1. **REQUERIMIENTOS TÉCNICOS DE LA SOLUCIÓN DE BALANCEO DE CARGA**

La Universidad Militar Nueva Granada desea adquirir una solución capaz de administrar y proteger el conjunto de aplicaciones de misión crítica, brindando adicionalmente la capacidad de realizar aceleración de las mismas y balanceo de carga no solo dentro del data center principal sino entre los dos data centers principales ubicados en las sedes de calle 100 y Cajicá.

CARACTERÍSTICAS FÍSICAS Y DE RENDIMIENTO				
A. Características Técnicas Mínimas Obligatorias (s/g bien, servicio u obra)				
Ítem 1. Solución de balanceo de carga sede calle 100	**CUMPLE**		**FOLIO**	**OBSERVACIONES**
	SI	**NO**		
Los equipos ofertados deben ser basados en una plataforma de hardware de propósito específico.				
El sistema operativo del equipo ofertado debe ser de propósito específico y no uno de uso genérico, es decir un SO desarrollado por el fabricante específicamente para propósitos de Balanceo de Carga de Servicios y Aplicaciones basadas en IP (TCP/UDP) y servicios web.				
Deben ser dos (2) equipos en Alta disponibilidad funcionando en par activo, no una solución de clúster virtual entre múltiples equipos pues se busca eficiencia en energía, espacios en rack, administración y facilidad de configuración, escalable a 4 veces su capacidad ofertada sin que esto aumente el espacio de rack inicialmente usado.				
Cada equipo debe cumplir con las características mencionadas a continuación Throughput Nominal de 40 Gbps para balanceo en condiciones de máxima carga. Debe permitir un crecimiento de hasta 160 Gbps de Throughput La solución debe soportar un Throughput en L7 de al menos 18 Gbps y crecimiento hasta 72 Gbps. La solución debe soportar al menos 24 Millones de conexiones simultáneas en total y crecimiento hasta 96 Millones de conexiones. La solución debe soportar al menos 400.000 conexiones por segundo en L4 y crecimiento hasta 1’600.000 de conexiones por segundo Debe Soportar defensa contra ataques de denegación de Servicio (DoS). La solución debe estar en la capacidad de soportar más de un módulo o funcionalidad dentro de la misma caja o dispositivo por ejemplo: Firewall de red. Firewall de Aplicaciones (WAF), Administrador de políticas de acceso, DNS, entre otros.				
Cada equipo debe contar con las siguientes Interfaces de red:				

8 Puertos Ópticos a 10 Gbps. Con mínimo 4 transceiversfp+ Por cada Blade o appliance. Permitir crecimiento hasta 32 puertos de Fibra Óptica a 10 Gbps				
Cada equipo debe contar con fuentes de poder redundantes AC, entradas de voltaje de 110 a 220 VAC que se puedan remover en caliente (hot-swap)				
Los equipos deberán ser instalados en rack estándar de 19".				
Los equipos deben tener la característica de soportar alta disponibilidad, es decir, tener la capacidad de conectarse a una unidad similar y operar en modo activo y la otra unidad en modo pasivo (fail-over) y deberá contar con la capacidad de direccionamiento virtual. El esquema debe tener la capacidad para recuperación de las sesiones del sistema en forma inmediata y automática en caso de fallo de un adaptador, cable de red, canal de controladora o alimentación de fluido eléctrico.				
Cada equipo debe incluir 32 Gb de Memoria RAM mínimo Cada equipo debe incluir mínimo un Disco duro de 400Gb de estado sólido (SSD)				
Cada equipo debe ser tipo chasis, con tarjetas blade modulares. Estas deben permitir agregar y remover blades sin interrupción del servicio. Al adicionar tarjetas blade adicionales el procesamiento y rendimiento del chasis completo se debe aumentar. Se debe incluir mínimo un blade con cada chasis. No debe ser una solución de clúster virtual entre múltiples equipos				
Debe soportar clúster Activo/Activo entre dos o más plataformas, no necesariamente del mismo modelo				
Para mejorar el rendimiento de la sincronización de configuración deberá poder sincronizar la configuración de manera incremental.				
Ante la necesidad de conmutar el tráfico a otros dispositivos del grupo, el sistema deberá poder realizar cálculos para determinar el mejor dispositivo basado en: recursos, capacidad, carga de tráfico en cada dispositivo. Identificando la mejor opción cuando el ambiente sea heterogéneo en cuanto se refiere a plataformas				
La configuración será sincronizada entre todos los dispositivos del grupo pudiendo optar si la sincronización se realiza de manera automática o manual.				

