INVITACIÓN PRIVADA No. 8103

1. GENERALIDADES.

1.1. ANTECEDENTES.

La Camara de Comercio de Bucaramanga está interesada en contratar una solución de Firewalls de Nueva Generación en un esquema de alta disponibilidad, que funcione adicionalmente como Wirelles Controller para los Access point con los que cuenta actualmente la entidad. Las soluciones deben ser postuladas en modalidad de compra de hardware a 1 año. El objetivo es contar con soluciones de seguridad informática estables y posicionadas en el mercado, así mismo poder administrar la red wifi de la entidad, a través de un proveedor que brinde un soporte oportuno y efectivo ante los incidentes, fallas, cambios de configuración y afinamientos.

1.2. OBJETO DE LA CONTRATACIÓN.

Adquisición y configuración de una solución Firewall de nueva generación (NGFW) en alta disponibilidad, que funcione adicionalmente como Controladora inalámbrica (WLC) para los puntos de acceso inalámbrico con los que cuenta actualmente la entidad

1.3. ALCANCE.

De acuerdo con el proyecto de seguridad y de red Inalámbrica que busca mitigar los riesgos asociados a la infraestructura crítica de la Camara de Comercio de Bucaramanga se plantea tener plataformas de seguridad y red robustas y de alto rendimiento con los últimos estándares de seguridad a costos razonables por el oferente

GENERALIDADES

Ítem	Requerimiento Técnico Mínimo (de obligatorio cumplimiento)
	• Las soluciones que se presenten en esta oferta deben ser postuladas en modalidad de compra a 1 año garantizando que la totalidad de servicios conexos se encuentren incluidos. • El oferente deberá realizar un análisis de la arquitectura de red actual, con el fin de aplicar las mejores prácticas para la implementación. • El proponente con su oferta deberá entregar una carta de certificación del fabricante donde indique las plataformas ofertadas.

FIREWALLS DE NUEVA GENERACION

1. SOLUCION DE DOS FIREWALL DE NUEVA GENERACIÓN EN HA

MARCA	
MODELO	
1.	**Generalidades.**
	Adquisición de dos (2) sistema de seguridad informática perimetral e interna que sea del tipo Firewall de Nueva Generación, donde se deberán ofrecer ya incluidas y listas para ser utilizadas, las funcionalidades que se detallan en el presente documento.
	La solución debe estar en la capacidad de soportar alta disponibilidad.
	El dispositivo debe ser un equipo de propósito específico.
	El dispositivo debe contar con tecnología ASIC para permitir acelerar los procesos (no solo por CPU) y de esta manera permita mejorar el rendimiento del procesamiento de trafico
	Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PCs o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN solaris, Apple OS-X o GNU/Linux.
	Los firewalls de nueva generación deberán cumplir también la funcionalidad de controladora inalámbrica (WLC) para los puntos de acceso inalámbrico con los que cuenta actualmente la entidad.
	El equipo deberá poder ser configurado en modo Gateway o en modo transparente en la red.
	El equipo debe entregar en tiempo real estadísticas de usuarios, aplicaciones, seguridad. Presentar preferiblemente en formato de drilldown este tipo de información donde sea posible por usuario verificar que aplicaciones, sitios, categorías y amenazas de seguridad se han tenido en un tiempo de 24 horas.
	La plataforma debe tener la capacidad de poder permitir observar el consumo de ancho de banda en tiempo real por usuario, fuente IP, aplicación y páginas web. Con el fin de detectar algún tipo de problema referente a consumos altos de ancho de banda.
	Debe tener la capacidad de generar un widget de visualización, una vez se realiza el filtro de algún tipo de búsqueda especifica
	La solución deberá pertenecer al cuadrante de líder de gartner para UTM y NGFW
	La solución deberá estar calificada como recomendada en el SVM de firewall de NSS LABS
2.	**Rendimiento**
	El equipo deberá cumplir con las siguientes características mínimas de desempeño ya activas y funcionales:
	• Rendimiento de Firewall 35.8 Gbps
	• Rendimiento de IPS 10 Gbps
	• Rendimiento de NGFW (FW + IPS + Control de Aplicaciones) 9.5 Gbps
	• Rendimiento Protección de amenazas (FW + IPS + Control de Aplicaciones + AntiMalware) 6.8 Gbps
	• Rendimiento IPSec VPN 20 Gbps
	• Soporte de 8 Millones sesiones concurrentes
	• Rendimiento de Inspección SSL 8 Gbps
	• Soporte de 10000 usuarios VPN SSL
	• Rendimiento de VPN SSL 6.8 Gbps
	• Disco Duro Interno: mínimo requerido 476 GB
3.	**Conectividad**
	El equipo deberá contar con las siguientes interfaces de conexión:
	• 10 interfaces de 1 Gbps RJ45
	• 8 interfaces de 1 Gbps SFP
	• 2 interfaces de 10 Gbps SFP+
	Aprovisionamiento transceiver:
	• 2 Modulos de transceiver de 10 GE SFP+.

	• 8 Modulos de transceiver de 1 GE SFP
4.	**Address Traslation**
	La plataforma debe soportar lo siguiente tipos de traducción de direcciones:
	• NAT y PAT
	• NAT estático
	• NAT: destino, origen
	• NAT, NAT64 persistente
5.	**Funciones básicas de Firewall**
	Las reglas de firewall deben analizar las conexiones que pasen por el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.
	La solución debe integrarse con el directorio activo y soportar políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios.
	La solución soportará políticas basadas en dispositivo. Esto Significa que podrán definirse políticas de seguridad de acuerdo al dispositivo (movil, laptop) que tenga el usuario. Esta característica no deberá incurrir en ningún tipo de licenciamiento adicional que ocasiones costos adicionales para la entidad.
	Debe ser posible hacer políticas basados en usuarios, grupos de usuarios y dispositivos sobre una misma política, y ser lo mas granular posible en la definición de políticas.
	Debe contar con una herramienta de búsqueda de políticas por medio del GUI (Graphical User Interface). que determine cual política procesara un flujo de datos dado (Resaltando la política que coincide), usando distintos parámetros como IP de origen, destino, servicio, protocolo, interface de fuente entre otros
	Debe tener la capacidad de generar una advertencia al administrador cuando este configure una política duplicada
	Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén predefinidos.
	Debe estar en la capacidad de integrase con plataforma Cloud IaaS como: AWS,Azure,Google etc. Con el fin de generar y actualizar objetos de direcciones de manera automática basado en los parámetros de red (IP,TAG etc) de la instancias desplegadas en la nube y estas ser usadas como objetos de reglas o políticas de firewall
	Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface) como por GUI (Graphical User Interface).
	La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP
	El dispositivo será capaz de crear e integrar políticas contra ataques DoS (Denial of service) las cuales se deben poder aplicar por interfaces
	El dispositivo será capaz de ejecutar inspección de tráfico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico.
	Tendrá la capacidad de hacer escaneo a profundidad de tráfico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis.
	Tener la capacidad de utilizar objetos de direcciones para ser utilizados en el enrutamiento con el fin de facilitar la administración y la visibilidad.
	Debe estar en la capacidad de dar estadísticas de uso por políticas como: Ancho de banda actual, Sesiones activas, Ultimo vez usada.
6.	**Conectividad y Enrutamiento**
	Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP.
	Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs.
	Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.
	Soporte a políticas de ruteo (policy routing)

