ANEXO No. 1 FICHA TÉCNICA

Grupo 1 - Ítem 1 Firewall tipo Appliance	
DESCRIPCION	**Appliance de red y seguridad informática perimetral e interna.**
CANTIDAD	Dos (2)
ATRIBUTO	**Especificaciones mínimas requeridas**
Tecnología	Next Generations Firewall
Rendimiento y Capacidad	Todas las características y funciones deben ser activadas con su respectivo licenciamiento. • Rendimiento de mínimo 14 Gbps, después de tener todas las funciones activas. • Rendimiento prevención de amenazas de mínimo 7.4 Gbps. • Rendimiento VPN IPSec de mínimo 6.5 Gbps. • Módulo de IPS mínimo de 7.5 Gbps. • Sesiones simultaneas concurrentes de mínimo 1´400.000 millones. • Soporte de nuevas sesiones por segundo mínimo 142.000. • Capacidad de etiquetas VLAN 802.1Q por equipo/interfaz: 4,094 • Capacidad de virtualización de router de mínimo 10 instancias.
Conectividad	• Mínimo 10 interfaces de red 1G en cobre. • Mínimo 4 interfaces de red ópticas 10G SFP/SFP+ para el tráfico de datos de la red. • Mínimo 2 interfaces de red ópticas 25G para el tráfico de datos de la red. • La plataforma deberá contar con al menos una interface adicional RJ45 de 10/100/1000 o interfaces SFP+ de 10 Gbps dedicadas a la sincronización de estado y configuración dentro del clúster de alta disponibilidad.
Traducción de direcciones de red	• NAT modos (IPv4): estático IP, dinámico IP. • NAT64, NPTv6. • Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2). • Soportar como mínimo las siguientes funcionalidades en IPv6: SLAAC (address auto configuration), NAT64, Identificación de usuarios a partir de LDAP/AD, IPv6 over IPv4 IPSec, Reglas o políticas de seguridad contra DoS, Descifrado SSL/TLS y SSH, PBR (Policy Base Routing) o PBF (Policy Based Forwarding), OSPFv3, QoS, DHCPv6 Relay, SNMP, NTP, NTP autenticado, SYSLOG, DNS y control de aplicaciones. • Soportar DNS Dinámico en las interfaces de red del equipo de seguridad. • Capacidad de inspeccionar el contenido en túneles GRE, GPRS, VXLAN e IPSec no cifrado.
Funcionalidades	• Permitir la creación de clusters de más de dos dispositivos para la sincronización de sesiones. • Permitir el control de políticas por zonas, puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, aplicaciones grupos estáticos de aplicaciones o grupos dinámicos de aplicaciones (basados en características y comportamiento de las aplicaciones) y categorías de aplicaciones. • Permitir especificar en las reglas de seguridad un grupo de objetos basados en IP y/o URL que se alimenten dinámicamente de una fuente externa. • Permitir agrupar las políticas de seguridad utilizando etiquetas u otro método. • Permitir añadir un comentario de auditoría cada vez que se cree o se edite la política de seguridad. • Validación de la configuración antes de ser aplicada o instalada e identificar y notificar cuando existan reglas generales superpuestas sobre otras específicas (shadowed rules).

ANEXO No. 1 FICHA TÉCNICA

Grupo 1 - Ítem 1 Firewall tipo Appliance	
Conexiones remotas seguras (VPN)	• La VPN IPSec debe soportar como mínimo: ➢ DES y 3DES; AES 128, 192 e 256 (Advanced Encryption Standard). ➢ Autenticación MD5, SHA-1, SHA-2. ➢ Diffie-Hellman Group 1, Group 2, Group 5 y Group 14. ➢ Algoritmo Internet Key Exchange (IKEv1 & IKEv2); • Soportar VPN Site-to-Site y Cliente-To-Site en protocolos IPSec o SSL. • Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de las VPN. • Las VPN client-to-site deben operar usando el protocolo IPSec o SSL y permitir la conexión por medio de agente o sin agente instalado en el sistema operativo y soportar una cantidad mínima de 1600 usuarios concurrentes. • Permitir crear políticas de control de aplicaciones, IPS, Antivirus, Antispyware para tráfico de los clientes remotos conectados en la VPN client-to-site. • Soportar autenticación vía AD/LDAP, Kerberos, TACACS+, SAML y RADIUS, incluyendo Doble Factor de Autenticación (2FA). • Debe asignar una IP a cada cliente que se conecte a la VPN en formato IPv4 e IPv6, de forma automática mediante un pool de IP. • Debe permitir monitorear a los usuarios conectados por VPN. • Permitir colocar en cuarentena equipos con actividad maliciosa identificada. • Permitir bloquear el acceso a la red, a los equipos colocados en cuarentena. • Permitir la configuración de políticas de seguridad de VPN basado en las características del equipo, recopilando entre otras las siguientes características: sistema operativo, dominio de red, versión de parche, software antivirus, software DLP y software de cifrado de disco. De tal forma que si el equipo no cumple cierta condición basado en esas características (Perfilamiento y Postura), no permita el acceso a la VPN o le otorgue acceso de mayores restricciones.
Descifrado de tráfico SSL/TLS	• Debe mostrar a través de un filtro, las reglas de seguridad que no han tenido uso en la red. • Debe permitir descifrar el tráfico de navegación de usuarios a internet mediante la instalación de un certificado digital en los equipos. • Debe permitir descifrar el tráfico entrante hacia servidores HTTPS publicados en internet importando el certificado del servidor en el Firewall. • Debe identificar y notificar al cliente si está visitando una página web con certificado digital no válido o emisor no confiable, a pesar de no aplicar descifrado al tráfico SSL/TLS. • Debe soportar certificados que utilice Subject Alternative Name (SAN) y Server Name Indication (SNI). • Debe permitir excluir sitios a los cuales no se les aplicará la política de descifrado, identificados por dominios y wildcards. • Capacidad de poder hacer decifrado TLS v1.1, v1.2 y v1.3
Identificación y contról de aplicaciones	• Debe procesar e inspeccionar aplicaciones que utilicen HTTP/2 • Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis de comportamiento del tráfico observado. • La aplicación de políticas de seguridad debe tener la posibilidad de aplicar reglas específicas a cada aplicación.
Protección ante ataques de denegación de servicio (DoS)	• Deberá permitir configurar límites o umbrales, contra ataques de denegación de servicios como syn flood, escaneo de puertos, inundación udp, inundación icmp, entre otros. • Debe identificar y bloquear ataques de escaneo de puertos TCP, UDP y Host Sweep.

ANEXO No. 1 FICHA TÉCNICA

Grupo 1 - Ítem 1 Firewall tipo Appliance	
	• Permitir definir una lista de excepciones basadas en direcciones IP, a los cuales no se le aplicarán la protección. • Debe proteger contra ataques basado en paquetes IP, como mínimo IP Spoofing, Paquetes Fragmentados, Strict Source Routing, Loose Source Routing, Record Route. • Debe proteger contra ataques basado en paquetes TCP, como mínimo Split Handshake, paquetes TCP SYN y TCP SYN/ACK con datos contenidos durante el handshake, Validación del Three Handshake. • Debe proteger contra ataques basado en paquetes ICMP, como mínimo paquetes con Ping ID 0, paquetes ICMP fragmentados, paquetes ICMP extensos • Debe proteger contra ataques basado en paquetes IPv6 e ICMPv6 • Debe contar con un mecanismo que proteja contra la saturación del buffer de paquetes por cada interfaz de datos de la solución • Debe permitir limitar un número máximo de sesiones que podrán ser generadas hacia un equipo destino, con la finalidad de evitar la saturación de sesiones hacia un equipo protegido. • Debe permitir reglas de prevención contra ataques DoS.
Prevención de amenazas	• Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS (Intrusion Prevention System), Antivirus (Antimalware de red), Antispyware/Antibot. • Capacidad de realizar DNS Sinkhole para la identificación de equipos comprometidos por Spyware en entornos corporativos. • La solución debe ser capaz de identificar decenas de millones de dominios maliciosos con análisis en tiempo real sin depender de firmas estáticas. • Debe clasificar los dominios maliciosos en categorias como: malware, DNS tunneling, Comando y Control, DNS dinamicos, phising o dominios recientemente registrados. • Las funcionalidades de IPS, Antivirus y Antispyware/Antibot deben operar en carácter permanente. • El equipo deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS, Antivirus y Antispyware/Antibot. • Debe soportar políticas de IPS, Antivirus y Antispyware/Antibot, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio, usuario y grupo de usuarios y la combinación de ítems. • Debe permitir capturar el paquete de red (en formato PCAP) asociada a la alerta de seguridad. • Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica dLa solución. • Permitir el bloqueo de virus y spyware en, por lo menos, los siguientes protocolos: HTTP, HTTP/2, HTTPS, FTP, SMB (versiones 1,2 y 3), SMTP, IMAP y POP3. Deberá tener cobertura tanto en IPv4 como en IPv6 para los protocolos en mención • Previene ataques utilizando Inteligencia de amenazas global. • Protección contra cargas ocultas en tipos de archivos comunes, como documentos de Microsoft® Office y PDF. • Debe permitir la detección de amenazas en tiempo real para detectar y bloquear exploits, malware, detectar navegación web peligrosa y amenazas desconocidas.
Proteccion avanzada de DNS	• La solución ofertada debe permitir realizar tareas de gestión a través del API basado en XML. • Integración con servicios de inteligencia global para identificar dominios maliciosos con análisis en tiempo real sin depender de firmas estáticas. • La solución debe ser capaz de predecir y detener dominios maliciosos de malware. • Debe utilizar machine learning y/o inteligencia artificial para detectar nuevos dominios.

