

## SOLICITUD DE COTIZACIÓN DE UNA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL PARA PROTEGER LA RED LAN Y WAN DEL INSTITUTO NACIONAL DE VIAS

### 1. INTRODUCCIÓN

El Instituto Nacional de Vías “INVIAS” es un establecimiento público del orden nacional adscrito al Ministerio de Transporte, creado en el año de 1994, con su sede principal en Bogotá y 26 sedes territoriales en todo el territorio colombiano; cuenta con personería jurídica, autonomía administrativa y patrimonio propio, y tiene como objetivo la ejecución de las políticas, estrategias, planes, programas y proyectos de la infraestructura no concesionada de la red vial nacional de carreteras primaria y terciaria, red férrea, red fluvial e infraestructura marítima, de acuerdo a los lineamientos del gobierno nacional.

Haciendo uso de la infraestructura tecnológica que se describe en el numeral 2, la entidad debe producir información que permita la toma de decisiones en materia de ejecución de las obras para el mantenimiento, construcción o rehabilitación de la red vial a su cargo.

### 2. INFRAESTRUCTURA TECNOLÓGICA

#### 2.1. Centro de cómputo

La entidad cuenta con un centro de cómputo con más de diez años de instalación, ubicado en el sexto piso de la sede principal, en la carrera 59 No. 26-60 (CAN), el cual será trasladado en el primer semestre del año en curso, al edificio Central Point, ubicado en Bogotá en la 73b, Cl. 25g #73b-90.

#### 2.2. Seguridad perimetral

La seguridad perimetral para la protección de los servicios tecnológicos ofrecidos por la entidad está integrada por dos dispositivos firewall conectados mediante enlaces en fibra de 1 Gbps (HA) para garantizar alta disponibilidad y balanceo de carga. El soporte tecnológico de estos dispositivos venció en el mes de marzo de 2018 (ver tabla No. 1).

<b>DISPOSITIVO</b>	<b>MARCA</b>	<b>SISTEMA OPERATIVO</b>	<b>FUNCIÓN</b>
FIREWALL	PALO ALTO 5020	PAN OS 7.03	FIREWALL PERIMETRO
FIREWALL	PALO ALTO 5020	PAN OS 7.03	FIREWALL PERIMETRO
SERVIDOR	MANAGEMENT PANORAMA	PAN OS 7.03	ADMINISTRACION FIREWALL
SWITCH	AVAYA SWITCH ERS-4826GTS	v5.8.1.029	ALTA DISPONIBILIDAD FW
SWITCH	AVAYA SWITCH ERS-4826GTS	v5.8.1.029	ALTA DISPONIBILIDAD FW

**Tabla No. 1: Dispositivos que integran la seguridad perimetral**

SOLICITUD DE COTIZACIÓN DE UNA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL PARA PROTEGER LA RED LAN Y WAN DEL INSTITUTO NACIONAL DE VIAS

Por otra parte, la cantidad aproximada de sesiones concurrentes es 100.000, el enrutamiento es manejado mediante 71 rutas estáticas configuradas a nivel del Firewall y el Switch de Core, y el tráfico de red es controlado a través de las zonas de seguridad descritas a continuación (ver figura 1).

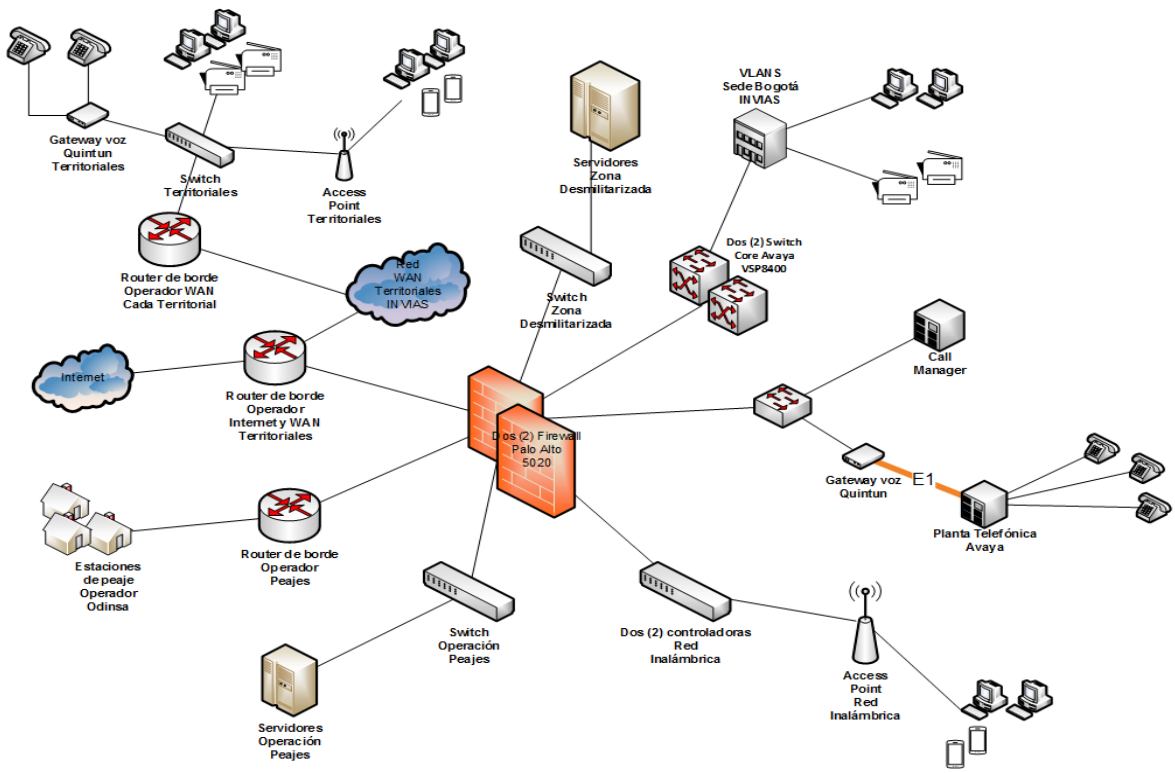


Figura 1: SEGMENTOS DE RED O ZONAS DE SEGURIDAD

- Red de servidores zona desmilitarizada (DMZ).
- Red inalámbrica con dos controladoras ubicadas en el centro de cómputo y, dispositivos Access Point ubicados en cada uno de los pisos de la sede principal y las veintiséis (26) territoriales (ver tabla No. 1).