	Soporte a ruteo dinámico RIP V1, V2, OSPF y BGP
	Soporte a ruteo dinámico RIPng, OSPFv3.
	Soporte de ECMP (Equal Cost Multi-Path) o balanceo de enlaces WAN por medio de lo siguiente métodos.
	Sesiones
	IP Fuente
	Volumen
	Spillover
	Soporte de reglas que permitan dirigir un tráfico especifico a través de un enlace WAN, ya sea por destino, aplicación (adobe,Facebook,youtube), servicio o fuentes (IP, Usuario)
	Soporte a ruteo de multicast PIM SM y PIM DM.
	La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow o Netflow.
	La solución podrá habilitar políticas de ruteo en IPv6
	La solución deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6.
	La solución debe contar con una herramienta de búsqueda de rutas por medio del GUI (Graphical User Interface) sobre la tabla de enrutamiento, con el fin facilitar la lectura y control de la tabla de enrutamiento usando parámetros de destino ya sea IP o FQDN
	La Solución deberá soportar balanceado de enlaces WAN inteligente (SD-WAN Seguro) sin licencia adicional basado en:
	Aplicaciones cloud
	SLA
	Mejor calidad de enlace basado en (Jitter, latencia, ancho de banda, perdida de paquetes)
	Integrar en una única interface lógica distintos tipos de enlaces WAN físicos para permitir balanceo de los mismos
7.	**VPN IPSEC**
	El equipo deberá soportar las siguientes características:
	Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site).
	Soporte para IKEv2 y IKE Configuration Method.
	Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES
	Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14.
	Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256.
	Posibilidad de crear VPN's entre gateways y clientes con IPSec. VPNs IPSeC site-to-site y VPNs IPSec client-to-site.
	La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN).
	En modo interface, la VPN IPSec deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de firewall.
	Deberá tener la capacidad de crear conexiones VPNs por demanda (ADVPN), con el fin de permitir la fácil gestion de topologías Hub-Spoke y estas puedan convertirse en full-mesh al momento de comunicaciones directas entre Spokes.
8.	**VPN SSL**
	Capacidad de realizar SSL VPNs por usuarios sin incurrir en costos adicionales.
	Soporte a certificados PKI X.509 para construcción de VPNs SSL.
	Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de VPN.
	Soporte de autenticación de dos factores con token, la solución debe estar en la capacidad de suplir o integrarse con tokens físicos, basados en software, SMS o correo

	Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet.
	Deberá poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL.
	La VPN SSL integrada deberá soportar a través de algun plug-in ActiveX y/o Java, la capacidad de poner dentro del túnel SSL tráfico que no sea HTTP/HTTPS
	Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL
	Deberá soportar la redirección de página http a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente.
	Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo al grupo de pertenencia de dichos usuarios
	Los portales personalizados deberán soportar al menos la definición de:
	Widgets a mostrar
	Aplicaciones nativas permitidas. Al menos: HTTP, CIFS/SMB, FTP, VNC
	Soporte para Escritorio Virtual
	Política de verificación de la estación de trabajo
	La VPN SSL integrada debe soportar la funcionalidad de Escritorio Virtual, entendiéndose como un entorno de trabajo seguro que previene contra ciertos ataques además de evitar la divulgación de información.
9.	**Autenticación**
	El dispositivo deberá manejar los siguientes tipos de autenticación:
	Capacidad de soporta autenticación local y remota integrándose con Servidores de Autenticación RADIUS ,LDAP o TACACS+.
	Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es aprovechar las credenciales del dominio de Windows bajo un concepto “Single-Sign-On”.
	Soporte de Token Físicos o Mobile sobre Smartphone basado en IOS o Android, token de SMS, email o con plataformas de terceros como RSA SecurID.
	Soporte autenticación de usuario a través de PKI y certificados.
	Capacidad de soportar autenticación de acceso de usuario a través de 802.1x y portal cautivo.
10.	**Manejo de tráfico y calidad de servicio.**
	Capacidad de poder asignar parámetros de traffic shapping atreves de reglas de manera independiente
	Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión
	Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación y categoría URL de las mismas para la regla en general.
	Capacidad de poder definir ancho de banda garantizado en Kilobits por segundo
	Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en Kilobits por segundo
11.	**Antimalware**
	Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP.MAPI
	El módulo de antimalware debe haber sido desarrollado por el mismo fabricante de la solución de firewall, así como las firmas deberán ser de su propiedad y no por medio de licenciamiento o concesiones de un tercero, esto con el fin de garantizar la idoneidad de la protección, así como los tiempos de respuesta del soporte de la misma.