ANEXO No. 1 FICHA TÉCNICA

Grupo 1 - Ítem 1 Firewall tipo Appliance	
	• Debe poseer políticas para bloquear dominios DGA o interrumpir las consultar de DNS a dichos dominios. • Debe poder clasificar los dominios maliciosos en categorías como: malware, DGA, DNS tunneling, Comando y Control, DNS dinamicos, phising o dominios recientemente registrados. • La solución debe obtener el historial y reputación de cada dominio (Opcional). • Debe brindar analítica de consultas DNS.
Análisis de malware de día cero (Sandboxing)	• Debe proteger la red de amenazas comunes y amenazas persistentes avanzadas (APT) • Debe contar con un mecanismo interno basado en ML que permita detectar el malware de día cero que se propaga por la red en tiempo real y sin depender de firmas de antivirus. • Debe incluir la detección de amenazas de día cero complejas a través de una integración con una plataforma Sandboxing. • Debe poder acceder y descargar protecciones contra malware de día 0 en tiempo real. • La plataforma de Sandboxing podrá ser ofrecido en Nube (Cloud) y/o On-premise. • Soportar el análisis de archivos maliciosos en ambiente controlado como mínimo en sistemas operacionales Windows. • Debe analizar Links/URLs para determinar si es o no malicioso. • Debe proveer información forense sobre las acciones realizadas por el malware y generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware. • Deberá soportar el análisis de archivos ejecutables (EXE), DLLs, ELF (Linux), archivos comprimidos (ZIP, 7ZIP, RAR) archivos office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar e class), archivos de tipos script (.vbs, .ps1, .js), email link, flash, archivos de MacOSX (mach-o, dmg, pkg) y Android APKs en el ambiente controlado. • La solución ofertada debe ser capaz de enviar al sandbox de manera automática, los archivos sospechosos que se propaguen por los protocolos HTTP, HTTPS, HTTP/2, FTP, SMTP, POP3, IMAP y SMB (versiones 1, 2 y 3 o superiores). Tanto en IPv4 como en IPv6. • Debe permitir al administrador la descarga del archivo original analizado por el Sandbox. • Debe permitir reportar al fabricante eventos que son falso-positivo y falso-negativo en el análisis de malware de día cero a partir de la propia consola de administración. • Permitir la subida de archivos al sandbox de forma manual y vía API.
Filtro de contenido Web	• Permitir especificar la política por tiempo, horario o determinado período (día, mes, año, día de la semana y hora) • Deberá incluir la capacidad de creación de políticas basadas en la visibilidad e identificar el usuario que accede a una URL a través de la integración con servicios de directorio, autenticación vía LDAP, Active Directory, e-Directory y base de datos local. • Debe soportar un cache local de URLs en el appliance, evitando el delay de comunicación/validación de las URLs • Debe poseer categorías de URLs, incluyendo las demalware y phishing. • Debe identificar y categorizar los dominios nuevos. • Debe permitir personalizar la página de bloqueo.
Identificación de usuarios	• Debe permitir notificar al usuario, mostrándole solo una página de alerta, pero permitiéndole continuar la navegación al site. • Debe incluir a capacidad de creación de políticas basadas en la visibilidad y control de usuarios y/o grupos de usuarios a través de la integración de servicios de autenticación vía LDAP, Active Directory, Exchange y base de datos local.

ANEXO No. 1 FICHA TÉCNICA

Grupo 1 - Ítem 1 Firewall tipo Appliance	
	• Debe poseer integración con Microsoft AD Domain Controller para la identificación de direcciones IP y usuarios. • Debe soportar la recepción de eventos de autenticación de controladoras Wireless, dispositivos 802.1x, soluciones NAC, soluciones proxy. • Debe permitir la definición de grupos dinámicos de usuarios. • Debe de permitir la identificación de los usuarios de la red utilizando una variedad de métodos de acceso y sistemas operativos, incluidos Microsoft Windows, Apple iOS, Mac OS, Android y Linux / UNIX.
Filtrado de datos	• Debe leer las direcciones IPv4 o IPv6 de los usuarios desde el encabezado X-Forwarded-For (XFF) en las solicitudes del cliente HTTP cuando el firewall se implementa entre Internet y un servidor proxy que de otro modo ocultaría las direcciones IP del usuario. • Los archivos deben ser identificados por extensión y firmas.
Alta disponibilidad	• La solución debe permitir ser configurada en modo Activo / activo y Activo / pasivo • Debe soportar IPv6 en modos de alta disponibilidad. • Debe ser capaz de operar en los modos Capa 3 (con capacidades completas de Ruteo y NAT), Capa 2, Transparente y Sniffer, de forma simultánea mediante el uso de sus interfaces físicas sin necesidad de tener que hacer uso de contextos o dominios virtuales. • Debe sincronizar: Sesiones, Certificados de descifrado, Configuraciones, políticas de Firewall, NAT, QoS y objetos de red. • Debe permitir el monitoreo de fallo de enlaces o pérdida de conectividad hacia una IP desde una de las interfaces. • La solución no puede ofertase con configuración de dispositivos o software externos a la configuración nativa soportada por el fabricante. • Se deben tener interfaces dedicadas para la alta disponibilidad y ser independiente de las interfaces de tráfico.
Gestión centralizada	• Se debe contar con una consola de gestión centralizada (tipo Appliance o virtual), que permita entre otros: Configurar de forma sincronizada ambos firewalls, mantener un registro de eventos escalable, almacenamiento propio para record de eventos, generar reportes y consultas por diferentes parámetros, así mismo soporte el manejo a copias de respaldo y gestione las actualizaciones de la plataforma. • Debe permitir establecer VPN's cliente a sitio con agente debe permanecer funcional para equipos windows y Mac aún con el vencimiento del licenciamiento y soporte. • Deberá tener una capacidad mínima de 1 TB utilizables. • Debe contar con fuentes de energía redundantes. • Debe tener al menos 2 interfaces 10/100/1000 RJ45 • El equipo debe mostrar por medio de su interfaz información sobre los equipos que administra con respecto a su rendimiento (CPU, memoria y desempeño), logs, información ambiental (como ventiladores y fuentes de alimentación) y correlacionar eventos (como cambios de configuración, instalaciones de contenido y actualizaciones de software) con datos de salud. • Debe permitir la visualización de los logs del tráfico de red, tráfico malicioso, envíos de archivos al sandbox, filtro web y eventos de sistema • Debe permitir la visualización de los logs de con información del Usuario y Dirección IP asignada. • Debe permitir la generación de logs de auditoria detallados, informando de la configuración realizada, el administrador que la realizo, su IP y el horario de la alteración

ANEXO No. 1 FICHA TÉCNICA

Grupo 1 - Ítem 1 Firewall tipo Appliance	
	• Debe ser capaz de enviar los logs vía SNMP Trap, Correo Electrónico, Syslog y HTTP (vía API) • Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de antivirus, antispyware, IPS, navegación a internet, aplicaciones, malware de día cero, debe permitir seleccionar columnas a mostrar, filtrar la información en base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico. • Debe permitir el control de acceso a la gestión del equipo a través de roles personalizables. • La autenticación deberá estar disponible localmente o integrado con plataformas SAML, Kerberos, RADIUS, TACACS+ y LDAP • Debe permitir comparar e indicar los cambios efectuados a una política de seguridad respecto a una versión anterior de dicha política. • Debe permitir el respaldo o backup de la configuración.y rollback de la última configuración estable.
Almacenamiento	Disco (de estado sólido) interno mínimo 480 GB o superior.
Alimentación eléctrica	Fuente de poder redundante.
Soporte y garantía	• Tres (3) años para todos los componentes, con el servicio de garantía más alto ofrecido por el fabricante y atención y soporte 7x24x4, incluyendo todos los repuestos necesarios originales de fábrica. La garantía deber ser certificada por parte del fabricante. • Se solicita como mínimo un (1) mantenimiento preventivo por cada año de garantía, realizado por personal certificado por el fabricante de los productos. • El contratista debe estar certificado en mejores prácticas de seguridad de la información ISO27001:2013 o superior. • Con el fin de garantizar el correcto uso y apropiación de las buenas prácticas dadas por el fabricante, el proponente cargara junto con la propuesta, una certificación que lo acredite como partner de la marca. Este documento deberá ser expedido por el fabricante con fecha no mayor a treinta (30) días calendario anteriores a la fecha del cierre del presente proceso de selección.
Personal	Asignar personal especializado en la instalación, configuración y puesta en funcionamiento de la solución ofertada y para ellos deberá demostrar: • Certificación emitida por el fabricante de los productos que detalle la idoneidad en la manipulación de los productos ofertados. • Certificaciones que demuestren experiencia mínima de tres (3) años en instalación configuración y puesta en funcionamiento de los productos ofertados. • Certificación mínima en CEH (Certified Ethical Hacker) o CCSP (Certified Cyber Security Professional) o CISM (Certified Information Security Manager) o CISSP (Certified Information Systems Security Professional) o CHFI - Computer Hacking Forensic Investigator • Certificado Auditor interno en sistema de gestión de seguridad en la información ISO 27001:2013 o superior o Especialista en seguridad informática o seguridad de la información.
Instalación	Todos los equipos y componentes de la solución ofrecida deben ser entregados e instalados en la sede central del Ministerio de Salud, ubicado en la Cra. 13 No. 32 76, piso 21

ANEXO No. 1 FICHA TÉCNICA

Grupo 1 - Ítem 1 Firewall tipo Appliance	
	Todos los licenciamientos que se requerida para activar o poner en funcionamiento todas y cada una de las características y funcionalidades de los equipos, módulos y componentes, deberán suministrarse, sin costo adicional para el Ministerio.

Grupo 1 - Ítem 2 – Software Seguridad de dispositivos	
DESCRIPCION	**Licencias de uso de Software de protección de dispositivos.**
CANTIDAD:	**Ciento Sesenta (160)**
ATRIBUTO	**Especificaciones mínimas requeridas**
Características Generales	• Debe permitir la detección de técnicas de explotación sin necesidad de utilizar firmas, patrones o heurísticas, enfocadas principalmente en la prevención de exploits lógicos, procesos vulnerables y exploits del sistema operativo del fabricante Microsoft. Toda que esta es la plataforma base del Ministerio. • El agente de protección para dispositivos de punto final debe contar con integración nativa con el firewall que se oferte y se entregue como resultado de este mismo proceso contractual. • Contar con la funcionalidad de Mitigación de vulnerabilidades conocidas, desconocidas y de día cero. • Identificar técnicas de explotación de vulnerabilidades. • Proporcionar una protección, de memoria contra, mediante el uso de la herramienta de extracción de contraseñas. • Proteger aplicaciones contra las técnicas de explotación de manera predeterminada y "out-of-the-box". Entre las aplicaciones predeterminadas se encuentran: Firefox, Internet Explorer, Microsoft Word, Microsoft Excel, entre otras. • Permitir la utilización de los módulos de protección contra técnicas de explotación en cualquier aplicación o proceso. • Capacidad de crear un snapshot de forma automática de la memoria RAM al momento de prevenir la ejecución de una técnica de explotación. • El agente del software deberá ser capaz de enviar automáticamente el archivo detectado como sospechoso a un entorno de sandbox para ser emulado. • El sandbox deberá estar basado en nube o On-premise • El sandbox deberá soportar el análisis de 100 mil archivos por día. • El sandbox deberá tener capacidad de analizar archivos de hasta 100 MB de peso. • El software deberá garantizar la privacidad y seguridad del contenido de los archivos analizados. • Deberá tener la capacidad de realizar análisis de sandboxing como mínimo en sistemas Windows • Permitir configurar perfiles de protección en modo de prevención o monitoreo. • Permitir la prevención de técnicas de explotación. • Permitir la prevención de técnicas de explotación que buscan secuestrar el flujo de control de un proceso mediante el monitoreo de intentos de enumeración de la distribución de la memoria para sistemas operativos Linux. • Permitir la prevención de técnicas de explotación que buscan redireccionar los flujos de entrada y salida estándares a sockets de red para sistemas operativos Linux. • Permitir la prevención de técnicas de explotación que utilizan return-oriented programming para sistemas operativos Linux. • Permitir la protección contra la explotación de vulnerabilidades sin necesidad de tener una conexión a la consola.