Ítem 2. Solución de balanceo de carga sede Cajicá	**CUMPLE**		**FOLIO**	**OBSERVACIONES**
	SI	**NO**		
El equipos ofertado debe ser basado en una plataforma de hardware de propósito específico				
El sistema operativo del equipo ofertado debe ser de propósito específico y no uno de uso genérico, es decir un SO desarrollado por el fabricante específicamente para propósitos de Balanceo de Carga de Servicios y Aplicaciones basadas en IP (TCP/UDP) y servicios web.				
Deben ser un (1) equipo con redundancia interna a nivel de conectividad, fuentes de poder, sistema de ventilación y unidades de procesamiento, no una solución de clúster virtual entre múltiples equipos pues se busca eficiencia en energía, espacios en rack, administración y facilidad de configuración, escalable a 2 veces su capacidad ofertada sin que esto aumente el espacio de rack inicialmente usado.				
La plataforma debe cumplir con las características mencionadas a continuación Throughput Nominal de 80 Gbps para balanceo en condiciones de máxima carga. Debe permitir un crecimiento de hasta 160 Gbps de Throughput La solución debe soportar un Throughput en L7 de al menos 36 Gbps y crecimiento hasta 72 Gbps. La solución debe soportar al menos 48 Millones de conexiones simultáneas en total y crecimiento hasta 96 Millones de conexiones. La solución debe soportar al menos				

800.000 conexiones por segundo en L4 y crecimiento hasta 1’600.000 de conexiones por segundo Debe Soportar defensa contra ataques de denegación de Servicio (DoS).La solución debe estar en la capacidad de soportar más de un módulo o funcionalidad dentro de la misma caja o dispositivo por ejemplo: Firewall de red. Firewall de Aplicaciones (WAF) Administrador de políticas de acceso, DNS, entre otros.				
La plataforma debe contar con las siguientes Interfaces de red: 16 Puertos Ópticos a 10 Gbps. Con mínimo 4 transceiversfp+ por cada Blade o appliance. Permitir crecimiento hasta 32 puertos de Fibra Óptica a 10 Gbps				
La plataforma debe contar con fuentes de poder redundantes AC, entradas de voltaje de 110 a 220 VAC que se puedan remover en caliente (hot-swap)				
Los equipos deberán ser instalados en rack estándar de 19”.				
Los equipos deben tener la característica de soportar alta disponibilidad, es decir, tener la capacidad de conectarse a una unidad similar y operar en modo activo y la otra unidad en modo pasivo (fail-over) y deberá contar con la capacidad de direccionamiento virtual. El esquema debe tener la capacidad para recuperación de las sesiones del sistema en forma inmediata y automática en caso de fallo de un adaptador, cable de red, canal de controladora o alimentación de fluido eléctrico.				
Cada equipo incluido en la plataforma debe incluir 32 Gb de Memoria RAM mínimo Cada equipo Cada equipo incluido en la plataforma debe incluir mínimo un Disco duro de 400Gb de estado sólido (SSD)				
La plataforma debe ser tipo chasis, con mínimo dos tarjetas blade modulares. Estas deben permitir agregar y remover blades sin interrupción del servicio. Al adicionar tarjetas blade adicionales el procesamiento y rendimiento del chasis completo se debe aumentar. No una solución de clúster virtual entre múltiples equipos				
Debe soportar clúster Activo/Activo entre dos o más plataformas, no necesariamente del mismo modelo				
Para mejorar el rendimiento de la sincronización de configuración deberá poder sincronizar la configuración de manera incremental.				
Ante la necesidad de conmutar el tráfico a otros dispositivos del grupo, el sistema deberá poder realizar cálculos para determinar el mejor dispositivo basado en: recursos, capacidad, carga de tráfico en cada dispositivo. Identificando la mejor opción cuando el ambiente sea heterogéneo en cuanto se refiere a plataformas				
La configuración será sincronizada entre todos los dispositivos del grupo pudiendo optar si la sincronización se realiza de manera automática o manual.				