	Debe soportar la inspección de archivos comprimidos como los son: GZIP,RAR,LZH,IHA,CAB,ARJ;ZIP entre otros con el fin de proteger contra estas técnicas de evacion.
	El Antivirus deberá poder configurarse de forma que los archivos que pasan sean totalmente capturados y analizados, permitiendo hacer análisis sobre archivos que tengan varios niveles de compresión.
	El Antivirus deberá integrarse de forma nativa con una solución sandbox del mismo fabricante, de tal manera que envíen muestras de archivos a dicho dispositivo para su análisis.
	Antivirus en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.
	El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6.
	La configuración de Antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP deberá estar completamente integrada a la administración del dispositivo appliance, que permita la aplicación de esta protección por política de control de acceso.
	El antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging).
	La solución debe incluir mecanismos para detectar y detener conexiones a redes Botnet y servidores C&C.
12.	**Filtrado WEB**
	Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 78 categorías y por lo menos 47 millones de sitios web en la base de datos.
	Debe poder categorizar contenido Web requerido mediante IPv6.
	La solución debe permitir realizar el filtrado de contenido, tanto realizando reconstrucción de toda la sesión como realizando inspección paquete a paquete sin realizar reconstrucción de la comunicación.
	Capacidad de filtrado de scripts en páginas web (JAVA/Active X).
	La solución de Filtrado de Contenido debe soportar el forzamiento de "Safe Search" o "Búsqueda Segura" independientemente de la configuración en el browser del usuario. Esta funcionalidad no permitirá que los buscadores retornen resultados considerados como controversiales. Esta funcionalidad se soportará al menos para Google, Yahoo! y Bing.
	Será posible exceptuar la inspección de HTTPS por categoría.
	Debe contar con la capacidad de restringir contenido de youtube usando restricción strict o Moderate por medio del perfil de Filtro de Contenido para trafico HTTP, garantizando de manera centralizada, que todas las sesiones aceptadas por una política de seguridad con este perfil, van a poder acceder solamente a contenido Youtbube configurado por el administrador de la cuenta, bloqueando cualquier tipo de contenido distinto al permitido
	Debe contar con la capacidad de bloquear contenido de youtube usando el Channel ID
	La solucion debe permitir controlar el acceso a sitios web por medio de palabras o patrones que se encuentren dentro de su contenido.
	El sistema de filtrado de URLs debe incluir la capacidad de definir cuotas de navegación basadas en volumen de tráfico consumido.
	El sistema de filtrado URL debe incluir la capacidad de no solo poner una entrada URL de manera simple si no que también por medio de metacaracteres (Wildcards o regular expressions)
	La solución debe poder aplicar distintos perfiles de navegación de acuerdo al usuario que se esté autenticando. Estos perfiles deben poder ser aplicados a usuarios o grupos de usuarios.
	La solución debe estar en la capacidad de filtrar el acceso a cuentas de google, permitiendo acceso solo a cuentas corporativas de google.
	El filtrado debe ser sobre tráfico http y https.
13.	**Protección contra intrusos (IPS)**

	El sistema de detección y prevención de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror.
	Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores.
	Capacidad de detección de más de 7000 ataques.
	Capacidad de actualización automática de firmas IPS mediante tecnología de tipo “Push” (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo “pull” (Consultar los centros de actualización por versiones nuevas)
	El sistema de detección y prevención de intrusos deberá estar integrado a la plataforma de seguridad “appliance”. Sin necesidad de instalar un servidor o appliance externo, La interfaz de administración del sistema de detección y prevención de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso.
	El sistema de detección y prevención de intrusos deberá soportar captar ataques por variaciones de protocolo y por firmas de ataques conocidos (signature based / Rate base). Basado en análisis de firmas en el flujo de datos en la red, y deberá permitir configurar firmas nuevas para cualquier protocolo.
	Actualización automática de firmas para el detector de intrusos
	El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios.
	Métodos de notificación:
	Alarmas presentadas en la consola de administración del appliance.
	Alertas vía correo electrónico.
	Debe tener la capacidad de cuarentena, prohibir el tráfico subsiguiente a la detección de un posible ataque. Esta cuarentena debe poder definirse al menos para el tráfico proveniente del atacante o para el tráfico del atacante al atacado.
	La capacidad de cuarentena debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. También podrá definirse el bloqueo de forma “indefinida”, hasta que un administrador tome una acción al respecto.
	Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP.
14.	**Control de Aplicaciones**
	La solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.
	La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.
	La solución debe tener un listado de al menos 3000 aplicaciones ya definidas por el fabricante.
	El listado de aplicaciones debe actualizarse periódicamente.
	Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log y resetear conexión
	Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.
	Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping.
	Preferentemente deben soportar mayor granularidad en las acciones.
	Debe ser posible inspeccionar aplicaciones tipo Cloud como dropbox, icloud entre otras entregando información como login de usuarios y transferencia de archivos.
15.	**Inspección de Contenido SSL/SSH**

	La solución debe soportar inspeccionar tráfico que esté siendo encriptado mediante SSL al menos para los siguientes protocolos: HTTP, IMAP, SMTP, POP3 y FTP en su versión segura
	Debe ser posible definir perfiles de inspección SSL donde se definan los protocolos a inspeccionar y el certificado usado, estos perfiles deben poder ser escogidos una vez se defina la política de seguridad.
	Debe ser posible definir si la inspección se realiza desde múltiples clientes conectando a servidores (es decir usuarios que navegan a servicios externos con SSL) o protegiendo un servidor interno de la entidad.
	Para el caso de URL Filtering, debe ser posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones deben poder determinarse al menos por Categoría de Filtrado.
	El equipo debe ser capaz de analizar contenido cifrado (SSL o SSH) para las funcionalidades de Filtrado de URLs, Control de Aplicaciones, Prevención de Fuga de Información, Antivirus e IPS
	Debe ser posible inspeccionar tráfico SSH funcionalidades como Port-Fortward o X11.
16.	**Alta Disponibilidad**
	Los dispositivos deberán soportar Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6
	Alta Disponibilidad en modo Activo-Activo de forma automática sin requerir hacer políticas de enrutamiento basado en orígenes y destino para poder hacer la distribución del tráfico.
	Posibilidad de definir al menos dos interfaces para sincronía
	El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red
	Debe ser posible definir interfaces de gestión independientes para cada miembro en un clúster.
	Debe ser posible definir que Firewall Virtual estará activo sobre un miembro del Cluster para hacer una distribución de carga en caso de ser necesario.
	El equipo debe soportar hasta 4 equipos en esquema de HA.
17.	**Visibilidad**
	La solución debe estar en la capacidad de visualizar el tráfico de usuario, aplicaciones, navegación y niveles de riesgo en tiempo real, esto deberá ser sobre la misma plataforma sin necesidad de software o licenciamiento adicional.
	Menú tipo dropdown para navegar por la información.
	Visualización de las sesiones top 100
	Mostrar los orígenes del tráfico o usuarios que lo generan.
	Mostrar las aplicaciones y su categorización según riesgo.
	Visibilidad de aplicaciones Cloud usadas por el usuario.
	Visibilidad de Destinos del tráfico.
	Visibilidad de los sitios web más consultados por los usuarios.
	Visibilidad de las amenazas o incidentes que han ocurrido o estén ocurriendo en la red
	En la información de sources, aplicaciones, navegación debe ser posible con un doble-click filtrar la información para ser más específica la búsqueda.
	Se debe ver aplicaciones, sitios, amenazas por cada usuario.
	Se debe ver el ancho de banda que se esta consumiendo en tiempo real por cada fuente, destino, sitio web, aplicación etc. Con el fin de tener una clara visión del consumo.
	Deber tener la capacidad de poder validar con que política la sesión se esta coincidiendo y un link hacia la misma.
	De las aplicaciones Cloud como Dropbox que permiten compartir archivos, debe ser posible ver que archivos fueron subidos y descargados por los usuarios.
	De aplicaciones de contenido como youtube debe ser posible ver que videos fueron vistos por los usuarios.