ANEXO No. 1 FICHA TÉCNICA

Grupo 1 - Ítem 2 – Software Seguridad de dispositivos	
	• El agente a instalar en los dispositivos deberá tener soporte para las siguientes versiones de sistemas operativos: ➢ Windows 10 Pro, Windows 11 Pro o superior, Windows Server, 2012 R2 y 2016, 2019, 2022 o superior . ➢ macOS 12.X (Monterrey), macOS 13.X (Ventura), macOS 14 (Sonoma) o superior ➢ CentOS 6.7 (y superiores), CentOS 7, CentOS 7.9 (aarch64 running on AWS Graviton), CentOS 8 (aarch64 running on AWS Graviton), CentOS Stream 8, CentOS Stream 9,Red Hat Enterprise Linux 6 (6.7 y superiores), Red Hat Enterprise Linux 7, RHEL 8, RHEL 8 (aarch64 running on AWS Graviton), RHEL 9,Suse for Enterprise 12.1, Suse for Enterprise 12.2, Ubuntu Server 12, Ubuntu Server 14, Ubuntu Server 16 o superior. • El agente a instalar debe ser del mismo fabricante del firewall perimetral ofertado.
Tiempo de activación, soporte y actualizaciones	Para el software ofertado y todos sus componentes, se debe suministrar licenciamiento como mínimo en Suscripción por 3 Años o a perpetuidad según corresponda. En caso de que el licenciamiento que se requiera esté disponible en el mercado en la modalidad a perpetuidad, esta es la opción es que la se debe entregar somo parte de la solución, y la titularidad del licenciamiento deberá ser del Ministerio de salud y Protección Social.
Identificación de ataques post-explotación	• Permitir Identificar y prevenir intentos de escalación de privilegios a nivel de Kernel. Esta protección debe poder ser utilizada en agentes Windows, Mac y Linux. • Permitir la detección y terminación de comportamientos considerados como maliciosos mediante el análisis continuo de la cadena de eventos que sucedan en un endpoint. La detección debe utilizar varias reglas preconfiguradas, las cuales deben de tener la capacidad de analizar varios eventos y no sólo un evento. • La protección no deberá depender de una conexión a la consola de administración.
Prevención contra malware	• Generar hashes de procesos en ejecución y verificación en una nube de inteligencia de amenazas. • Envíar ejecutables cuando su hash es desconocido para su análisis en un sandbox ubicado en la nube o On-Premise, para sistemas operativos Windows, Mac, Linux y Android. • Prevenir contra shells reversos (reverse shell) para sistemas operativos Linux. • Generar los hashes de archivos ejecutables que estén almacenados en la computadora en una nube de inteligencia de amenazas. • Permitir enviar los archivos clasificados como maliciosos a cuarentena, ya sea que hayan sido identificados al momento de intentar ejecutarse o al momento de ser identificados mediante un escaneo. • Contar con un módulo de prevención con ransomware, generar una alerta y termina el proceso que está intentando llevar a cabo esas acciones. • Prevenir ejecución de procesos utilizando su hash, de manera que el administrador puede determinar qué aplicaciones pueden ser ejecutadas. • Identificar si la macro contenida en un documento de Word o Excel es maliciosa, sin necesidad de tener que ejecutar la macro ni observar su comportamiento o ejecución, para determinar si es maliciosa. • Proporcionar protección contra malware sin necesidad de contar con firmas, patrones y/o heurísticas. • Permitir configurar las políticas en modo de prevención o monitoreo. • Permitir poner los archivos detectados como maliciosos en una cuarentena, ya sea de manera automática o bajo demanda. • Utilizar características escaneo que no impacten negativamente en la experiencia del usuario por sobrecarga de recursos.

ANEXO No. 1 FICHA TÉCNICA

Grupo 1 - Ítem 2 – Software Seguridad de dispositivos	
Escaneo de archivos ejecutables	• Permitir realizar el escaneo de archivos ejecutables sin la necesidad de firmas. • Permitir programar el escaneo de archivos de manera semanal o mensual. • Permitir definir el día y la hora en la cual se iniciará el escaneo. • Permitir habilitar el escaneo de dispositivos de almacenamiento removible. • Permitir crear listas blancas de carpetas para que sean excluidas del proceso de escaneo. • Permitir poner en cuarentena los archivos identificados como maliciosos, si es que la política está configurada de esta manera.
Restricciones de ejecución	• Permitir restricciones de ejecución de archivos a partir de cierta carpeta. • Permitir restricciones de ejecución de archivos a partir de recursos compartidos. • Permitir restricciones de ejecución de archivos a partir de dispositivos USB o CD/DVD. • Permitir restricciones granulares de ejecución de procesos hijo definiendo el proceso padre y los procesos hijo a restringir o permitir. • Permitir restricciones granulares de ejecución de procesos hijo sin necesidad de contar con una conexión a la consola de administración. • Permitir configurar políticas de restricción de creación de procesos hijo configuradas de manera predeterminada. • Crear excepciones para permitir la ejecución de archivos a partir de ciertas carpetas. • Capacidad de crear excepciones para permitir la creación de procesos hijo. • Capacidad de crear excepciones para permitir la ejecución de archivos a partir de carpetas dentro de los dispositivos de almacenamiento removibles. • Permitir configurar perfiles en modo de prevención o monitoreo.
Restricción de uso de puertos USB.	• Permitir generar perfiles que gestionen el bloqueo de puertos USB cuando se conecten desde dispositivos externos • Permitir generar perfiles de excepciones para poder conectar dispositivos en puertos USB, permitir asignar permisos (lectura/escritura o sólo lectura). • Permitir la creación de políticas que utilicen los perfiles de bloqueo y de excepciones generados y sin ser excluyentes. • Permitir que las políticas generadas se puedan asignar a una computadora en particular o a un grupo de computadoras definido previamente. • Permitir la creación de excepciones permanentes utilizando dispositivos de conexión externos. Estas excepciones permanentes no deben de depender de ser aplicadas a una política para que surtan efecto. • Permitir la creación de excepciones temporales a partir de una violación registrada. • Mostrar las violaciones a las políticas que se hayan registrado con el siguiente detalle: hora, Dispositivo, usuario, dirección IP, tipo de dispositivo, producto, fabricante y número de serie del dispositivo que intentó conectarse. Esta funcionalidad deberá de estar soportada para sistemas operativos Windows y Mac.
Firewall de host	Las siguientes funcionalidades deberán de estar disponibles para sistemas operativos Windows: • Controlar todas las comunicaciones entrantes y salientes utilizando direcciones IP. • Configuración de reglas para ser aplicadas de acuerdo con la ubicación del dispositivo, por ejemplo, que sólo apliquen si están en la red interna. • Determinar, mediante la configuración, si el dispositivo se encuentra dentro o fuera de la organización. • Especificar direcciones locales o remotas, así como puertos locales o remotos. También se podrá especificar el protocolo dentro de estas cuatro opciones: ICMP, TCP, UDP, ICMPv6. Las siguientes funcionalidades deberán de estar disponibles para sistemas operativos Mac: • Permitir habilitar o deshabilitar el firewall nativo del sistema operativo.

ANEXO No. 1 FICHA TÉCNICA

Grupo 1 - Ítem 2 – Software Seguridad de dispositivos	
	• Permitir o bloquear las comunicaciones de red entrantes. • Habilitar el modo stealth • Crear exclusiones por aplicaciones para permitir o bloquear programas de manera específica y utilizando la funcionalidad del sistema operativo conocido como BlundleID.
Análisis de alertas e investigación de actividad sospechosa	• La solución deberá permitir la creación de una secuencia gráfica que correlacione las alertas individuales con el objetivo de describir la secuencia de un ataque. • Permitir hacer zoom in o zoom out para poder observar con mayor facilidad la secuencia mencionada anteriormente. • Mostrar una advertencia cuando un ejecutable en particular, que forme parte de la secuencia gráfica, tenga un comportamiento sospechoso. • Mostrar datos generales de la ejecución de un proceso que forme parte de la secuencia gráfica, entre los que se encuentran ruta de ejecución, nombre de usuario que ejecutó el proceso, tiempo de su ejecución, valor MD5 del ejecutable relacionado con el proceso, veredicto del análisis del sandbox, valor SHA256 y línea de comandos de la ejecución. • Mostrar la actividad de cada proceso identificado, en columnas y por categorías. Entre las categorías a incluir debe de estar la actividad de red, actividad de los archivos, actividad del registro, módulos ejecutados e intentos de inyección a procesos. • Para cada una de las funcionalidades relacionadas anteriormente, La solución deberá de desplegar los siguientes datos: fecha, nombre de la computadora, IP del host que generó la alerta, nombre de usuario, sistema operativo del host, tipo de actividad identificada, descripción de la actividad identificada, nombre del archivo asociado, nombre previo del archivo, ruta del archivo, ruta anterior del archivo, valor MD5 del archivo, valor SHA256 del archivo, ruta del archivo que fue el ejecutor del archivo, comando que utilizó el ejecutor del archivo, identificador del proceso que fue el ejecutor del archivo, valor MD5 del ejecutor del archivo que fue la causa raíz de la alerta, valor SHA256 del ejecutor del archivo que fue la causa raíz de la alerta, indicador sobre si el ejecutor de la alerta está firmado, comando del archivo que fue la causa raíz de la alerta, valor SHA 256 del archivo que fue la causa raíz de la alerta, indicador sobre si el archivo que fue la causa raíz de la alerta está firmado.
Telemetría y colección de eventos	• El agente deberá poder capturar, como mínimo, las siguientes acciones en equipos Windows: ➢ Proceso ejecutado, incluyendo el tiempo de inicio, el tamaño del archivo asociado. ➢ Actividades de creación, escritura, renombre, eliminación, modificación de archivos. ➢ Archivos DLL: ruta completa, dirección base, id del proceso, tamaño de la imagen, firma, valores hash calculados con los algoritmos MD5 y SHA256 del archivo DLL. ➢ Creación y terminación de los procesos, incluyendo los siguientes atributos: nombre del proceso padre, ID del proceso, ruta completa, argumentos de la línea de comando, nivel de integridad para determinar si el proceso está siendo ejecutado con privilegios elevados, valores hash calculados con los algoritmos MD5 y SHA256, detalles de la firma o el certificado utilizado para firmar el archivo. ➢ Inyecciones en hilos de procesos: ID del hilo padre, ID del hilo nuevo o que se ha terminado, proceso que inició el hilo (en caso de ser un proceso distinto). ➢ Interacciones de red de cada enpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP), resolución de dominio (hostname), tráfico entrante y saliente, país destino de la IP pública. ➢ Estadísticas de red: volumen de tráfico en eventos de subida y descarga de tráfico TCP. ➢ Acciones sobre los registros de Windows: Configuración o eliminación de valores del registro. Creación, modificación, eliminación, adición, restauración y guardar llaves