Ítem 3. Funcionalidades Mínimas para sedes calle 100 y Cajicá				
Ítem 3.1. Administración de tráfico para sedes calle 100 y Cajicá	**CUMPLE**		**FOLIO**	**OBSERVACIONES**
	SI	**NO**		
La solución debe realizar funciones de balanceo de tráfico a aplicaciones basadas en TCP/UDP, incluidos servicios web.				
La solución debe permitir la definición de dirección IP y puerto virtual para la prestación de un servicio, que permita atenderlo mediante una granja de servidores identificados mediante una dirección IP y un puerto del servicio igual o diferente del presentado al público.				
La solución debe tener arquitectura Full-Proxy, control de entrada y salida de conexiones distinguiendo conexiones del lado del cliente y del lado del servidor o los recursos				

Deberá permitir hacer persistencia de conexiones hacia la aplicación con base en cualquier información contenida en cualquier parte del paquete completo, esto para poder adaptar la solución a las necesidades de las diferentes aplicaciones				
La solución debe permitir hacer control de balanceo de tráfico según se defina entre uno o varios tipos de algoritmos especializados de balanceo: Round Robin Proporcional Proporcional dinámico Respuesta rápida Conexiones mínimas Análisis de carga Menor número de sesiones				
El sistema debe ser capaz de identificar fallos en servicios para redundancia de las aplicaciones.				
La solución debe tener reglas que permitan el control de ancho de banda de manera dinámica				
La solución debe realizar monitoreo de la salud de los Servidores que gestione el equipo de Balanceo de tráfico, por medio de: Ping. Chequeo a nivel de TCP y UDP a puertos específicos Monitoreo http y https Monitoreo del hardware y software mediante Windows Management Instrumentation (WMI) o mediante un sistema similar reconocido y aprobado por Microsoft Verificación de la salud de una combinación de servicios, permitiendo tomar la decisión del estado de salud aplicando varios monitores simultáneos. Ejecución de scripts para determinar la respuesta emulando un cliente. Configurar monitores predefinidos y personalizados que permitan comprobar y verificar la salud y disponibilidad de los componentes de la aplicación y de la red. Monitoreo en línea, donde el funcionamiento de la aplicación determine el estado de salud de la misma Monitoreo de aplicaciones de mercado LDAP FTP SMTPIMAP/POP3 Oracle MSSQLMySQLRADIUS SIP Protocolo SASPSOAPWMISNMP				
Control de persistencia de las conexiones: Dirección IP origen Dirección IP destino Cookies Hash SIP: Debe permitir definir el campo SIP sobre el cual hacer persistencia Sesiones SSL Microsoft Remote Desktop Debe Permitir crear persistencia por cualquier valor del paquete por medio de reglas. Debe garantizar afinidad del servidor, de tal forma que una solicitud de un cliente y cada solicitud posterior se dirijan al mismo servidor de la granja.				
Soporte de API para construir aplicaciones de administración o monitoreo personalizadas: Soporte de SOAP/XML, que sea base del Sistema Operativo. Que permita la integración con aplicaciones como VMWare vCenter, Microsoft System Center Virtual Machine Manager (SCVMM), Soporte de Java, .NET, PERL, PHP, PowerShell y Python. Las interfaces de control deben ser accesibles por conexiones SSL con requerimientos de autenticación vía http básica, para evitar accesos no autorizados. Soporte de API REST				
Deberá ser posible modificar el contenido HTML utilizando objetos de configuración y sin necesidad de generar scripts.				
Debe soportar el protocolo TDS para balanceo de MSSQL				
El sistema deberá soportar scripts de programación basados en un lenguaje estructurado (TCL) que permita crear funcionalidades que por defecto no se encuentren en el menú de configuración u opciones y debe soportar la creación de Procedimientos o funciones que pueden ser utilizadas desde cualquier otro script				
El equipo debe ser compatible con tráfico IPSEC.				

