMIENTO INFRAESTRUCTURA COMPOSABLE, HIPERCONVERGENTE Y ANÁLISIS TRANSACCIONAL

- a) Integración con un servidor syslog para el envío de alertas en formato CEF de eventos detectados por la plataforma (Incluyendo campos que permitan la visibilidad de descripción de tipo de riesgo, categoría y severidad).
- b) Generación de URLs que habiliten el acceso a eventos dentro de la consola para su investigación.

Deberá soportar STIX/TAXII para la ingestión de indicadores de compromiso (IoCs) de terceros, que complementen la capacidad de detección de tráfico potencialmente malicioso.

Deberá soportar al menos autenticación Local, LDAP, RADIUS, TACACS, Windows domain, SAML.

Deberá contar con un panel de alertamiento temprano, donde se puedan visualizar las potenciales amenazas detectadas en el ambiente de red bajo diferentes grupos:

- a) Riesgos de Seguridad – Se deberán detectar situaciones no deseadas o protocolos/aplicaciones que representen una vulnerabilidad dentro de las comunicaciones de tráfico de red: Expiración de certificados, Versiones SSL/TLS débiles, Comunicación con Servidores DNS Externos, Tráficos SMBv1, Telnet, Rlogin, Ciphers débiles, certificados autofirmados, etc.
- b) Indicadores de Amenazas – Se deberán detectar eventos que se generen ante la existencia de tráfico que supera las líneas base de aprendizaje automático de la solución y umbrales predefinidos, consecuencia de ataques DDoS de Capa Aplicativa (Inundación HTTP, Inundación DNS), Agotamiento de Tablas de Estado (TCP SYN, Nuevas Sesiones, Tiempo de Conexión) o Volumétricos (Amplificación Chargen, Amplificación DNS, ICMP, Banderas TCP Invalidas, Fragmentación IP, L2TP, mDNS, Amplificación MS SQL RS, NetBIOS, Amplificación NTP, Rpcbind, Amplificación SNMP, Amplificación SSDP, Amplificación TCP SYN/ACK, PCR)
- c) Ciber Amenazas – Permitirá detectar tráfico malicioso basado en indicadores de compromiso (IoCs) a partir de todas las conversaciones IP analizadas por los dispositivos de captura.
- d) Cambios en la Superficie de Ataque – Deberá mostrar cambios de comportamientos en los tráficos analizados, donde se muestre si hay nuevas conexiones con países, protocolos y aplicaciones de forma proactiva y basado en baselines automáticos construidos por la solución.

La solución deberá permitir el definir grupos de protección conformado por servidores críticos, que cumplan una misma función para darles seguimiento de manera detallada antes riesgos de seguridad y amenazas.



FICHA TÉCNICA FORTALECIMIENTO INFRAESTRUCTURA COMPOSABLE, HIPERCONVERGENTE Y ANÁLISIS TRANSACCIONAL

Deberá contar con un módulo de análisis de tráfico que permita analizar los eventos de seguridad detectados, representando gráficamente los patrones de tráfico de cada uno de los puntos de captura a manera de tasa de tráfico, tasa de paquetes, volumen de datos, cantidad de paquetes y porcentaje de utilización.

Para cada uno de los puntos de captura analizados, el sistema deberá agrupar las estadísticas en función de al menos los siguientes elementos:

- Aplicaciones
- Grupos de Protección
- Servidores
- Host
- Conversaciones
- Riesgos
- Geolocalización

El sistema deberá tener la capacidad de asociar las direcciones IP Públicas detectadas de acuerdo con su Geolocalización.

El sistema deberá proveer un mecanismo para descubrir múltiples asociaciones de contenido para búsqueda de información. Las búsquedas al menos deberán ser a partir de Aplicaciones, Direcciones IP de Servidores y Clientes, Hosts, Subredes, Puertos TCP/UDP.