Grupo 1 - Ítem 2 – Software Seguridad de dispositivos	
	del registro. Con los siguientes parámetros: ruta del registro del valor o llave que fue modificado. Nombre del valor o llave modificado. Datos del valor modificado. ➢ Sesiones del sistema operativo: inicio de sesión, cierre de sesión, conexión y desconexión. Considerando los siguientes atributos: inicio de sesión interactivo, id de la sesión, estado de la sesión, y si la sesión es local o remota. ➢ Logs de eventos de Windows. • El agente deberá poder capturar, como mínimo, las siguientes acciones en equipos MacOS: ➢ Actividades de creación, escritura, renombre, eliminación, modificación de archivos. ➢ Inicio y detención de procesos, con los siguientes parámetros: PID de proceso del proceso padre, PID del proceso, ruta completa, argumentos de la línea de comando, nivel de integridad para determinar si el proceso está siendo ejecutado con privilegios elevados, valores hash calculados con los algoritmos MD5 y SHA256, detalles de la firma o el certificado utilizado para firmar el archivo. ➢ Interacciones de red de cada endpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP). ➢ Acciones de red: accept, connect, connect failure, disconnect, listen, statistics. ➢ Logs de eventos de autenticación. • El agente deberá poder capturar, como mínimo, las siguientes acciones en equipos Linux: ➢ Para los archivos: las acciones de creación, apertura, escritura y eliminación, incluyendo la ruta completa del archivo y el hash del archivo (para ciertos archivos y sólo si el archivo fue escrito). Información del copiado o renombrado de los archivos, incluyendo las rutas completas tanto del archivo original como del modificado. Las acciones para cambiar el dueño (chown) y el modo (chmod) de los archivos, incluyendo la ruta completa del archivo, así como el nuevo dueño o nuevos atributos. ➢ Inicio y detención de procesos, con los siguientes parámetros: PID de proceso del proceso padre, PID del proceso, ruta completa, argumentos de la línea de comando, nivel de integridad para determinar si el proceso está siendo ejecutado con privilegios elevados, valores hash calculados con los algoritmos MD5 y SHA256, detalles de la firma o el certificado utilizado para firmar el archivo. ➢ Interacciones de red de cada endpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP). ➢ Acciones de red: accept, connect, connect failure, disconnect, listen, statistics. ➢ Logs de eventos de autenticación. • Las búsquedas deberán estar disponibles tanto para endpoints en línea y fuera de línea. • Las búsquedas deberán de poder programarse para ser ejecutadas en un día y hora determinados durante una sola ocasión y también de manera recurrente. • Todas las opciones de búsqueda anteriormente detalladas deberán poder ser utilizadas para configurar reglas personalizadas de seguridad, que permitan generar una alerta cuando un endpoint en particular genere ese comportamiento. • La solución deberá de contar con un dashboard que permita visualizar alertas generadas de distintas fuentes. • El timeline del ataque deberá mostrar el intento de ataque en diferentes fases de explotación acorde al Framework MITRE ATT&CK, tales como Ejecución, Persistencia, Descubrimiento, Desplazamiento Lateral, Command & Control, Exfiltración. • La solución deberá permitir realizar búsquedas avanzadas sobre la actividad de los endpoints y toda la información de telemetría deberá enviarse de manera recurrente a la consola para su posterior procesamiento y almacenamiento: ➢ Actividad de red, identificando el tráfico saliente, entrante, IP origen e IP destino, Puerto origen y Puerto destino, protocolo de red.

Grupo 1 - Ítem 2 – Software Seguridad de dispositivos	
	➢ Actividad en el registro Windows, identificando la creación, eliminación, renombrado, definición de valores, eliminación de valores de las llaves de registro. ➢ Actividad de procesos, identificando si se trata de una ejecución o inyección, ruta desde donde se ejecuta, comando que inicializa el proceso, usuario, hash en SHA256 y MD5. ➢ Actividad en el Log de Eventos de Windows, identificando la descripción, ID del evento, nivel, mensaje, nombre del proveedor y usuario.
Gestión de Incidentes	• Deberá agrupar todas las alertas relacionadas a un incidente de seguridad de manera automática. • Por cada incidente mostrado deberá mostrar los elementos relacionados como ejecutables, hashes, direcciones IP. • Deberá mostrar los hosts y usuarios asociados al incidente. • Deberá ser posible asignar la revisión del incidente a un investigador con acceso a la consola, con el objetivo de llevar un orden sobre la atención de incidentes. • Capacidad de comentar los incidentes para detallar los avances realizados en la revisión. • Capacidad de clasificar el estado del incidente como abierto, en revisión, gestionado, cerrado, etc. • Capacidad de agrupar y desagrupar los incidentes de manera manual. • Capacidad de modificar la severidad del incidente de manera manual. • La consola deberá estar basada 100% en nube, con el objetivo de no depender ni administrar infraestructura física local. La nube del fabricante deberá contar con las siguientes características: * Contar con la certificación SOC2 Tipo II de AICPA, ISO 27001. * Contar con doble factor de autenticación para el login. * Permitir el acceso solo desde un rango de IP pública de la Entidad. • La consola debe permitir la gestión de usuarios mediante roles preconfigurados y debe ser capaz de crear roles personalizados. • Permite utilizar cualquier aplicación de un tercero para poder realizar la instalación del agente. • Cuenta con la capacidad de crear grupos que pueden alimentarse de forma estática y dinámica. • Capacidad de personalización del dashboard para mostrar los widgets según las necesidades de la Entidad. • Capacidad de almacenar una auditoría de eventos sobre las acciones realizadas en la consola • Deberá permitir el envío automático de alertas al correo electrónico cuando se identifica una actividad maliciosa. Podrán aplicarse filtros a dichas alertas para solo mostrar las de mayor relevancia. • Deberá permitir la generación de reportes a través de plantillas preconfiguradas y también permitir definir reportes personalizados. • Mantener un historial de los reportes que han sido generados para su posterior consulta. • Los reportes podrán ser enviados de forma automática y programada a una o más direcciones de correos electrónicos.
Threat Intelligence	• Capacidad de alimentar la plataforma de Indicadores de Compromiso (IOC) de manera manual o automática vía API • Los IOC soportados deberán ser de tipo Hash, Ruta, Nombre de archivo, Dominio, Dirección IP.

ANEXO No. 1 FICHA TÉCNICA

Grupo 1 - Ítem 2 – Software Seguridad de dispositivos	
	• Capacidad de agregar IOC de manera individual o masiva (por ejemplo, subiendo un archivo CSV) • Capacidad de colocar un nivel de reputación, confiabilidad del IOC y una fecha de expiración. • Debe poder integrarse a una plataforma tercera de Threat Intelligence como Virus Total. • Mostrar un mapa geográfico que permita analizar la dirección IP detectada como parte de incidente, como mínimo deberá mostrar lo siguiente: fecha de registro, ISP (Internet Service Provider), país. La información deberá poder ser mostrada en base al país, proceso, puerto e IP destino. • Deberá contar con un dashboard que permita analizar el comportamiento del hash de un archivo en particular, mostrando su nivel de reputación y si dicho hash ha sido detectado en otras alertas e incidentes.
Capacidades de Respuesta	• Deberá ser posible colocar en lista bloqueada y/o lista permitida uno o más hashes. • Deberá permitir colocar en cuarentena un archivo malicioso detectado y/o bloqueado. La colocación en cuarentena deberá poder realizarse de manera manual y automática. • Capacidad de extraer el archivo dump de la memoria RAM del endpoint a partir de una alerta revisada. • Capacidad de extraer el malware o archivo sospechoso del endpoint hacia la consola, para poder ser analizado por el investigador • Debe ser posible aislar el endpoint de la red para que no tenga comunicación con ningún dispositivo de la red interna o externa. • Capacidad de configurar reglas de automatización que permitan ejecutar una acción determinada en los endpoints en base condiciones de alertas de seguridad, como mínimo estas reglas deberán permitir las siguientes acciones de manera automática: aislar el endpoint, hacer un escaneo de malware, extraer el malware desde el endpoint. • Deberá ser posible realizar una conexión remota a cada endpoint que forme parte de una investigación para ejecutar las siguientes acciones: * Listar procesos y archivos * Ejecutar instrucciones por línea de comandos (CMD y Powershell para el caso de Windows; Bash para el caso de Linux). * Ejecutar scripts basados en Python • Capacidad de ejecutar scripts remotamente a múltiples endpoints de manera concurrentes. • Deberá contar con una librería de scripts predefinidos y deberá ser posible configurar scripts personalizados basados en Python. • Capacidad de tareas remotas a múltiples endpoints, como mínimo cerrar procesos, eliminar archivos, eliminar y/o modificar claves de registro. • Mostrar sugerencias para las remediaciones de un equipo comprometido. • Capacidad de integración con un SIEM vía Syslog y plataformas SOAR. • La plataforma deberá contar con una capa de automatización para realizar acciones de manera automática basada en filtros tanto generales como específicos en el que se incluyan, nombres, hostnames, IP's, alertas, severidad, etc.
Visualización	• Deberá de contar con un dashboard en nube que permite visualizar alertas generadas de distintas fuentes. • Deberá correlacionar alertas de datos de los agentes instalados en los endpoint y agruparlas dentro de incidentes • Deberá de poder mostrar el número total de alertas e incidentes, y debe incluir la capacidad de filtrar la información de forma flexible

Grupo 1 - Ítem 2 – Software Seguridad de dispositivos	
	• La solución deberá permitir la creación de una secuencia gráfica que correlacione las alertas individuales con el objetivo de describir la secuencia de un ataque. • La solución deberá de mostrar información específica de cada proceso involucrado en la secuencia gráfica. • En la pantalla emergente, en caso de estar disponible, deberá de mostrarse los datos relacionado con el perfil de comportamiento y la ejecución del archivo. • La solución deberá mostrar una advertencia cuando un ejecutable en particular, que forme parte de la secuencia gráfica, tenga un comportamiento sospechoso. • La solución deberá de mostrar datos generales de la ejecución de un proceso que forme parte de la secuencia gráfica, entre los que se encuentran ruta de ejecución, nombre de usuario que ejecutó el proceso, tiempo de su ejecución, valor MD5 del ejecutable relacionado con el proceso, veredicto del análisis del sandbox, valor SHA256 y línea de comandos de la ejecución. • La solución deberá mostrar la actividad de cada proceso identificado, en columnas por categorías. Entre las categorías a incluir debe de estar la actividad de red, actividad de los archivos, actividad del registro, módulos ejecutados e intentos de inyección a procesos. • La solución deberá de proporcionar la capacidad de decodificar cadenas de caracteres codificadas en base-64 para mostrarlo en texto plano. • La solución deberá de poder identificar, de todas las actividades mencionadas anteriormente, aquellas que sean maliciosas o altamente sospechosas y separarlas en una categoría de fácil acceso para el analista. • Deberá contar con inteligencia de amenazas compartida para distribuir inteligencia de amenazas de crowdsourcing del servicio de análisis de malware basado en la nube a firewalls, agentes de punto final y servicios de detección y respuesta • Para cada una de las actividades mencionadas anteriormente, la solución debe permitir desplegar los datos en columnas para si visualización, administración y gestión. • La solución deberá mostrar si existió una inyección de código o si el protocolo RPC es utilizado en otro proceso desde una computadora local o remota. • La solución deberá proporcionar de manera gráfica la interacción que existe con las direcciones IP que se quieran investigar. Deberá de poder mostrar diferentes opciones de vistas como la ubicación geográfica o los archivos ejecutables que generaron esa comunicación. • La solución deberá proporcionar de manera gráfica la interacción que existe entre uno o varios procesos que sean investigados. La gráfica deberá de mostrar la interacción entre los procesos, y si existe una relación entre las computadoras que ejecutan dichos procesos, entre otros aspectos.
Visibilidad - Vulnerabilidades	• Deberá poder generar un inventario de las aplicaciones instaladas en las computadoras con sistema operativo Windows, MacOS y Linux • Deberá generar un inventario de características de hardware del endpoint, como mínimo cantidad de memoria RAM; tipo, marca y capacidad de procesador; almacenamiento del disco duro; identificar si es servidor, desktop o laptop; sistema operativo y arquitectura. • Deberá poder listar los usuarios locales creados en el endpoint y su respectivo estado (activo o inactivo) • Deberá poder listar los autoruns, servicios y unidades o carpetas compartidas para el caso de Windows. • Deberá mostrar los daemons para el caso de MacOS y Linux