Ítem 3.2. Funciones de seguridad para sedes calle 100 y Cajicá	**CUMPLE**	**FOLIO**	**OBSERVACIONES**

	SI	NO		
Cada equipo debe soporte de seguridad SSL con las siguientes características: Incluir el soporte de Aceleración SSL usando Hardware Dedicado Incluir mínimo 21.000 Transacciones por segundo SSL para llaves de 2K Soportar al menos 4.000.000 de Conexiones Concurrentes SSL Soportar al menos 12 Gbps de bulkencryption (Throughput SSL) Soporte de llaves SSL de 1024, 2048 y 4096 bits				
La solución debe manejar AES, AES-GCM, SHA1/MD5 y soporte a algoritmos de llave pública: RSA, Diffie-Hellman, Digital SignatureAlgorithm (DSA) y Elliptic curve cryptography (ECC)				
Debe soportar e incluir Geolocalización de direcciones IP				
Cada equipo debe contar con Protección de la cookie de SYN contra ataques de SYNflood. Esta funcionalidad deberá ser realizada por Hardware específico para la función y soportar 40.000.000 de SYN cookies por segundo.				
Firmado criptográfico de cookies para verificar su integridad.				
Capacidad de integración con dispositivos HSM externos. Deberá soportar al menos ThalesnShield Y SafeNet Luna S				
La solución debe permitir la funcionalidad Proxy SSL. esta funcionalidad permite que sesión SSL se establezca directamente entre el usuario y el servidor final, pero el equipo balanceador debe ser capaz de des encriptar, optimizar y re encriptar el trafico SSL sin que el balanceador termine la sesión SSL				
Se requiere que soporte la extensión STARTTLS para el protocolo SMTP de manera de poder cambiar una conexión en texto plano a una conexión encriptada sin necesidad de cambiar el puerto.				

Ítem 3.3. Funciones de aceleración de tráfico para sedes calle 100 y Cajicá	**CUMPLE**		**FOLIO**	**OBSERVACIONES**
	SI	**NO**		
La implementación de la solución debe incluir la capacidad de hacer aceleración de aplicación a nivel de: Memoria cache. Compresión tráfico HTTP Optimización de conexiones a la aplicación a nivel TCPMultiplexación de conexiones hacia los servidores				
Características de Compresión de tráfico: El sistema deberá permitir comprimir tráfico http a través del estándar GZIP y compatible con browsers MS Internet Explorer, Google Chrome, Mozilla Firefox, Safari, etc. Cada equipo debe contar con una capacidad de compresión de tráfico a una tasa de 12 Gbps o superior usando aceleración por Hardware dedicado, no la CPU de propósito general.				
Debe soportar el protocolo SPDY y funcionar como Gateway SPDY aun cuando los servidores Web no soporten esta característica.				
Permitir la modificación de los tags de cache para cada objeto del sitio web de manera independiente, pudiendo respetar los tags generados por el Web server o modificarlos				
Permitir la definición de múltiples subdominios para un sitio web con el fin de incrementar el número de conexiones simultáneas que puedan darse desde un browser hacia este sitio.				
Permitir reordenamiento de contenido para objetos CSS y Javascript.				

Permitir especificar subdominios adicionales para permitir un mayor número de conexiones TCP mayor.				
Incorporar aceleración para contenidos PDF en el sitio Web				
El acelerador Web debe permitir optimización de imágenes en el sitio web cambiando el formato de la imagen, cambiando el tamaño de la imagen, eliminando encabezados EXIF, cambiando el número de colores.				
Permitir definir múltiples políticas de aceleración y políticas generadas por el usuario				
Debe contar con un editor de políticas de aceleración web integrado a la solución				
Permitir la configuración de reglas de aceleración basado en los encabezados del request o en los encabezados de la respuesta				
Permitir aceleración simétrica y asimétrica				
Soporte al protocolo SPDY, debe permitir funcionar como Gateway SPDY una cuando los servidores Web no soporten el protocolo				
Debe soportar optimización de video HTTP Live Streaming (HLS)				
Debe soportar Adaptive Forward Error Correction a nivel TCP y UDP				
Debe permitir optimización realizando “Content Inlining”, permitiendo poner en línea Javascripts, CSS e imágenes directamente en el HTML (codificados)				
Debe soportar Minificación de contenido removiendo espacios y comentarios del código fuente de Javascripts y CSS reduciendo el tamaño de los archivos.				
La solución debe soportar la optimización de enlaces WAN entre dos equipos utilizando De duplicación, Compresión y optimizaciones TCP de ser necesario.				