	Debe tener la capacidad de generar un diagrama de conexión lógicas. En el cual se visualice la plataforma y los equipos conectados a ella (por medio del tráfico que los mismos generan)
18.	**Características de Administración**
	Interface gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interface debe soportar SSL sobre HTTP (HTTPS)
	Interface basada en línea de comando (CLI) para administración de la solución.
	Puerto de consola dedicado para administración. Este puerto debe estar etiquetado e identificado para tal efecto.
	Comunicación cifrada y autenticada con usuario y contraseña, tanto como para la interface gráfica de usuario como la consola de administración de línea de comandos (SSH)
	El administrador del sistema podrá tener las opciones incluidas de autenticarse vía usuario/contraseña y vía certificados digitales.
	El equipo ofrecerá la flexibilidad para especificar que los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet, Http o Https.
	El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional.
	Soporte de SNMP versión 2
	Soporte de SNMP versión 3
	Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos
	Soporte de Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall.
	Monitoreo de comportamiento del appliance mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red.
	Debe ser posible definir la dirección IP que se utilizará como origen para el tráfico iniciado desde el mismo dispositivo. Esto debe poder hacerse al menos para el tráfico de alertas, SNMP, Log y gestión.
	Permitir que el administrador de la plataforma pueda definir qué funcionalidades están disponibles o deshabilitadas para ser mostradas en la interfaz gráfica.
	Contar con facilidades de administración a través de la interfaz gráfica como ayudantes de configuración (setup wizard).
	Contar con la posibilidad de agregar una barra superior (Top Bar) cuando los usuarios estén navegando con información como el ID de usuario, cuota de navegación utilizada, y aplicaciones que vayan en contra de las políticas de la empresa.
	Contar con herramientas gráficas para visualizar fácilmente las sesiones en el equipo, incluyendo por lo menos por defecto Top de sesiones por origen, Top de sesiones por destino, y Top de sesiones por aplicación.
19.	**Virtualización**
	El dispositivo deberá poder virtualizar los servicios de seguridad mediante “Virtual Systems”, “Virtual Firewalls” o “Virtual Domains”
	La instancia virtual debe soportar por lo menos Firewall, VPN, URL Filtering, IPS.
	Cada instancia virtual debe poder tener un administrador independiente
	La configuración de cada instancia virtual deberá poder estar aislada de manera lógica del resto de las instancias virtuales.
	Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red
	Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual

	Debe ser posible definir distintos servidores de log (syslog) para cada instancia virtual.
	Debe ser posible definir y modificar los mensajes mostrados por el dispositivo de forma independiente para cada instancia virtual.
	Debe ser posible definir enlaces de comunicación entre los sistemas virtuales sin que el trafico deba salir de la solución por medio de enlaces o conexiones virtuales, y estas conexiones deben poder realizarse incluso entre instancias virtuales en modo NAT y en modo Transparente
	Se debe poder ver el consumo de CPU y memoria de cada instancia virtual.
20.	**Licenciamiento y actualizaciones**
	El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones,VPNs equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo.
	La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS, Application Control y URL Filtering debe proveerse por al menos 3 años.
	La plataforma es requerida por un periodo de tres (3) años en un esquema 7x24 ante el fabricante.
21.	**Funcionalidades de Wirelles Controller**
	Debe implementar mecanismos de protección para identificar ataques a la infraestructura inalámbrica (wIDS / wIPS);
	Debe permitir la conexión de dispositivos inalámbricos que implementen los estándares IEEE 802.11a / b / g / n / ac y que transmitan tráfico IPv4 e IPv6 a través del controlador;
	Debe permitir la creación de múltiples dominios de movilidad (SSID) con configuraciones distintas de seguridad y red;
	Debe implementar los siguientes métodos de autenticación: WPA (TKIP) y WPA2 (AES);
	La solución debe ser capaz de administrar puntos de acceso de tipo indoor y outdoor;
	La solución debe optimizar el rendimiento y la cobertura inalámbrica (RF) en los puntos de acceso administrados por ella, realizando automáticamente el ajuste de potencia y la distribución adecuada de canales a ser utilizados. La solución debe permitir además deshabilitar el ajuste automático de potencia y canales cuando sea necesario;
	El encaminamiento de tráfico de los dispositivos conectados a la red inalámbrica debe realizarse de forma centralizada a través del túnel establecido entre el punto de acceso y el controlador inalámbrico. En este modo todos los paquetes deben ser tunelados hasta el controlador inalámbrico;
	La solución debe implementar recursos que posibiliten la identificación de interferencias provenientes de equipos que operen en las frecuencias de 2.4GHz y 5GHz y que no sean compatibles con los estándares IEEE 802.11 (no WiFi);
	La solución debe permitir el equilibrio de carga de los usuarios conectados a la infraestructura inalámbrica de forma automática. La distribución de los usuarios entre los puntos de acceso cercanos debe ocurrir sin intervención humana y basada en criterios como número de dispositivos asociados en cada punto de acceso;
	La solución debe implementar la función de DHCP Server para facilitar la configuración de pequeñas redes de visitantes;
	Debe implementar el protocolo IEEE 802.1X con la asociación dinámica de VLAN para los usuarios en función de los atributos proporcionados por los servidores RADIUS;
	Debe admitir los siguientes métodos de autenticación EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS y PEAP;
	Cualquier licencia y / o software necesario para la plena ejecución de todas las características descritas en este término de referencia deberá ser suministrada;