Grupo 1 - Ítem 2 – Software Seguridad de dispositivos	
	• Deberá mostrar las vulnerabilidades de los endpoints, ofreciendo detalles de los CVEs, incluyendo el nivel de severidad y métricas según la base de datos de vulnerabilidades de NIST • Deberá ser capaz de guardar un histórico diario de estos inventarios, para poder comparar cambios que hubiesen ocurrido. Este histórico deberá estar disponible por al menos 30 días. • La plataforma podrá contar con la capacidad de eliminar los IOC's de todos los dispositivos que tengan un agente instalado y siempre que tengan una ruta o hash, md5 respectivamente.
Configuración y elementos de identificación	• La solución deberá de contar con mecanismos de generación de alertas considerando el comportamiento mostrado por los procesos de los equipos de computo. • Las alertas generadas por el comportamiento de los procesos no deberán de utilizar firmas o heurísticas. • Cada alerta generada por el comportamiento de los procesos deberá de tener una descripción del comportamiento identificado. • Cada alerta generada deberá de contar con una clasificación de acuerdo a su severidad. • La solución deberá permitir al analista definir comportamientos de procesos para que generen alertas. • La solución deberá de permitir la generación de excepciones a los comportamientos de los procesos que hayan sido identificados como maliciosos o sospechosos. • La solución deberá de permitir deshabilitar, modificar, exportar o eliminar los comportamientos que generen las alertas por el comportamiento de los procesos. • La solución deberá de soportar el uso de indicadores de compromiso tradicionales, incluyendo rutas de archivos, nombres de archivos, dominios, direcciones IP y hashes. • La solución deberá de permitir deshabilitar, modificar, exportar o eliminar un indicador de compromiso mediante un menú contextual. • La solución deberá de permitir la gestión de los indicadores de compromiso por comportamiento de procesos e indicadores de compromiso tradicionales mediante la consola de administración.
Consola de Administración y Reportes de la Solución	• Administración de políticas centralizada, vía una consola web. • La consola debe clasificar los eventos en tres niveles de acuerdo a su severidad: bajo, medio y alto. • La consola de administración debe identificar claramente los eventos que han sido reportados y/o bloqueados y aquellos que han sido detectados. • Debe clasificar el estado de los incidentes en cuatro distintos niveles de severidad: alto, mediano, bajo e informativo. • Debe clasificar el estado de las alertas en cuatro distintos niveles de severidad: alto, mediano, bajo e informacional. • Capacidad de poder agrupar las alertas relacionadas en incidentes, así como proporcionar un contexto del mismo. • Capacidad de poder extraer los elementos importantes o relevantes de las alertas, y mostrarlos a manera de resumen en la pantalla de análisis del incidente. • La consola deberá de proporcionar información detallada bajo demanda de los eventos identificados como exploits. • Permitir la actualización y desinstalación del agente a partir de la consola. • Permitir utilizar cualquier aplicación de un tercero para poder realizar la instalación del agente. • Permitir la integración con Active Directory para la gestión de computadoras y configuración de políticas.

Grupo 1 - Ítem 2 – Software Seguridad de dispositivos	
	• Debe tener la capacidad de poder crear perfiles granulares. • Debe tener la capacidad de poder crear políticas basadas en los perfiles creados. • Debe tener la capacidad de poder aplicar políticas a usuarios, grupos, computadoras o unidades organizacionales de Active Directory. • Debe tener la capacidad de crear grupos virtuales que pueden alimentarse de forma estática y dinámica. • La alimentación dinámica de los grupos virtuales podrá ser de forma estática y dinámica, siendo posible configurar para la forma dinámica el nombre de la computadora y dirección IP como mínimo. • Cada evento de prevención o notificación cuenta con información básica como tipo de evento, módulo que realizó la prevención, detalles de ese módulo, nombre de la computadora, nombre del usuario, sistema operativo, versión del agente, proceso que generó el evento de prevención, ruta de ejecución del proceso que generó el evento de prevención (en caso de estar disponible), horario y fecha del evento, información forense (en caso de estar disponible). • La consola deberá de ser proporcionada bajo un esquema software as a service. • Dashboard donde se muestran los incidentes de seguridad que no han sido atendidos (clasificados de acuerdo a su criticidad en alta, media y baja), un resumen sobre los incidentes de seguridad, la cantidad de endpoints que tienen instalado el agente (clasificados por su plataforma), la cantidad de licencias disponibles y la versión del agente. • Dashboard donde se describen las características de los incidentes de seguridad que se han generado. Este dashboard debe de permitir analizar a mayor detalle las alertas de seguridad, incluyendo los reportes generados por el agente. • Debe permitir la Integración con una plataforma de ciberseguridad la cual incluya una nube de inteligencia y contextualización de amenazas, a través de un API. • Debe permitir crear excepciones a reglas, mecanismos de detección y/o mecanismos de protección desde la consola. Estas excepciones deben de poder aplicarse a una computadora en específico, o a un grupo de computado • Deberá de poder utilizar los datos capturados por el agente que se utiliza para realizar las tareas de detección e investigación. • Deberá de contar con un dashboard que permite visualizar alertas generadas de distintas fuentes • La solución deberá implementar un menú contextual que permita analizar de manera detallada la alerta, generar una línea de tiempo, editar una regla, eliminar una alerta, copiar el URL de una alerta y copiar la alerta. • La solución deberá de mostrar el nombre de la computadora, su dirección IP y el nombre del proceso que generó la alerta. • La solución deberá de permitir exportar los datos contenidos en el dashboard, incluso si se han aplicado filtros, a un archivo plano. • La solución deberá permitir al analista copiar toda la información de la actividad identificada, por cada renglón. • La consola debe permitir la gestión de usuarios mediante roles.
Soporte y Garantía	• Garantía de mínimo Tres (3) años para todos los componentes, con el servicio de garantía más alto ofrecido por el fabricante y atención y soporte 7x24x4, incluyendo todos los repuestos necesarios originales de fábrica. La garantía deber ser certificada por parte del fabricante. • Mínimo Tres (3) años Tiempo de activación, soporte y actualizaciones • Se solicita como mínimo un (1) mantenimiento preventivo por cada año de garantía, realizado por personal certificado por el fabricante de los productos.Con el fin de

Grupo 1 - Ítem 2 – Software Seguridad de dispositivos	
	garantizar el correcto uso y apropiación de las buenas prácticas dadas por el fabricante, el proponente deberá acreditar que es distribuidor autorizado de los productos. Este documento deberá ser expedido por el fabricante con fecha no mayor a treinta (30) días calendario anteriores a la fecha del cierre del presente proceso de selección.
Personal	Asignar personal especializado en la instalación, configuración y puesta en funcionamiento de la solución ofertada y para ellos deberá demostrar: • Certificación emitida por el fabricante de los productos que detalle la idoneidad en la manipulación de los productos ofertados. • Certificaciones que demuestren experiencia mínima de tres (3) años en instalación configuración y puesta en funcionamiento de los productos ofertados.
Instalación	Todos los equipos y componentes de la solución ofrecida deben ser entregados e instalados en la sede central del Ministerio de Salud, ubicado en la Cra. 13 No. 32 76, piso 21 Todos los licenciamientos que se requerida para activar o poner en funcionamiento todas y cada una de las características y funcionalidades de los equipos, módulos y componentes, deberán suministrarse, sin costo adicional para el Ministerio.

ANEXO No. 1 FICHA TÉCNICA

Grupo 2. Ítem 1 - Balanceador de Carga Tipo Appliance	
ATRIBUTO	**ESPECIFICACION**
DESCRIPCION	**Appliance de red y seguridad informática perimetral e interna.**
CANTIDAD:	Uno (1)
Especificaciones mínimas requeridas	
Tecnología	Balanceador de carga
Características Generales	• La solución debe estar compuesta por mínimo dos equipos de idénticas características, para su funcionamiento en Alta Disponibilidad (HA), ya sea en Activo-Pasivo o Activo-Activo. • La solución deberá utilizar discos duros de tecnología SSD, evitando la utilización de piezas móviles y maximizando así la fiabilidad del sistema. • Deberá disponer de hardware criptográfico dedicado para realizar procesamiento SSL acelerado de alto desempeño • Los gabinetes deben tener una altura máxima de hasta 1U (unidad de rack) por equipo. • La solución debe suministrarse con fuentes de alimentación redundantes e intercambiables en caliente. • La solución debe suministrarse con ventilación redundante e intercambiable en caliente (Fan). • La solución debe permitir el repositorio redundante de versiones de firmware para aumentar su disponibilidad. • Debe contar con software de protección contra ataques de denegación de servicio distribuido. Todas las funcionalidades relacionadas anteriormente, deberán ser suministradas con los mismos equipos o hardware ofertados. No se aceptan soluciones que incluyan algunas funcionalidades con hardware adicional. En caso de requerir licencia para la instalación, configuración y puesta en funcionamiento de la solución, deberán ser asumidas por el proveedor sin costo adicional para el Ministerio.
Conectividad	• Mínimo 4 puertos 10Gbe SFP+ • Mínimo 5 puertos de cobre de 1 Gb • Mínimo 4 puertos de cobre o Fibra de 1 Gb SFP • Mínimo 1 puerto de gestión dedicado para acceso GUI y CLI. • Mínimo 1 puerto de consola RJ-45 compatible con cables de consola,
Estándares de Red	• Soportar VLAN 802.1q, Vlan tagging • Soportar el estándar 802.1AX • Soportar el estándar 802.3ad • Soportar NAT, SNAT, PAT • Soporte de IPv6: El equipo debe funcionar como Gateway entre redes IPv6 e IPv4 permitiendo tener ambos tipos de redes simultáneamente. • Calidad de Servicio: Soportar QoS • Soportar de VXLan • Soporte enrutamiento estático y dinámico con los protocolos RIP, OSPF, y BGP. • Soportar NVGRE
Interoperabilidad IPV4 IPV6	• Soportar Balanceo de servidores en diferente protocolo. SLB-PT, SLB-64 (Ipv4-ipv6, ipv6-ipv4) • Soportar Application level gateway para protocolos con puertos dinámicos SIP y FTP • La solución deberá permitir el balanceo de cargas entre servidores Ipv6 e Ipv4.