Ítem 3.4. Balanceo a nivel global para sedes calle 100 y Cajicá	**CUMPLE**		**FOLIO**	**OBSERVACIONES**
	SI	**NO**		
La solución debe soportar el permitir alta disponibilidad de aplicaciones distribuidas en 2 o más datacenters.				
Debe funcionar como un servidor DNS autoritativo de alto desempeño, permitiendo manejar un dominio completo o delegación de parte de un dominio. Debe ser autónomo sin necesidad de balancear requerimientos DNS a una granja de servidores				
Debe funcionar como un servidor DNS cache autónomo, sin necesidad de balancear requerimientos DNS a una granja de servidores				
Debe permitirlos siguientes métodos de balanceo estático y dinámico: Round Robin Global Availability Application Availability Geolocalización Virtual Server Capacity Least Connections Packets Per Second Round Trip Time Hops Packet Completion Rate User-defined QoS Dynamic Ratio Ratio Kilobytes Per Second				
Debe manejar persistencia a nivel global, manteniendo a los usuarios en un mismo datacenter por el transcurso de su sesión				
Permitir Balanceo de cargas ente datacenters de acuerdo a la ubicación geográfica				
Debe permitir la creación de topologías personalizadas con el fin de permitir distribución de tráfico por topología que concuerde con la infraestructura interna				
Debe permitir monitoreo de la infraestructura y las aplicaciones, integrándose con otros equipos del mismo fabricante o de terceros.				
Las zonas del DNS Autoritativo deben cargarse en RAM, para evitar latencias y tener tiempos de respuesta rápidos				
Debe permitir realizar balanceo de servidores DNS.				
Debe soportar el protocolo DNSSEC				

Debe incluir herramienta de administración grafica para el manejo de zonas DNS				
Debe soportar registros AAAA para IPv6				
Debe soportar traducción entre DNS IPv4 y DNS IPv6				

Ítem 3.5. Funciones de firewall y anti-DDOS para sedes calle 100 y Cajicá	**CUMPLE**		**FOLIO**	**OBSERVACIONES**
	SI	**NO**		
Debe incluir protección contra ataques de DDoS en capas 2-4 utilizando vectores de ataque personalizables				
Debe bloquear ataques a nivel de red como flood, sweep, teardrop, smurfattacks				
Debe mitigar ataques basados en protocolos, incluyendo SYN, ICMP, ACK, UDP, TCP, IP, DNS, ICMP, ARP				
Opcionalmente debe soportar un sistema de suscripción de reputación IP para prevenir conexiones bidireccionales (entrantes y salientes) a direcciones IP no confiables y agrupadas en categorías.				
Debe permitir la creación de reglas basadas en aplicación, independientes para cada una de ellas.				
Debe permitir la creación de reglas globales.				
Debe tener la opción de funcionar como un firewall statefull full-proxy.				
Debe permitir la definición de horarios (schedules) que apliquen a las reglas configuradas, permitiendo activar reglas Entre intervalos de tiempo Hasta una fecha específica Después de una fecha específica.				
Debe soportar e incluir Geolocalización de direcciones IP				
Debe permitir la creación de listas blancas (White lists) de direcciones IP				
Debe permitir la configuración de túnel IPSECSite-to-Site				
Debe incluir funcionalidad de applicationdeliverycontroller o integrarse con dispositivos de ApplicationDelivery				
Debe brindar protección contra Ataques de Denegación de Servicio para el protocolo DNS, poder controlar el tráfico DNS de acuerdo al tipo de Registro solicitado y detectar anomalías a nivel del protocolo				
Debe brindar protección contra Ataques de Denegación de Servicio para el protocolo SIP y poder controlar el tráfico SIP de acuerdo al Método SIP recibido y detectar anomalías a nivel del protocolo				
Debe permitir personalizar los Logs, y ser exportados a un repositorio Syslog externo que conste de uno o varios servidores.				