3. SERVICIOS

1	**SERVICIO SOPORTE FABRICANTE** Todos los equipos propuestos por el proveedor deben contar con soporte otorgado por el fabricante, el cual incluya atención a incidentes, descarga de parches, actualización de software y firmware y garantía para los equipos 24 x 7 a 3 o 5 años. El esquema de soporte debe permitir que tanto el proveedor como puedan escalar directamente tickets y solicitudes de atención a fábrica.
2	**SERVICIOS DE IMPLEMENTACION** El proponente seleccionado deberá entregar implementada y funcionando la solución completa, de acuerdo con los requerimientos y políticas, tal como lo muestra la topología que se encuentra al inicio de este documento. Se deben considerar los siguientes parámetros para la implementación de los Firewalls de Nueva Generación: ➢ Instalación de los equipos en el rack ➢ Levantamiento de información para la configuración y políticas ➢ Configuración de las interfaces ➢ Actualización a la última versión estable disponible ➢ Creación de firewall virtuales, mínimo 2. ➢ Creación de zonas de seguridad. ➢ Creación de salidas a internet. ➢ Creación de políticas y perfiles de seguridad. ➢ Creación de VPNs. ➢ Pruebas de funcionamiento de controles de seguridad. ➢ Puesta en producción. ➢ Seguimiento. En general los servicios deben incluir: • Levantamiento de información • Entregar dentro los cinco (5) días hábiles del inicio del contrato, un plan de trabajo en el cual se indiquen las actividades a realizar y las fechas para la instalación de los equipos en modalidad de compra o servicios. • Configuración de las funcionalidades de NGFW (Firewall, VPN, filtrado de contenido, antivirus e IPS). • Transferencia de conocimiento de 8 horas para 3 empleados de la Compañía, orientada a explicar cómo quedaron configuradas las plataformas de seguridad y red, incluyendo nociones básicas de administración. • Flexibilidad en horarios para ventanas de procesos, pruebas, implementación y pasos a producción. • Mejores prácticas para integración de Directorio activo para la red corporativa.

	• Estudio de riesgos para el proceso de implementación respecto a servicios críticos de la organización. • Generación de ambiente de pruebas para migración.
3	**SERVICIOS DE SOPORTE PRIMER Y SEGUNDO NIVEL** El proponente seleccionado deberá prestar el servicio de soporte nivel 1 y 2 por un (1) año, en modalidad 7x24 con tiempo de respuesta máximo de 30 minutos para el primer contacto y una hora y media para obtener un diagnóstico de la falla o incidente. El objetivo principal de los servicios ofrecidos es brindar un soporte integral de primer y segundo nivel (siendo este el más alto) para las plataformas de seguridad informática y red. Este objetivo, incluye los siguientes objetivos específicos y alcance: • Cambios de configuración solicitados sin generarse ningún costo adicional. • Problemas existentes. • Configuración de los equipos para satisfacer las necesidades existentes. • Afinamiento de las tecnologías para obtener el mejor desempeño de la mismas. • Disponer un soporte de calidad, para realizar las actividades correctivas que garanticen la disponibilidad de los equipos.
6	**BANCO DE HORAS** El proveedor debe ofrecer un banco de 30 horas para el servicio de atención de casos no relacionados con fallas en las plataformas en horario 7x24.
7	**ADMINISTRACION DE LAS PLATAFORMAS OFERTADAS** El proponente deberá cotizar el servicio de administración de todas las plataformas ofertadas en el presente pliego. Este valor debe ser discriminado en la propuesta de forma mensual y el servicio deberá tener el siguiente alcance: • Administración con límite de veinte (20) cambios de configuración por mes por cada plataforma ofertada durante la vigencia del contrato. • Administración remota con disponibilidad 8 x 5 de un ingeniero con experiencia mínima de 3 años en implementación y administración de proyectos de seguridad informática y redes LAN y WLAN. • Disponibilidad 7 x 24 para atención de incidentes, fallas y ventanas de mantenimiento de cualquier plataforma ofertada.
8	**EQUIPO DE TRABAJO** El oferente debe contar con un equipo de trabajo para la ejecución del proyecto, el cual debe estar conformado por profesionales con experiencia en implementación, soporte y/o administración en soluciones de seguridad y/o red de la marca ofrecida de por lo menos dos (2) años. El personal propuesto debe estar certificado por el fabricante de la marca ofrecida, con el fin de garantizar que está vigente y que el personal tiene los conocimientos sobre las últimas versiones, equipos y funcionalidades liberadas por el fabricante. Se debe anexar la HV de los integrantes del equipo de trabajo.

1.4. RESULTADOS ESPERADOS Y ENTREGABLES.

El proveedor seleccionado se compromete a entregar los equipos instalados y configurados en la cámara de comercio de Bucaramanga carrera 19 # 36 - 20 según las especificaciones del numeral 1.3 Alcance y debe realizar la transferencia de conocimiento a 4 ingenieros de la unidad de tecnología de la cámara.

1.5. DURACIÓN DEL CONTRATO.

La duración prevista para la ejecución del contrato será en un tiempo máximo de tres (3) meses , contados a partir de la fecha de aprobación de garantías que se establezca, sí aplica .

2. REQUISITOS Y DOCUMENTOS DE LA PROPUESTA.

2.1. QUIÉNES PUEDEN PARTICIPAR.

En esta invitación privada podrán participar las personas que se señalan a continuación con una equis (**X**):

PERSONAS NATURALES	_____	**PERSONAS JURÍDICAS**	_____**X**_____

Las personas jurídicas con domicilio en Colombia , que se encuentren al día en sus compromisos, por todo concepto con la Cámara de Comercio de su domicilio.

Solamente en el caso que esta invitación este dirigida a Personas Jurídicas, será requisito indispensable lo siguiente (de lo contrario favor hacer caso omiso):

a) Tener como mínimo de constitución el tiempo solicitado para acreditar la experiencia general, sin que sea inferior a un (1) año.
b) Tener debidamente renovada su matrícula y al día en sus compromisos con la Cámara de Comercio de su domicilio.
c) No estar en liquidación o bajo condiciones financieras o de cualquier otra índole que pudieran implicar un riesgo no admisible para la Cámara de Comercio de Bucaramanga.
d) No estar incurso en ninguna de las causales de inhabilidad, incompatibilidad o conflicto de intereses de acuerdo con las normas legales vigentes.
e) En la presente invitación privada, no está habilitada para la participación de consorcios, uniones temporales u otras formas de asociación.