ANEXO No. 1 FICHA TÉCNICA

Grupo 2. Ítem 1 - Balanceador de Carga Tipo Appliance	
Administración	• La solución debe permitir como mínimo el acceso para la administración del equipo appliance vía CLI (Interfaz de línea de comandos) por SSH, interfaz de administración gráfica basada en Web seguro (HTTPS) • La solución debe como mínimo integrarse con LDAP y RADIUS. • La solución debe soportar el envío de alertas y eventos a un Sistema Centralizado mediante: Protocolo SysLog, Notificación vía SMTP, SNMP versión.2.0 o superior • El sistema de administración debe ser totalmente independiente del sistema de procesamiento de tráfico y no consumir recursos de procesamiento de tráfico. • Debe Contar con plantillas para la implementación rápida de aplicaciones de mercado conocidas (ej, Oracle, Microsoft, SAP, IBM) y permitir crear plantillas customizadas que puedan ser actualizadas/exportadas entre equipos. • Permitir la creación de Roles de administración diferentes para el acceso a los equipos. • Soporte Rest-style XML API • Soporte de port Mirroring. • Soporte de Netflow v9 y v10(IPFIX), sflow • Opción de seleccionar el número de CPUs para tareas administrativas. • Soportar generación de eventos de auditoría sobre las operaciones realizadas en la solución. • Debe permitir la creación de paneles de información "Dashboard" para monitorear el tráfico en tiempo real. • Los paneles de información deben permitir incluir estadísticas sobre tráfico enviado, recibido, sesiones establecidas, solicitudes capa 7, estado de operación de servidores, entre otras. • La solución debe contar con un módulo de estadísticas, que permita identificar cantidad de paquetes recibidos, ataques generados, métodos de optimización usados, estadísticas del tráfico sobre aplicaciones en diferentes capas de modelo OSI, entre otras. • El componente de visibilidad debe permitir identificar anomalías de tráfico como picos generados y fallas. • La solución ante un evento generado, debe permitir la notificación por SNMP o SMPT a los administradores, optimizando el tiempo de reacción sobre la plataforma. • Mostrar información del estado actual de operación referente a CPU, Memoria, Disco, Rendimiento, sesiones, conexiones procesadas a nivel general de la solución. • Debe incluir un mapa de servicios el cual permita tener una vista general de todas las aplicaciones configuradas y determinar el estado de operación de cada una, permitiendo identificar de manera inmediata el servicio / servidor afectado. • La solución debe incluir la capacidad de crear y manejar dominios virtuales independientes (desde capa 3 hasta capa 7).
Requerimientos de Rendimiento	• Permitir procesar como mínimo un throughtput de mínimo 20 Gbps en capa 4 (Layer 4). • Deberá ser capaz de procesar como mínimo un throughtput de mínimo 20 Gbps en capa 7 (Layer 7). • Como mínimo 500.000 Nuevas Conexiones por Segundo tratadas a nivel 4 • Como mínimo 180.000 Conexiones por Segundo (CPS) tratadas a nivel 7 • Como mínimo 1.4 Millones de Queries Por Segundo DNS Stateful • Como mínimo 2 Millones de Queries Por Segundo DNS Stateless • Deberá contar con al menos 16 GB de memoria RAM • Deberá ser capaz de procesar 32 millones de sesiones concurrentes • La solución deberá de contar con un hardware específico para realizar el procesamiento SSL, esto es, debe ser independiente a la CPU y Memoria RAM central del dispositivo. • La solución deberá incluir y soportar 15.000 Conexiones por segundo (CPS) con algoritmos RSA de 2048 bits, y 8 CPS con algoritmo ECDSA (P256)

ANEXO No. 1 FICHA TÉCNICA

Grupo 2. Ítem 1 - Balanceador de Carga Tipo Appliance	
	• Deberá ser capaz de procesar al menos 130.000 transacciones por segundo (TPS) para procesamiento de SSL con llaves de 2048 bits • Deberá ser capaz de procesar al menos 500 mil Sesiones Concurrentes SSL • Deberá ser capaz de procesar al menos SSL Bulk Throughput de 9 Gbps para llaves de 1024 y 2048. • Deberá tener la capacidad de soportar ataques de Denegación de servicio Syn flood al menos de 4 millones de syn/sec
Balanceo Local	• La solución debe permitir hacer control de balanceo de tráfico utilizando algoritmos especializados como: Round-Robin, Least Connection, Service Least Connection, Weighted Round Robin o Wighted dinámico, Fastest Response time, Least Request" • Deberá contar con monitores de salud configurables para protocolos: (icmp, tcp, udp, http/s, ftp, smtp, pop3, snmp, dns, radius, ldap, rtsp, sip, ntp, imap,kerberos, bases de datos mssql/Oracle/mysql/posgre). Así como la agrupación de varios monitores mediante el uso de operadores lógicos • Deberá aplicar monitorización basada en scripting “monitores externos”. • Deberán admitirse scripts en bash, python, perl ó tcl • Permitir la ejecución de scripts en lenguaje TCL para determinar la respuesta emulando un cliente. • Estos scripts en lenguaje TCL deberán ser capaces de evaluar tanto tráfico TCP como UDP. • A través de los scripts TCL deberá poder realizarse inspección profunda de paquetes y tomar acciones sobre el tráfico tales como bloqueo, redirección, decisiones de balanceo e incluso modificación del contenido del tráfico. • Permitir en los scripts eventos basados en cliente, eventos basados en servidor y flujo de conexión. • Deberá soportar la configuración de monitores predefinidos y personalizados que permitan comprobar y verificar la salud y disponibilidad de los componentes de la aplicación y de la red. • La solución debe soportar persistencia en el balanceo basado en Ip origen, ip destino, ID de session, y hash. • La solución deberá permitir balanceo basado en el Host o la Url del request http. • La solución deberá permitir la configuración de una Url en caso que todos los servidores estén caídos, a la cual se enviarán los usuarios. • La solución debe soportar balanceo de SIP para VoIP. • La solución debe soportar el balanceo de Firewall manteniendo persistencia de las sesiones para garantizar la comunicación. • Soportar balanceo de Proxy a traves de la funcionalidad TCS (Transparent Cache Switching) • El balanceo de Proxy con TCS deberá poderse realizar tanto en capa 4 como en capa 7 • La solución deberá soportar TCS en IPv6 asi como para servidores FTP (TCS for FTP) • Soportar el balanceo de multiples enlaces de conexión a internet • Soportar el balance de Diameter y bases de datos • soportar ICAP para la integración con herramientas de seguridad • La solución deberá soportar protocolo SPDY • Deberá contar con técnicas de aceleración y optimización de las aplicaciones tales como Compresión, Caching, Offloading SSL y Multiplexación de conexiones. • Deberá soportar SSLOffload, Terminacion de SSL, SSL Bridging, SSL Proxy, SSL session ID reuse"

Grupo 2. Ítem 1 - Balanceador de Carga Tipo Appliance	
	• A nivel terminación SSL, deberá soportar como mínimo el estándar TLS 1.2 con soporte del mecanismo SNI para permitir la publicación de múltiples aplicaciones https sobre una única dirección IP • Deberá soportar el envío de notificación via Email cuando un certificado de una aplicación publicada esté cercano a expirar. • Soportar las funcionalidades de encripción a través de hardware dedicado y que se soporten al menos los siguientes algoritmos de acuerdo a los standares y recomendaciones internacionales actuales: TLS_RSA_WITH_3DES_EDE_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TSLv 1.2, • Podrá aplicar políticas de acceso o limitación de conexiones a los servicios en base a categorías de geo-localización ó listados de redes/hosts de origen. • Dispondrá de la funcionalidad de debuging. • Deberá de contar con la capacidad de realizar inspección profunda, así como transformación de paquetes para proveer funcionalidad de balanceo avanzado de aplicaciones • Deberá soportar balanceo avanzado de servidores en capa 4 y 7 que incluya diferentes metodos para la persistencia de sesiones como son: Cookie, IP destino, IP origen e ID de sesión de SSL • La solución deberá contar con soporte a direccionamiento IPv6 tanto para procesamiento de tráfico referente a la función de balanceo de servicios como a la administración propia mediante el puerto designado para esta función. Así mismo es necesario soporte a ambientes mixtos de IPv4/IPv6 • Deberá de soportar como mínimo los protocolos de ruteo dinámico: OSPFv2 para IPv4 y OSPFv3 para IPv6, IS-IS para IPv4 e IPv6 y BGP4+ para IPv4 e IPv6 sin necesidad de una licencia adicional o la misma debe de ser incluida en la oferta. • Deberá incluir como mínimo la funcionalidad de cacheo de contenido web utilizando la memoria RAM de la plataforma cumpliendo con el RFC 2616.. • Deberá tener la capacidad de realizar compresión del tráfico web para mejorar los tiempos de respuesta de las aplicaciones web a los usuarios. • Deberá como mínimo poder reasignar las respuestas de servidores con mensajes 5xx para reenviarlas a servidores en mejores condiciones de operación. • Deberá permitir el tratamiento de tráfico que no sea web pero que utilice el puerto 80, para enviarlo a una herramienta de seguridad. • Deberá soportar la Inserción y/o reemplazo de encabezados en el tráfico http. De manera particular la inserción de la Ip del cliente cuando el modo de implementación determine la utilización de Nat en el tráfico. • Deberá soportar la redirección y/o la reescritura del URL en un request de http • Deberá permitir el balanceo de servidores de bases de datos aplicando capa de seguridad con procolos SSL y TLS para proteger información sensible hacia los servidores. • Deberá soportar el balanceo a través de múltiples enlaces si la latencia del enlace está por debajo de un cierto umbral configurable. • Deberá soportar el balanceo a través de múltiples enlaces permitiendo hacer control de balanceo entre uno o varios tipos de algoritmos especializados de balanceo: fastest-link-always, threshold, Round Robin, Least-connections