Ítem 3.6. Web application firewall (WAF) para sedes calle 100 y Cajicá	**CUMPLE**		**FOLIO**	**OBSERVACIONES**
	SI	**NO**		
La solución debe incluir funcionalidad de Firewall de Aplicaciones (WAF) en la misma caja, no debe ser un appliance independiente.				
Debe trabajar en un esquema proxy TCP reverso y/o transparente				
Debe soportar la creación automática de políticas				
La creación automática de políticas deberá unificar múltiples Urls explícitas utilizando wildcards de manera de reducir la cantidad de objetos en la configuración.				
Debe trabajar en modo de bloqueo o en modo informativo				

Debe permitir diferentes políticas de seguridad para diferentes aplicaciones				
Debe permitir la creación de firmas personalizadas				
Debe trabajar con modelos de seguridad positiva y negativa				
Debe poder aprender el comportamiento de la aplicación automáticamente sin intervención humana				
Debe permitir personalizar las páginas de bloqueo incluyendo la capacidad de responder a webservices mediante un código HTTP 500.				
Debe prevenir exponer el "OS fingerprinting"				
Debe permitir la integración con Herramientas de verificación de vulnerabilidades, en particular WhiteHat, Cenzic, Qualys, IBM AppScan, HP WebInspect.				
El WAF Debe soportar: Restringir protocolo y versión utilizada multi-byte languageencoding Validar URL-encodedcharacters Restringir la longitud del método de request Restringir la longitud del URI solicitado Restringir el número de Encabezados (headers) Restringir la longitud del nombre de los encabezados Restringir la longitud del valor de los encabezados Restringir la longitud del cuerpo (body) de la solicitud Restringir la longitud del nombre y el valor de las cookies Restringir el número de cookies Restringir la longitud del nombre y valor de los parámetros Restringir el número de parámetros				
El WAF Debe incluir protección a Web Services XML y restringir el acceso a métodos definidos vía Web ServicesDescriptionLanguage (WSDL)				
El WAF debe incluir protección contra el Top 10 de ataques definidos en OWASP				
El WAF debe incluir protección contra Web Scraping				
Debe ser Session-aware es decir identificar y forzar que el usuario tenga una sesión e identificar los ataques por usuario				
Permitir la definición y detección de las condiciones a cumplir para que una aplicación externa que vía Java realiza un requerimiento cross-domian, permitiendo evitar un CORS (Cross-OriginResourceSharing).				
Debe permitir verificar las firmas de ataque en las respuestas del servidor al usuario				
Debe permitir el enmascaramiento de información sensible filtrada por el servidor				
Debe poder bloquear basado en la ubicación geográfica e incluir la base de datos de geolocalización.				
Debe permitir la integración con servidores Antivirus por medio del protocolo ICAP				
Debe brindar reportes respecto a la normativa PCIDSS 2.0				
Debe integrarse con Firewall de Base de Datos: Oracle Database Firewall IBM InfoSphereGuardium				
Debe proteger contra ataque DoS /DDoS de Capa 7				
Una vez detectado un ataque deberá ser posible descartar todos los paquetes que provengan de una dirección IP sospechosa				
En caso de detectarse un ataque se requiere tener la posibilidad de iniciar una captura de tráfico (tipo tcpdump) para poseer información forense.				
Debe soportar tecnologías AJAX y JSON				
Debeprotegercomomínimo: Ataques de FuerzaBruta Cross-site scripting (XSS) Cross Site Request Forgery SQL injection Parameter and HPP tampering Sensitive information leakage Session highjacking Buffer overflows Cookie manipulation Various encoding attacks Broken access control Forceful browsing Hidden fields manipulation Request smuggling XML bombs/DoS Open Redirect				

Debe poder identificar y configurar Urls que generen un gran consumo de recursos en los servidores como método de protección de ataques de denegación de servicios.				
Debe permitir verificaciones de seguridad y validación a protocolos FTP y SMTP				
Debe permitir comparar dos políticas de seguridad y mostrar las diferencias entre ambas				
El equipo debe soportar bases de datos de reputación de IP que permita bloquear tráfico desde y hacia direcciones IP en categorías como: Scanners Exploits Windows Denial of Service Proxies de Phishing Botnets Proxies anónimos				