2.2. PERFIL Y EXPERIENCIA DEL OFERENTE.

a) El objeto social o actividad económica, según corresponda, deberá contemplar actividades afines a las señaladas en la presente invitación privada.
b) Experiencia comprobada mínimo de dos (2) años en actividades relacionadas con el objeto de la presente invitación privada, debidamente soportada con tres (3) certificaciones de cumplimiento de contratos en los últimos dos (2) años .

2.3. CONTENIDO DE LA PROPUESTA Y ANEXOS

Solicitamos adjuntar la información y documentación que a continuación relacionamos, como requisitos para realizar la evaluación de las propuestas que se reciban:

a) Propuesta técnico-económica, denominada en pesos colombianos que detalle el costo básico del bien y/o servicio, el valor del IVA y a continuación su valor total. Si el servicio o bien a proveer está exento o excluido del IVA, deberá hacer expresa mención de esta circunstancia en su propuesta.
b) Certificado de existencia y representación legal expedido por la autoridad competente con la facultad de hacerlo, no mayor a treinta (30) días calendario anteriores a la presentación de la propuesta. Este requisito no aplica para las personas naturales y jurídicas inscritas en Cámaras de Comercio.
c) Copia del Registro Único Tributario (RUT) con impresión generada al año de presentación de la propuesta. No se aceptarán documentos en trámite ante la DIAN.
d) Acreditar la experiencia del oferente allegando los certificados de cumplimiento de contratos celebrados en los últimos dos (2) año(s). (El objeto debe ser igual o relacionado con el enunciado en esta invitación privada)
e) En atención al perfil del oferente señalado en el numeral 2.1. y si la propuesta a presentar excede las facultades del representante legal de la persona jurídica, ya sea por razón de la naturaleza o la cuantía, deberá anexar junto con la propuesta, la autorización concedida al representante legal para presentar propuesta y celebrar el contrato, otorgada por parte del órgano que corresponda de acuerdo con los estatutos.
f) Diligenciar y firmar el "Formato Único de Proveedores" – Anexo 1.
g) Presentar la Garantía de Seriedad de la Oferta y soporte de pago de la prima, en las condiciones mencionadas en el numeral siguiente. **→ Este requisito aplica únicamente para ofertas que superen los 100 SMMLV antes de IVA**.

2.4. GARANTÍA DE SERIEDAD DE LA OFERTA

SOLAMENTE CUANDO la propuesta o presupuesto definido en la presente invitación privada **SUPERE los 100 SMMLV antes del IVA**, la presentación de esta garantía será requisito indispensable, bajo los siguientes parámetros:

El hecho de presentar la propuesta se entenderá que la misma es irrevocable y que el oferente mantiene vigente todas las condiciones originales de su propuesta, durante todo el tiempo que dure la invitación privada, incluidas las prórrogas de los plazos que llegaren a presentarse. Esta garantía debe ser expedida por una Compañía de Seguros legalmente constituida en el país, a favor de la Cámara de Comercio de Bucaramanga con NIT. 890.200.110-1, de acuerdo con lo establecido a continuación:

a) La garantía deberá ser expedida en formato de entidades PARTICULARES, por un valor equivalente al diez por ciento (10%) del valor total de la propuesta incluido el IVA, con una vigencia de sesenta (60) días calendario, contados a partir de la fecha de cierre de la invitación privada. En caso de prórroga del plazo, el oferente deberá mantener vigente todos los plazos y condiciones originales de su propuesta y ampliar la validez de la garantía de seriedad por el término adicional que señale la Cámara de Comercio de Bucaramanga.
b) La garantía de seriedad deberá estar acompañada del recibo o constancia del pago de la prima efectuada a la Compañía de Seguros, es decir, que no será viable adjuntar constancia de que "la póliza no expirará por falta de pago", así mismo no se aceptarán soportes de pago expedidos por los intermediarios del seguro.

2.5. PRESUPUESTO, FORMA DE FACTURACIÓN Y PAGO

La propuesta económica la definirá el oferente de acuerdo a sus precios, incluyendo el costo básico del bien o servicio, el valor del IVA (si hay lugar a ello) y demás costos directos e indirectos necesarios para el cumplimiento del objeto del contrato; entre otros, pero no limitándose, a los siguientes: Honorarios, desplazamientos, alojamiento y

manutención del personal que disponga en la ejecución; herramientas y materiales de trabajo utilizados en las actividades, impuestos, pólizas, transportes, fletes, despachos; tasas, contribuciones legales y cualquier otro tipo de gasto que pueda generarse durante la ejecución del contrato. El valor máximo presupuestado por Camara de Comercio de Bucaramanga para este contrato es de $135.000.000 ciento cuarenta millones de pesos IVA incluido

El valor de la presente contratación será atendida con recursos de origen público

En cuanto a la forma de facturación y pago *se hará mediante un único pago, previa entrega y configuración de los equipos enumerados en el numeral 1.3 Alcance más la capacitación a los ingenieros de la unidad TIC de la Cámara.*

Para la forma de pago tener en cuenta que no aplica desembolso por concepto de anticipos sin la previa viabilidad de la Cámara de Comercio de Bucaramanga, en razón a los montos permitidos en el manual de contratación de compras de bienes y/o servicios; que cubra determinadas necesidades de acuerdo con la naturaleza del contrato y que el mismo tenga un respaldo, mediante un amparo adicional a la póliza de seguro con una suma asegurada equivalente al 100% de su valor y cuyos costos asociados a la expedición correrán por cuenta del oferente.

Para la legalización de los pagos, la Cámara de Comercio de Bucaramanga verificará el cumplimiento del pago de los aportes al sistema de seguridad social integral del oferente y del personal que éste disponga para la ejecución del contrato, en los montos y condiciones establecidas en la ley colombiana.

3. PREPARACIÓN DE LA PROPUESTA

Todos los costos asociados a la preparación y presentación de la propuesta estarán a cargo del oferente. La Cámara de Comercio de Bucaramanga en ningún caso será responsable de los mismos.

La propuesta junto con todos los documentos que la acompañan deberá ser presentados en español y todas sus páginas deben estar enumeradas en forma ascendente consecutiva, con el correspondiente índice o tabla de contenido que permita su fácil consulta. Estos documentos deben ser entregados en original en sobre sellado y debidamente firmados por el oferente o por el Representante Legal si es persona jurídica. En caso de existir incongruencias en el contenido de la propuesta, es decir, que una parte de la misma establezca algo que se contradiga en otra parte, la Cámara de Comercio de Bucaramanga podrá solicitar las aclaraciones pertinentes.