ANEXO No. 1 FICHA TÉCNICA

Grupo 2. Ítem 1 - Balanceador de Carga Tipo Appliance	
Balanceo Global	• Deberá contar con funcionalidad de controlador GSLB (Global server load balancer) tanto en modo stand-alone como sobre particiones (instancias virtuales), para el balanceo de datacenters y balanceo de enlaces de internet tanto de tráfico entrante como saliente. • Podrá operar como servidor DNS tanto en modo "Server" mediante delegación de zonas/nombres como en modo "Proxy" mediante la reescritura transparente de respuestas DNS, incluso ambos modos mezclados para un mismo dominio. • Proporcionará técnicas de Route Health Injection para aquellos protocolos no basados en DNS pudiendo propagar/eliminar rutas a host mediante RIP, OSPF, BGP ó IS-IS. • Deberá aplicar todas las técnicas de monitorización disponibles para balanceo convencional, incluso aquellos monitoreos más complejos basados en scripting. • Permitirá efectuar cambios en las configuraciones de los controladores. • Deberá incluir la funcionalidad para realizar balanceo de enlaces de internet, ya sea de tráfico entrante, como de tráfico saliente, en caso de requerir licenciamiento adicional para esta funcionalidad, sin requerir licenciamiento adicional para ello. • Deberá incluir la funcionalidad para realizar balanceo global de servicios entre sitios geográficamente dispersos, sin requerir licenciamiento adicional para ello. • Deberá poder responder a Ipv6 AAAA records. • La solución debe admitir el equilibrio global de solicitudes con varias métricas para garantizar mayores redundancias de los servicios equilibrados entre diferentes centros de datos. La solución debe admitir las siguientes métricas: a. Number of active Servers under each site b. Admin Preference c. Bandwidth Cost d. Connection Load e. Geolocation f. Health Check g. Least Response h. Number of Sessions i. Ordered IP j. Round Robin l. Weighted IP j. Weighted Site.
Seguridad	• Debe permitir limitar el número de conexiones y solicitudes por IP de origen para cada dirección IP Virtual; • Debe permitir la adición automática de direcciones IP de origen que excedan el límite establecido a una lista de bloqueo, por un período de tiempo determinado mediante configuración. • La solución debe admitir la creación de políticas de equilibrio en las que cierto tráfico se envía a un grupo de servidores, mientras que un tráfico diferente se envía a otro grupo de servidores, como los servidores honeypot. • La solución debe ofrecer una política de balanceo de carga según listados de Redes y/o Hosts. • La solución debe ofrecer la posibilidad de actualizar dichas listas de forma manual o automática en función de equipos de terceros; • La solución debe ofrecer protección contra ataques DDoS (en particular, ataques SYN Flood) • La solución debe soportar la correlación de Source NAT que se realizará con ACL, con el objetivo de tener un mayor control sobre el tráfico transportado. • La solución debe admitir WAF

ANEXO No. 1 FICHA TÉCNICA

Grupo 2. Ítem 1 - Balanceador de Carga Tipo Appliance	
	• Debe ser un sistema de monitoreo de seguridad de aplicaciones que monitorea el tráfico web anómalo y sospechoso y protege contra ataques dirigidos a aplicaciones y servidores. Debe proporcionar una protección para aplicaciones y API, ofreciendo ventajas sobre el WAF heredado. Como mínimo, debe ofrecer: API de protección de fuerza bruta, Prevención del acceso API no autorizado, Mitigación del abuso de API, Lista blanca de URL / verificación de lista negra, Examinar las URL a las que se dirigen las solicitudes entrantes y bloquear las conexiones a las URL que no figuran en la lista blanca de URL, Verificar el cumplimiento del protocolo HTTP, Verificar la solicitud para detectar varias violaciones del protocolo HTTP, Prevención de ataques a USERAGENT para evitar que el software automatizado pueda identificar vulnerabilidades de seguridad, Falsificación de solicitudes del lado del servidor, Protección contra ataques de puerta trasera, Protección contra ataques de ejecución de comandos (CMDEXE), Protección contra ataques de Cross Site Scripting (XSS), Protección contra ataques de cruce de directorios, Protección contra ataques tipo Log4J JNDI, Protección contra ataques de inyección SQL, Protección contra anomalías de ruta anormales, Protección contra anomalías del tipo Bad Hop Headers, Protección contra Anomalías del tipo Inyección de Código PHP, Protección contra anomalías detectadas por compresión, Protección contra anomalías de navegación contundentes, Protección contra anomalías de la API GraphQL, Protección contra anomalías de variables duplicadas de GraphQL, Protección contra anomalías de GraphQL IDE, Protección contra anomalías de introspección GraphQL, Protección contra anomalías de profundidad máxima GraphQL, Protección contra anomalías de nombres de operaciones requeridas faltantes en GraphQL, Protección contra anomalías GraphQL Variable indefinida, Protección contra anomalías de división de respuestas HTTP, Protección contra anomalías de codificación no válidas, Protección contra anomalías de errores de codificación JSON, Datos mal formados en el cuerpo de la solicitud, Protección contra anomalías maliciosas del tráfico IP, Protección contra anomalías del encabezado de solicitud de tipo de contenido faltante, Protección contra anomalías sin agente de usuario, Protección contra anomalías de bytes nulos, Protección contra anomalías de archivos privados, Protección contra anomalías tipo escáner. Identifica servicios y herramientas de escaneo populares, Protección contra anomalías del impostor SearchBot, Protección contra anomalías de IP marcadas en el sitio, Protección contra anomalías del tráfico Tor, Protección contra anomalías de errores de codificación XML, Cifrado de cookies. • Deberá incluir la funcionalidad necesaria para realizar Web Application Firewall (WAF), sin requerir el pago de licenciamiento adicional para ello o en caso de requerirse licenciamiento, éste se debe incluir dentro de la solución ofertada.
ANTIDDOS	• Debe contener la funcionalidad de antiDDoS para proteger los recursos balanceados de ataques de inundación a nivel de red. • La funcionalidad de DDoS debe proteger y clasificar el tipo de ataque a partir del comportamiento de la fuente, Identificando las fuentes incorrectas basándose en múltiples métricas para perfilar anomalías en el comportamiento de las fuentes. • Las características de protección DDoS deberán incluir al menos las siguientes técnicas: Syn flood Attack protection, ACK flood Attack protection, Icmp flood attack protection, UDP flood attack protection, Smurf Attack protection, Syn cookie protection, Dynamic SYN Cookies, SYN Cookie Buffering, Network Attack - malformed packets, Lan Attack protection, Ping of Death, Ip Fragmentation Attack, TCP No flag exploit, Slowloris protection Sockstress protection, http get flood protection, http post flood protection, Slow Post Attack protection, TCP Zero Window Attack protection, TCP syn fragmentation attack protection, Tear Drop Attack protection, Scripts personalizados para generar protección DDoS, IP anomaly protection, Connection Rate Limiting, Connection LImiting, Bandwidth Rate Limiting Por ip Origen, Ip limiting, icmp rate limiting, icmp rate limiting.

Grupo 2. Ítem 1 - Balanceador de Carga Tipo Appliance	
	• Permitir la adición dinámica de Ip a listas Blancas y Negras configurando de forma personalizada los criterios de clasificación como atacantes.
Tráfico DNS	• Permitir control de acceso a servicio basado en Geolocalización • La Solución deberá contar con la funcionalidad de Firewall de DNS mediante el uso de mecanismos de validación de tráfico que permita descartar o redireccionar consultas malformadas de DNS, protecciones de alto desempeño contra incrementos súbitos de tráfico como: cache de DNS por IP virtual o por registro, restricciones basadas en nombre de dominio. • Deberá permitir la regulación de flujo de tráfico dinámico mediante limitación de conexiones basada en IP origen y balanceo de servidores basado en políticas. • La solución debe soportar políticas de respuesta de DNS (RPZ) para bloquear hosts, sitios, nombres de dominio y direcciones IP maliciosos y mitigar las consultas de DNS con formato incorrecto. • Soportar DNS recursivo ayudando a proporcionar rápidamente la respuesta sin comunicarse con ningún otro servidor DNS. • La solución ofrecerá protección al tráfico DNS al menos con las siguientes técnicas: DNS amplification Attack protection, DNS flood Attack protection, DNS server attack protection, DNS Malformed Packet-drop, DNS Amplification Attacks, DNS Any Filtering, DNS Any Rate Limiting. • A nivel SMTP, soportará la funcionalidad STARTTLS, para iniciar el tráfico de correo seguro a través del balanceador. • Soportar filtros de Spam basado en listas negras y blancas. • Deberá soportar StartTLS para procolos Imap y Pop3 • Deberá soportar la administración de acceso a aplicaciones Web, con integración de authenticación SAML, kerberos, NTLM, LDAP, RADIUS, WIA. • Soportar autenticación y autorización usando SAML • En la funcionalidad anterior debe soportar Single Sigh-on • Soportar autenticación para Microsoft SharePoint, Outlook Web Access. • La funcionalidad de acceso a aplicaciones, debe soportar: Cookie Attributes, OAuth 2.0 y OpenID Connect, reCAPTCHA Challenge Authentication, SAML Redireccion de URL por "Bad Request". • La solución deberá soportar trabajar como Forward Proxy. • Deberá soportar integración con RSA para doble factor de autenticación y RSA Passcode.
Alta Disponibilidad	• Deber soportar configuraciones tanto Activo-Pasivo como Activo-Activo • Debe permitir realizar clustering del sistema, incluyendo todos el cableado y accesorios necesarios. • Debe permitir sincronización de sesiones transportadas entre equipos redundantes, asegurando que no habrá "tiempo de inactividad" y caída de sesiones en caso de fallo de una de las unidades; • Debe soportar tracking y ponderación del estado de elementos externos para controlar el failover entre equipos/particiones.
Visibilidad y Análisis	• La solución debe incluir un sistema de Analítica y Administración centralizada que permita la integración de manera nativa lo siguiente: • Aceleración y rendimiento • tiempo de respuesta end to end • Tiempo de respuesta de servidores • Latencia end-to-end experimentada por clientes • total bytes intercambiados • promedio de porcentaje de requerimientos por segundo • Análisis de comportamiento por URL, servicios y dominios

ANEXO No. 1 FICHA TÉCNICA

Grupo 2. Ítem 1 - Balanceador de Carga Tipo Appliance	
	• Hits en cache y hits perdidos en franjas de tiempo • cantidad de bytes comprimidos y descomprimidos en linea de tiempo • Métodos y códigos de respuesta empleados en solicitudes HTTP / HTTPS" • Trafico: • Top de URL, dominios, puerto y servicios más populares • Distribución geográfica de los request • Top de clientes activos • Estadística de conexiones por aplicación • Estadística de número de conexiones por clientes • Estadísticas de ataques a las aplicaciones y su tipo • Estadísticas de ataques DDoS • WAF: • Información sobre la infracción de la política WAF, incluida la distribución de tipos de infracción, infracciones del umbral HTTP y del protocolo • Estadísticas de infracciones de WAF de series de tiempo por tipos • Manejo de solicitudes WAF de series de tiempo y estadísticas de eventos • Información sobre la seguridad de las cookies • Principales fuentes de solicitudes recibidas que provocaron infracciones de la política WAF" • Promedio de Latencia por servicio del lado del servidor • Promedio de Latencia por servicio del lado del cliente • Información de clientes como OS, Dispositivo de uso y navegador • Gestión Centralizada de tareas sobre los equipos incluidos tales como: Configuración de dispositivos, Respaldo de configuración de los dispositivos, Tareas de despliegue centralizado de imágenes de actualización a los equipos, permite generar programación automática para la ejecución de tareas, Monitoreo de Salubridad de los equipos.
Soporte y Garantía	• Garantía de mínimo Tres (3) años para todos los componentes, con el servicio de garantía más alto ofrecido por el fabricante y atención y soporte 7x24x4, incluyendo todos los repuestos necesarios originales de fábrica. La garantía deber ser certificada por parte del fabricante. • Se solicita como mínimo un (1) mantenimiento preventivo por cada año de garantía, realizado por personal certificado por el fabricante de los productos • El contratista debe estar certificado en mejores prácticas de seguridad de la información ISO27001:2013 con el fin de estar alineado a las prácticas y políticas del Ministerio de Salud y Protección Social. • Con el fin de garantizar el correcto uso y apropiación de las buenas prácticas dadas por el fabricante, el proponente deberá acreditar que es distribuidor autorizado de los productos. Este documento deberá ser expedido por el fabricante con fecha no mayor a treinta (30) días calendario anteriores a la fecha del cierre del presente proceso de selección.
Personal	Asignar personal especializado en la instalación, configuración y puesta en funcionamiento de la solución ofertada y para ellos deberá demostrar: • Certificación emitida por el fabricante de los productos que detalle la idoneidad en la manipulación de los productos ofertados. • Certificaciones que demuestren experiencia mínima de tres (3) años en instalación configuración y puesta en funcionamiento de los productos ofertados. • Certificación mínima en CEH (Certified Ethical Hacker) o CCSP (Certified Cyber Security Professional) o CISM (Certified Information Security Manager) o CISSP (Certified Information Systems Security Professional) o CHFI - Computer Hacking Forensic Investigator

Grupo 2. Ítem 1 - Balanceador de Carga Tipo Appliance	
	• Auditor interno en sistema de gestión de seguridad en la información ISO 27001:2013 o superior o Especialista en seguridad informática o seguridad de la información.
Instalación	Todos los equipos y componentes de la solución ofrecida deben ser entregados e instalados en la sede central del Ministerio de Salud, ubicado en la Cra. 13 No. 32 76, piso 21 Todos los licenciamientos que se requerida para activar o poner en funcionamiento todas y cada una de las características y funcionalidades de los equipos, módulos y componentes, deberán suministrarse, sin costo adicional para el Ministerio.