Ítem 3.7. Funciones de acceso para sedes calle 100 y Cajicá	**CUMPLE**		**FOLIO**	**OBSERVACIONES**
	SI	**NO**		
El equipo debe soportar la implementación de VPN SSL				
Entre los métodos soportados deben incluir un modo "Portal" donde la máquina se comporte como un proxy reverso, buscando los contenidos de portales web internos y presentarlos como vínculos seguros en el portal del usuario				
Entre los métodos soportados deben incluir un modo de "Network", donde un usuario se conecta a la red interna obteniendo una dirección IP enrutable dentro de la red interna				
Proporcionar un acceso remoto seguro a toda la red para cualquier aplicación basada en IP (TCP o UDP)				
Soporte de Split Tunnel, solo el trafico especificado debe ir por VPN				
Soportar túneles de aplicación, donde únicamente una aplicación en particular tenga acceso a los recursos de red				
Soporte de compresión HTTP.				
Permitir establecimiento de una conexión segura para el acceso remoto sin la necesidad de instalar software de cliente en la máquina del usuario				
Permitir un transporte seguro utilizando encapsulamiento DTLS (Datagramas TLS)				
Posibilidad de personalizar la página de acceso de usuario, portal, y mensajes de pre-inicio de sesión presentados al usuario				
Incluir licencias para mínimo 500 usuarios simultáneos VPN SSL				
El equipo suministrado debe soportar un crecimiento de al menos 60000 usuarios concurrentes VPN SSL, que se pueden habilitan por medio de licencias adquiridas a futuro				
El equipo debe tener soporte para Single-Sign-On (SSO)				
El equipo deberá ser capaz de solicitar las credenciales de usuario sólo una vez, y autenticar al usuario en todos los portales que requieran autenticación				
El equipo debe ser capaz de almacenar en caché todas las credenciales del usuario y utilizar las credenciales adecuadas en cada portal (por ejemplo, algunos portales requieren correo electrónico como nombre de usuario, otros requieren el usuario de Dominio/ AD).				
La solución es incluir soporte para la validación de la estación del usuario. Debe validar por lo menos: Presencia de anti-virus y que este actualizado Presencia de Firewall personal Presencia de los procesos ejecutándose en el equipo Presencia de los certificados digitales instalados en la máquina Presencia de archivos en el equipo Búsqueda de entradas de registro en clientes Windows Verificación de Sistema Operativo Identificación de hardware del equipo CPU Motherboard Numero Serial BIOS MAC Address				

Para cada elemento de la validación de la estación del usuario, debe ser posible configurar una acción a tomar si la prueba es satisfactoria o no.				
La configuración de estas acciones debe ser a través de una interfaz gráfica y fácil de entender				
El sistema debe ser capaz de verificar la ubicación geográfica de las direcciones IP, lo que permite la creación de reglas de acceso en función del país o del estado				
La base de datos de direcciones IP debe estar presente en la caja, y debe ser periódicamente suministrada por el fabricante de la solución sin coste adicional				
La solución debe ser capaz de autenticar a los usuarios contra sistemas LDAP, LDAPS, RADIUS, TACACS+, Directorio Activo, HTTP, RSA, OCSP, CRLDP				
La solución debe soportar limpieza de cache del lado del cliente final				
La solución debe permitir la creación de un Entorno Protegido para los usuarios donde no se permita la creación de archivos fuera del entorno.				
La solución debe ser compatible con múltiples factores de autenticación que utiliza tokens de hardware				
La solución debe soportar el uso de un cliente stand-alone incluido con la solución				
El cliente stand-alone debe ser capaz de hacer Roaming inteligente, donde el cambio de dirección IP no implica re-autenticación manual del usuario sin importar el tipo de enlace utilizado. (Punto de Acceso WiFi, 3G, etc.)				
El cliente stand-alone debe soportar Windows, Linux, MAC OS, iOS, Android				
Debe soportar Single-Sign-On utilizando Security AssertionMarkupLanguage (SAML) 2.0 funcionando como identityprovider (IdP) y/o serviceprovider (SP).				
La solución debe integrarse con Oracle Access Manager				
La solución debe integrarse con VMwareHorizon y funcionar como proxy PCOIP				
La solución debe integrarse con Citrix XenApp y Citrix XenDesktop y funcionar como proxy ICA				

Ítem 3.8. Estándares de red para sedes calle 100 y Cajicá	**CUMPLE**		**FOLIO**	**OBSERVACIONES**
	SI	**NO**		
Soporte VLAN 802.1q, Vlantagging				
Soporte de 802.3ad para definición de múltiples troncales				
Soporte de NAT, SNAT				
Soporte de IPv6: El equipo debe funcionar como Gateway entre redes IPv6 e IPv4 permitiendo tener ambos tipos de redes simultáneamente.				
Soporte de RateShapping.				
Soporte de dominios de Enrutamiento, donde cada uno pueda tener su propio Default Gateway y estar conectados a redes IP con el mismo direccionamiento.				
Debe soportar VXLAN, VXLAN Gateway, NVGRE y Transparent Ethernet Bridging para entornos de redes virtualizadas.				