En el sobre de la propuesta será requisito hacer constar el nombre del oferente, su dirección comercial y datos de contacto, así como el número de la invitación privada a la que se postula. Se aceptarán las propuestas entregadas en físico en las condiciones y plazos que más adelante se señalarán.

3.1. VALIDEZ DE LA PROPUESTA

La propuesta presentada deberá tener una validez mínima de sesenta (60) días calendario, contados a partir de la fecha de cierre de la invitación privada.

3.2. CALIFICACIÓN DE LAS PROPUESTAS

De acuerdo con la necesidad requerida, ya sea para bienes o servicios, en relación con el objeto contractual de esta invitación privada, tenga en cuenta a continuación los criterios que aplican para la calificación de las propuestas:

3.2.1. CRITERIOS GENERALES PARA CONTRATACIÓN DE BIENES	PUNTOS
a) Propuesta técnica	30
b) Propuesta económica	45
c) Experiencia específica	25
Puntaje Total:	**100**

PARA ESTA CONVOCATORIA SE APLICARÁN LOS CRITERIOS DE EVALUACIÓN DE LA TABLA 3.2.1

a. Propuesta Técnica:
Se calificará según la lógica del enfoque técnico, el cubrimiento de las necesidades técnicas, la metodología y el plan de trabajo o cronograma de actividades propuestos en respuesta a esta invitación privada.

b. Propuesta Económica:
Se calificará según el procedimiento negociado en régimen competitivo, donde el mayor puntaje lo recibe la propuesta más ventajosa en términos económicos para la Cámara de Comercio de Bucaramanga y las demás se califican en forma proporcional descendiente

c. Experiencia Específica:
Se calificará según la experiencia acreditada y específica en contratos similares durante los últimos dos (2) años.

3.2.2. CRITERIOS GENERALES PARA CONTRATACIÓN DE SERVICIOS	PUNTOS
a) Propuesta técnica o metodología	30
b) Propuesta económica	35
c) Experiencia específica	35
Puntaje Total:	**100**

LOS CRITERIOS DE LA TABLA 3.2.2 NO APLICAN PARA ESTA CONVOCATORIA

Criterio de desempate: En caso de que dos o más propuestas obtengan el mismo puntaje en la calificación, la calidad de "afiliado" a la Cámara de Comercio de Bucaramanga, será el criterio que se utilizará para desempate, si aplica.

3.3. EXCLUSIÓN DE PROPUESTAS:

La Cámara de Comercio de Bucaramanga no tendrá en cuenta las propuestas recibidas en las que:

a) El oferente no cumpla con demostrar la experiencia específica solicitada, no adjunte la respectiva propuesta económica, técnica, metodológica u hoja de vida según sea el caso, siempre y cuando haga parte de los requisitos y documentos solicitados en esta invitación privada o no presente la póliza de seriedad de la oferta, siempre que aplique.
b) Se hubiere presentado la propuesta en forma subordinada al cumplimiento de cualquier condición del oferente.
c) Se incluya información no veraz.
d) Se incluyan disposiciones contrarias a la ley colombiana.
e) Las propuestas recibidas con posterioridad a la fecha y hora de cierre de la presente invitación privada.

f) Se advierta que el oferente se encuentra en proceso de liquidación o bajo condiciones financieras que impliquen un riesgo no admisible para la Cámara de Comercio de Bucaramanga.
g) No se encuentre al día en la renovación de la matrícula mercantil, en caso de ser aplicable.

3.4. CAUSALES DE APERTURA DE NUEVA INVITACIÓN PRIVADA

La invitación privada deberá concluirse y motivar la realización de una nueva, en los siguientes casos:

a) Cuando ninguna de las propuestas evaluadas cumpla con los requisitos exigidos en la presente invitación privada.
b) Por motivos o causas que impidan la escogencia objetiva.
c) Cuando se hubiere violado la reserva de las propuestas presentadas.
d) Cuando no se presente ninguna propuesta.
e) Cuando las propuestas superen el presupuesto de la entidad.

4. CONDICIONES PARA LA SUSCRIPCIÓN Y EJECUCIÓN DEL CONTRATO

4.1. SUSCRIPCIÓN DEL CONTRATO

La Cámara de Comercio de Bucaramanga suscribirá contrato con el oferente seleccionado, una vez se cumpla con los requisitos exigidos y las etapas previas establecidas en el manual de contratación de compras de bienes y/o servicios de la Cámara de Comercio de Bucaramanga.

Solo si está invitación tiene por objeto la contratación de prestación de servicios y está dirigida a personas naturales para la legalización del contrato, se tendrá que presentar el certificado de afiliación **vigente** como **independiente**, con fecha de **expedición no superior a 1 mes a la fecha de presentación** de la oferta, de **SALUD (EPS)** y **PENSIÓN (AFP)**. En caso de estar exento de cotizar pensión, deberá presentar el certificado correspondiente. **(**Si se encuentra **afiliado a ARL**, favor adjuntar también el respectivo **certificado**, bajo las mismas condiciones indicadas anteriormente, con el fin de evitar una multiafiliación).

NOTA: En caso de que la contratacion sea igual o superior a un (1) mes y que el oferente seleccionado sea persona natural, deberá cumplir con lo establecido en la normativa vigente (Ley 1562 de 2012 reglamentada por el Decreto 723 de 2013 y el Decreto 1072 de 2015), presentando previamente a la legalización del contrato, la certificación expedida por un médico especialista con licencia en Salud Ocupacional de cualquier IPS avalada por la Secretaría de Salud Departamental, como soporte de haberse realizado los respectivos exámenes preocupacionales para la contratación.

4.2. FECHA DE INICIO

La ejecución del contrato iniciará previo cumplimiento de los requisitos establecidos en él y con la aprobación por parte de la Cámara de Comercio de Bucaramanga de las garantías exigidas en el contrato, en caso de que aplique.