ANEXO No. 1 FICHA TÉCNICA

Grupo 3. Ítem 1 SOLUCIÓN DE VISIBILIDAD, CONTROL DE LOS CANALES PUBLICOS DEL MINISTERIO	
ATRIBUTO	**ESPECIFICACION**
DESCRIPCION	**Appliance para administración de canales públicos y privados**
CANTIDAD:	Uno (1)
Especificaciones mínimas requeridas	
Características Generales	• La solución debe permitir optimizar y monitorear la red. • La solución debe permitir el control de la red en tiempo real y permitir conocer el rendimiento de las aplicaciones a las cuales el Ministerio accesa para el desarrollo de sus actividades. • La solución debe identificar el uso de la red, los puntos de congestión del tráfico y las áreas problemáticas mediante el análisis del rendimiento de las aplicaciones o del Nivel 7 por aplicación, usuario, dispositivo y ubicación. • La solución debe identificar las aplicaciones más importantes, así como las aplicaciones no autorizadas que puedan estar degradando el ancho de banda • La solución debe priorizar, determinar y asignar, el ancho de banda a utilizar por parte de los usuarios, las aplicaciones y sitios web. • La solución debe usar una biblioteca de informes predefinidos diseñados para solucionar los problemas. • La solución debe modelar e interactuar con los datos para mejorar u optimizar la salud de la red. • La solución debe asegurar que las aplicaciones de la entidad, ya sean locales o en la nube, estén disponibles para su uso y tengan aplicabilidad de calidad de servicios QoS.
Rendimiento	• Rendimiento 1.2 Gbps • Flujo simultáneo 260.000 • Velocidad de nuevas conexiones 11.000/s • Paquetes por segundo 260.000 • Políticas de tráfico 1024 • Rendimiento de caché perimetral 70 Mbps • Conexiones optimizadas 9,000
Conectividad	• Mínimo dos (2) puertos 1G RJ45 con característica bypass bridge pair • Mínimo 2 puertos x 10G SFP+ con característica bridge pair • Mínimo un puerto de administración de consola RJ-45 serial
Capacidades	Debe poder permitir gestionar y administrar los siguientes canales: • Un (1) canal dedicado de 2 Gbps simétrico • Un (1) canal dedicado de 100 Mbps simétrico
Soporte y Garantía	• Garantía de mínimo Tres (3) años para todos los componentes, con el servicio de garantía más alto ofrecido por el fabricante y atención y soporte 7x24x4, incluyendo todos los repuestos necesarios originales de fábrica. La garantía deber ser certificada por parte del fabricante. • Se solicita como mínimo un (1) mantenimiento preventivo por cada año de garantía, realizado por personal certificado por el fabricante de los productos • El contratista debe estar certificado en mejores prácticas de seguridad de la información ISO27001:2013 con el fin de estar alineado a las prácticas y políticas del Ministerio de Salud y Protección Social. • Con el fin de garantizar el correcto uso y apropiación de las buenas prácticas dadas por el fabricante, el proponente deberá acreditar que es distribuidor autorizado de los productos. Este documento deberá ser expedido por el fabricante con fecha no mayor a treinta (30) días calendario anteriores a la fecha del cierre del presente proceso de selección.

ANEXO No. 1 FICHA TÉCNICA

Grupo 3. Ítem 1 SOLUCIÓN DE VISIBILIDAD, CONTROL DE LOS CANALES PUBLICOS DEL MINISTERIO	
Personal	Asignar personal especializado en la instalación, configuración y puesta en funcionamiento de la solución ofertada y para ellos deberá demostrar: • Certificación emitida por el fabricante de los productos que detalle la idoneidad en la manipulación de los productos ofertados. • Certificaciones que demuestren experiencia mínima de tres (3) años en instalación configuración y puesta en funcionamiento de los productos ofertados. • Certificación mínima en CEH (Certified Ethical Hacker) o CCSP (Certified Cyber Security Professional) o CISM (Certified Information Security Manager) o CISSP (Certified Information Systems Security Professional) o CHFI - Computer Hacking Forensic Investigator • Auditor interno en sistema de gestión de seguridad en la información ISO 27001:2013 o superior o Especialista en seguridad informática o seguridad de la información.
Instalación	Todos los equipos y componentes de la solución ofrecida deben ser entregados e instalados en la sede central del Ministerio de Salud, ubicado en la Cra. 13 No. 32 76, piso 21 Todos los licenciamientos que se requerida para activar o poner en funcionamiento todas y cada una de las características y funcionalidades de los equipos, módulos y componentes, deberán suministrarse, sin costo adicional para el Ministerio.

Grupo 3. Ítem 2 SOLUCIÓN DE VISIBILIDAD, CONTROL Y ACELERACIÓN DE LOS CANALES PRIVADOS DEL MINISTERIO	
ATRIBUTO	**ESPECIFICACION**
DESCRIPCION	**Appliance para administración de canales públicos y privados**
CANTIDAD:	Dos (2)
Especificaciones mínimas requeridas	
Características Generales	• La solución debe permitir optimizar y monitorear la red. • La solución debe permitir el control de la red en tiempo real y permitir conocer el rendimiento de las aplicaciones a las cuales el Ministerio accesa para el desarrollo de sus actividades. • La solución debe identificar el uso de la red, los puntos de congestión del tráfico y las áreas problemáticas mediante el análisis del rendimiento de las aplicaciones o del Nivel 7 por aplicación, usuario, dispositivo y ubicación. • La solución debe identificar las aplicaciones más importantes, así como las aplicaciones no autorizadas que puedan estar degradando el ancho de banda • La solución debe priorizar, determinar y asignar, el ancho de banda a utilizar por parte de los usuarios, las aplicaciones y sitios web. • La solución debe usar una biblioteca de informes predefinidos diseñados para solucionar los problemas. • La solución debe modelar e interactuar con los datos para mejorar u optimizar la salud de la red. • La solución debe asegurar que las aplicaciones de la entidad, ya sean locales o en la nube, estén disponibles para su uso y tengan aplicabilidad de calidad de servicios QoS. • La solución debe emplear funciones de aceleración de datos y almacenamiento en caché para garantizar la eficiencia de los canales administrados.

ANEXO No. 1 FICHA TÉCNICA

Grupo 3. Ítem 2 SOLUCIÓN DE VISIBILIDAD, CONTROL Y ACELERACIÓN DE LOS CANALES PRIVADOS DEL MINISTERIO	
Rendimiento	• Rendimiento 6 Gbps • Flujo simultáneo 625.000 • Velocidad de nuevas conexiones 25.000/s • Paquetes por segundo 900.000 • Políticas de tráfico 2048 • Rendimiento de caché perimetral 180 Mbps • Conexiones aceleradas 25.000 • Aceleración 175 Mbps
Conectividad	• Mínimo dos (2) puertos 1G RJ45 • Mínimo 2 puertos x 10G SFP+ • Mínimo 2 puertos fibra multimodo. • Mínimo un puerto de administración de consola DB-9 serial
Capacidades	• Un (1) canal MPLS ubicado en la sede principal Calle 32 de 1 Gbps, el cual debe ser licenciado para visibilidad y control para un (1) Gbps y para la aceleración se debe licenciar 150 Mbps. • Un (1) canal MPLS ubicado en la sede zona franca de 150 Mbps, el cual debe ser licenciado para visibilidad y control en los 150 Mbps y para la aceleración de debe licenciar 150 Mbps.
Soporte y Garantía	• Tres (3) años para todos los componentes, con el servicio de garantía más alto ofrecido por el fabricante y atención y soporte 7x24x4, incluyendo todos los repuestos necesarios originales de fábrica. La garantía deber ser certificada por parte del fabricante. • Se solicita como mínimo un (1) mantenimiento preventivo por cada año de garantía, realizado por personal certificado por el fabricante de los productos. • El contratista debe estar certificado en mejores prácticas de seguridad de la información ISO27001:2013 con el fin de estar alineado a las prácticas y políticas del ministerio de salud • Con el fin de garantizar el correcto uso y apropiación de las buenas prácticas dadas por el fabricante, el proponente cargara junto con la propuesta, una certificación que lo acredite como partner de la marca. Este documento deberá ser expedido por el fabricante con fecha no mayor a treinta (30) días calendario anteriores a la fecha del cierre del presente proceso de selección.
Personal	Asignar personal especializado en la instalación, configuración y puesta en funcionamiento de la solución ofertada y para ellos deberá demostrar: • Certificación emitida por el fabricante de los productos que detalle la idoneidad en la manipulación de los productos ofertados. • Certificaciones que demuestren experiencia mínima de tres (3) años en instalación configuración y puesta en funcionamiento de los productos ofertados. • Certificación mínima en CEH (Certified Ethical Hacker) o CCSP (Certified Cyber Security Professional) o CISM (Certified Information Security Manager) o CISSP (Certified Information Systems Security Professional) o CHFI - Computer Hacking Forensic Investigator • Auditor interno en sistema de gestión de seguridad en la información ISO 27001:2013 o superior o Especialista en seguridad informática o seguridad de la información.

Grupo 3. Ítem 2 SOLUCIÓN DE VISIBILIDAD, CONTROL Y ACELERACIÓN DE LOS CANALES PRIVADOS DEL MINISTERIO	
Instalación	Los equipos y componentes de la solución ofrecida deben ser entregados e instalados en la sede central del Ministerio de Salud, ubicado en la Cra. 13 No. 32 76, piso 21 y la sede Zona Franca Fontibón carrera 106 No. 15-25 Manzana 14 Bodega 80, en atención a las indicaciones del supervisor del contrato Todos los equipos y demás componentes de la solución ofrecida, deben ser instalados, configurados y puestos en funcionamiento, por personal técnico debidamente certificado por el fabricante de los productos ofrecidos.