Ítem 3.9. Administración del sistema para sedes calle 100 y Cajicá	**CUMPLE**	**FOLIO**	**OBSERVACIONES**

	SI	NO		
La solución debe permitir 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 de integrarse con Directorio Activo Windows 2003 o superior, LDAP, RADIUS.				
La solución debe incluir comunicación cifrada y permitir la autenticación del equipo y de los usuarios administradores/supervisores con Certificados Digitales				
La solución debe soportar el envío de alertas y eventos a un Sistema Centralizado mediante: Protocolo SysLog Notificación vía SMTPSNMP versión.2.0 o superior.				
El sistema de administración debe ser totalmente independiente del sistema de procesamiento de tráfico.				
El equipo debe contar con un módulo de administración tipo lightsout que permita encender/apagar el sistema de manera remota y visualizar el proceso de arranque.				
La interfaz gráfica debe contar con un Dashboard personalizable que permita monitorear el estado del equipo en tiempo real				
Debe contar con un módulo de reportes que permita visualizar gráficamente el comportamiento de las aplicaciones HTTP como latencias hacia los servidores, latencias en los URL, Direcciones IPs que acceden las aplicaciones, Urls más visitados en las aplicaciones, Throughput hacia los servidores y estadísticas acerca de los servicios creados y los servidores físicos.				
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.				

Ítem 3.10. Virtualización para sedes calle 100 y Cajicá	**CUMPLE**		**FOLIO**	**OBSERVACIONES**
	SI	**NO**		
Cada equipo debe soportar virtualización del dispositivo que soporte mínimo 8 instancias del sistema operativo corriendo simultáneamente (StrictIsolation), cada una con CPU y Memoria independientes.				
Cada instancia virtual debe permitir diferentes versiones del sistema operativo				
La solución debe permitir configurar clúster entre chasis o equipos de rack con el fin de contar con un sistema altamente escalable y en demanda que permita hacer failover de uno o más servicios hacia cualquier equipo miembro del clúster.				

Ítem 4. Otros requerimientos para sedes calle 100 y Cajicá	**CUMPLE**		**FOLIO**	**OBSERVACIONES**
	SI	**NO**		
La solución debe permitir configurar clúster entre chasis o equipos de rack con el fin de contar con un sistema altamente escalable y en demanda que permita hacer failover de uno o más servicios hacia cualquier equipo miembro del clúster.				
1 año de Garantía de fábrica				
3 Años en modalidad 7x24x4 de Tiempo de Servicios de				

reposición de partes y piezas (Hardware)				
Tiempo máximo de respuesta a llamadas de servicio técnico para reposición de Hardware de 4 horas en modalidad 7x24x4 Proactivo, una vez confirmado el daño de la parte y la necesidad de reposición				
Tiempo de Servicios de actualización del sistema operativo (Software) y Sistema de gestión 3 años en modalidad 7x24x4				
El oferente deberá adjuntar en su propuesta una hoja de vida de un ingeniero especialista en networking para que lidere las actividades de instalación e integración con la red actual, con certificación técnica a nivel de especialización (Cisco CCIE, HP MASE, Juniper JNCIE-ENT). Esto con el fin de garantizar la calidad en la integración de los productos ofrecidos.				
El oferente debe ser partner Gold o nivel superior, además de estar autorizado en Colombia por el fabricante de los equipos ofertados y estar en capacidad técnica de configurar mantener y dar soporte técnico de los equipos. En consecuencia el oferente deberá presentar documentación que lo acredite como partner de la marca, documento que debe ser expedido por el fabricante de los equipos ofertados.				
El contratista deberá realizar capacitaciones oficiales (impartidas por fabricante) del producto ofrecido para los módulos de Administración, DDoS, Balanceo de Datacenter y Protección de aplicaciones en capa 7, cada capacitación deberá ser independiente y el plan de estudio deberá ser aprobado por la entidad				