4.3. GARANTÍAS FUTURAS

El oferente seleccionado, se obliga a constituir a su costo y a favor de la Cámara de Comercio de Bucaramanga, con el lleno de los requisitos legales y contractuales, póliza de seguros expedida por una compañía de seguros autorizada para funcionar en Colombia que ampare los siguientes riesgos:

a) De cumplimiento: Por un monto equivalente al veinte por ciento (20%) del valor del contrato incluido el IVA, con una duración igual a la del contrato y dos (2) meses más.

b) De salarios, prestaciones sociales e indemnizaciones laborales: Por un monto equivalente al quince por ciento (15%) del valor total del contrato incluido el IVA, con una duración igual a la del contrato y treinta y seis (36) meses más, si aplica.

c) Una póliza de calidad del servicio: Por un monto equivalente al 30% del valor total del contrato incluido el IVA, con una vigencia igual a la del contrato y seis (6) meses más, si aplica.

De ser necesario de acuerdo con la naturaleza del contrato, podrá exigirse otro tipo de amparos.

4.4. RÉGIMEN DE SEGURIDAD SOCIAL INTEGRAL Y PAGO DE APORTES

El oferente seleccionado deberá afiliar y realizar los aportes necesarios a las entidades que pertenecen al régimen de seguridad social integral (EPS, ARL, AFP) y parafiscales, conforme la legislación aplicable y deberá mantenerse vigente durante todo el tiempo de ejecución del contrato para el personal que disponga en el cumplimiento del objeto contratado. Para el caso del oferente persona natural, los aportes al sistema deberán efectuarse sobre un monto equivalente al 40% de sus honorarios, siempre y cuando este porcentaje no sea inferior a un (1) Salario Mínimo Mensual Legal Vigente acorde con lo establecido en el art. 135 de la Ley 1753 de 2015, la Ley 789 de diciembre de 2002, la Ley 797 de enero de 2003 y demás disposiciones legales vigentes.

En cualquier caso, **se comprometerán a presentar los soportes del pago respectivo durante la vigencia del contrato**, lo cual constituirá un requisito indispensable para los pagos que le corresponden en virtud del contrato.

5. CRONOGRAMA DE LA INVITACIÓN PRIVADA

ACTIVIDAD	FECHA Y HORA	LUGAR
Apertura de la Invitación Privada, publicación de la invitación privada en la página web.	24 de enero de 2020 a las 00:00 horas.	www.camaradirecta.com/solicitar-servicios-empresariales/ofertas-para-proveedores
Cierre de la invitación privada y fecha máxima de recepción de propuestas.	04 de febrero de 2020 hasta las 5:00 pm.	En sobre sellado a nombre de la Coordinación de Contratación y Compras en la ventanilla única de correspondencia Carrera 19 No. 36-20 Piso 2 de la Cámara de Bucaramanga.
Evaluación y definición de la oferta favorecida.	12 de febrero de 2020	En la Unidad Tecnología
Publicación de resultados invitación privada.	28 de febrero de 2020	www.camaradirecta.com/solicitar-servicios-empresariales/ofertas-para-proveedores

5.1. RECEPCIÓN PROPUESTAS E INFORMACIÓN GENERAL.

Las propuestas deberán ser entregadas en medio físico, en original y en sobre sellado en las instalaciones de la oficina/seccional más cercana a su domicilio de la Cámara de Comercio de Bucaramanga o preferiblemente en la Carrera 19 No. 36 – 20 Piso 2, en la Ventanilla Única de Correspondencia “VUC”, de la siguiente manera:

Coordinador de Contratación y Compras
Cámara de Comercio de Bucaramanga
Asunto: INVITACIÓN PRIVADA No. 8103 **- CONTRATAR** Adquisición y configuración de una solución Firewall de nueva generación (NGFW) en alta disponibilidad, que funcione adicionalmente como Controladora inalámbrica (WLC) para los puntos de acceso inalámbrico con los que cuenta actualmente la entidad

a) Se entenderán por fecha y hora de presentación las que aparezcan en el sello o escrito puesto en el sobre sellado y en la copia del recibido por parte del empleado responsable en la ventanilla única de correspondencia, en el momento exacto de su llegada al sitio de entrega de esta.
b) Si la propuesta es enviada por correo certificado u ordinario, el oferente debe hacerlo con suficiente antelación para que sea recibida en el lugar indicado antes de la hora y fecha límite de cierre. En todo caso, la Cámara de Comercio de Bucaramanga no será responsable del retardo o extravío que se derive de esta forma de presentación.
c) Con la presentación de la propuesta, el oferente manifiesta que estudió el contenido de la presente invitación privada y demás documentos anexos a la misma, que conoce la naturaleza de la contratación y su tiempo de ejecución, que formuló su propuesta de manera libre, responsable, precisa y coherente de acuerdo con lo requerido por la Cámara de Comercio de Bucaramanga.
d) El simple hecho de que el oferente no haya obtenido la información necesaria para la correcta elaboración de su propuesta, no lo exime de asumir las responsabilidades que le correspondan, ni le dará derecho a reclamaciones, ajustes o reconocimientos adicionales por parte de la Cámara de Comercio de Bucaramanga, inclusive, cuando dichas omisiones deriven en posteriores sobrecostos para el contratista.
e) La información contenida en este documento de invitación privada sustituye totalmente cualquier otra que pudiera habérsele suministrado en forma preliminar a los oferentes interesados en esta invitación, por parte del personal vinculado a la Cámara de Comercio de Bucaramanga.

5.2. MECANISMOS DE COMUNICACIÓN

En esta invitación privada los mecanismos de comunicación de carácter oficial que se utilizarán entre los oferentes y la Cámara de Comercio de Bucaramanga, son:

Encargado: Jose Rogelio Gutierrez Solano – Jefe de Infraestructura Tecnológica
Correo electrónico: rogelio.gutierrez@camaradirecta.com
Carrera 19 No. 36-20 Piso 2 Bucaramanga
Tel. 6527000 ext. 240 - 242

Favor remitir sus inquietudes consolidadas en un único correo electrónico a más tardar un (1) día hábil antes de la fecha de cierre de la presente invitación privada, indicando en el asunto: INVITACIÓN PRIVADA No.: 8103 **- CONTRATAR** Adquisición y configuración de una solución Firewall de nueva generación (NGFW) en alta disponibilidad, que funcione adicionalmente como Controladora inalámbrica (WLC) para los puntos de acceso inalámbrico con los que cuenta actualmente la entidad.

5.3. DOCUMENTOS ANEXOS

a) **ANEXO 1 – f-adm-01-07 "Formato Único de Proveedores", diligenciado completamente y firmado.**