Deberá ofrecer un módulo de análisis de sesiones, al cual se pueda acceder desde los módulos de investigación entregando información detallada y contextualizada de sesiones particulares.

El módulo de sesiones deberá mostrar la trazabilidad de la sesión analizada entre el cliente y servidor, indicando los deltas de tiempo que existe entre cada transacción.

El sistema deberá incluir un módulo gráfico para la investigación de las conversaciones establecidas por un Host específico. La información resultante se deberá expresar a manera de matriz en donde se pueda observar la relación que dicho Host tuvo con el resto de los Hosts con quien estableció conversaciones IP para el intervalo de tiempo seleccionado y con capacidad de filtrar por tipo de aplicación, tipo de riesgo, indicadores de amenazas y conversaciones en específico.



FICHA TÉCNICA FORTALECIMIENTO INFRAESTRUCTURA COMPOSABLE, HIPERCONVERGENTE Y ANÁLISIS TRANSACCIONAL

Al posicionarse sobre cualquier Hosts en la matriz, deberá presentarse información relativa a dicha conversación tales como: Dirección IP, Geolocalización, Aplicación, Volumen de Tráfico, Porcentaje de Fallas y Grupo de Protección.

Para cada Host detectado, deberá ofrecer una función que permita expandir la representación de las conversaciones establecidas por ese Host. Esta función deberá ofrecer una profundidad de hasta cuatro niveles.

Deberá incluir un módulo para el análisis de paquetes que permita acceder a aquellos almacenados en los dispositivos de captura. Su acceso deberá ser directo o bajo el contexto en tiempo o de aplicación o hosts generado a través de cualquier otro módulo. Y al menos deberá tener las siguientes características:

- a) Deberá permitir decodificar los paquetes en el mismo GUI y presentarlos en un formato de Analizador de Protocolos Estándar.
- b) Exportar los paquetes en formato pcap.
- c) Generar capturas de paquetes en tiempo real bajo demanda.
- d) Para el análisis detallado de los paquetes, se deberá incluir un constructor de filtros que permita el aislamiento de información específica con un enfoque pre y post captura.

El módulo de análisis de paquetes debe permitir la visualización de los paquetes IP asociados a cada sesión, para labores forenses. Si los paquetes están encriptados, debe tener la capacidad de hacer decodificación de paquetes encriptados IPSec, utilizando las llaves de encriptación y autenticación.

Deberá soportar integración con un módulo especializado para descifrado de tráfico del mismo fabricante, que permita la visibilidad a nivel de capa 7 para tráfico encriptado, el cual debe tener la capacidad de ser desplegado en modo fuera de banda o en línea, así como soportar cifrado y descifrado SSL/TLS y SSH, y llaves de cifrado estáticas y efímeras, simétricas y asimétricas.

La solución deberá tener un módulo de reporte que permita la generación de reportes basado en el análisis de tráfico, al menos para:

- a. Análisis de Ciber Amenazas
- b. Análisis de Riesgos de Seguridad
- c. Análisis de Indicadores de Amenazas
- d. Análisis de Tráfico



FICHA TÉCNICA FORTALECIMIENTO INFRAESTRUCTURA COMPOSABLE, HIPERCONVERGENTE Y ANÁLISIS TRANSACCIONAL

	Los reportes deberán generarse de manera calendarizada con una frecuencia de al menos por hora, día y semana.
	El módulo de reporte permitirá enviar los reportes vía correo electrónico a diferentes destinos, donde el reporte podrá ser adjuntando como un archivo en PDF, Texto o una URL.
Otras condiciones	El contratista deberá garantizar la continuidad del servicio con el que cuenta la entidad actualmente desde el inicio y hasta el 24 de junio de 2025. Ahora bien, si como producto del proceso de subasta se obtiene remanentes en recursos que posibilite la extensión del servicio, el contratista deberá garantizarlo hasta el agotamiento de ello.
	Al finalizar el servicio, el contratista deberá entregar los archivos de configuración de la solución a la entidad.