DESCRIPCIÓN	MARCA - MODELO
CUARENTA Y NUEVE (49) ACCESS POINT	Access Point Extreme Altitude 4620
DOS ONTROLADORAS	EXTREME -WM3600
UN AIRDEFENSE	MOTOROLA

Tabla No. 2: Dispositivos que integran la red inalámbrica

## SOLICITUD DE COTIZACIÓN DE UNA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL PARA PROTEGER LA RED LAN Y WAN DEL INSTITUTO NACIONAL DE VIAS

---

- Red para los servidores y equipos del centro de control operativo que reciben la información de las estaciones de peaje a cargo del INVIAS.
- Red internet a la cual se tiene acceso mediante un enlace en redundancia con un ancho de banda de 1 Gbps. Haciendo uso de este enlace, se tienen configuradas cinco (5) conexiones VPN Site-to-Site, para servicios en la nube de Amazon y Microsoft (Azure).
- Red WAN a la cual se tiene acceso mediante un enlace con un ancho de banda de 750 Mbps.
- Red para veintisiete (27) sedes, cada una con un ancho de banda de 32 Mbps.
- Red para telefonía IP en la sede principal con 650 extensiones, con teléfonos marca Avaya.
- Red LAN conformada por las siguientes VLAN, configuradas en el Switch de Core:
  - Seis VLAN, una para cada uno de los pisos de la sede principal (Bogotá).
  - Una VLAN para gestión de dispositivos de comunicación.
  - Una VLAN para servidores que se encuentran por fuera de la DMZ.
- Red para los equipos que hacen parte del Programa de Seguridad en las Carreteras Nacionales.

### 2.3 Switch y Core

La entidad cuenta los siguientes equipos switch instalados en todas sus sedes:

- Dos (2) Switch Core Avaya VSP8400 conectados en alta disponibilidad, ubicados en el centro de cómputo.
- Trece (13) switch ERS 4850GTS-PWR con PoE, quince (15) ERS 4850GTS Sin PoE y un (1) switch 3524GT, instalados en la sede central.
- Nueve (9) switch HP 4210G y diecisiete (17) switch 3COM 5500G-EI 3CR17250-91, instalados en las sedes territoriales.

### 2.4. Servidores

Los servicios tecnológicos, aplicaciones y sistemas de información están instaladas en 75 servidores entre físicos y virtuales, entre los que podemos destacar:

- Dos servidores SPARC ORACLE T5 y ocho máquinas virtuales con sistema operativo Linux SUN, para soportar las instancias de base de datos Oracle en alta disponibilidad.

## SOLICITUD DE COTIZACIÓN DE UNA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL PARA PROTEGER LA RED LAN Y WAN DEL INSTITUTO NACIONAL DE VIAS

- Dos servidores Hewlett Packard con sistema operativo Microsoft Windows Server 2008 R2 Data Center.
- Tres servidores Hewlett Packard y dos máquinas virtuales con sistema operativo Microsoft Windows Server 2008 R2 Enterprise.
- Nueve máquinas virtuales con sistema operativo Microsoft Windows Server 2008 R2 Standard.
- Dos (2) servidores HP BL460cGen9 con sistema operativo Windows Server 2012 R2 Datacenter para gobierno.
- Dos servidores (2) HP ML380 G9 con sistema operativo Windows Server 2012 R2 Datacenter
- Una máquina virtual con sistema operativo Microsoft Windows Server 2012 Datacenter.
- Cuatro servidores Hewlett Packard y una máquina virtual con sistema operativo Microsoft Windows Server 2012 R2 Standard.
- Cinco servidores Hewlett Packard y catorce máquinas virtuales con sistema operativo Microsoft Windows Server 2012 Standard.
- Un servidor Hewlett Packard con sistema operativo Microsoft(R) Windows(R) Server 2003 Standard x64 Edition.
- Tres servidores Hewlett Packard y una máquina virtual con sistema operativo Microsoft(R) Windows(R) Server 2003, Enterprise Edition.
- Dos máquinas virtuales con sistema operativo Microsoft(R) Windows(R) Server 2003, Standard Edition.
- Tres servidores Hewlett Packard con sistema operativo Microsoft® Windows Server® 2008 Enterprise.

### 2.5. Computadores de escritorio

La entidad, cuenta con un promedio de 1261 computadores de escritorio de diferentes marcas y modelos, distribuidos a lo largo de las 26 sedes territoriales y Bogotá, con sistema operativo Windows 7 pro, Windows 8 Pro y Windows 10 Pro, como se describe a continuación (ver tabla No. 3).

<i><b>Marca</b></i>	<i><b>Modelo</b></i>
Acer	Aspire S3-391
ASUS	All Series
ASUSTeK	COMPUTER X550LD

**SOLICITUD DE COTIZACIÓN DE UNA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL PARA PROTEGER LA RED LAN Y WAN DEL INSTITUTO NACIONAL DE VIAS**

INC.	
Compaq	DSDT
Compaq-Presario	GJ371AA-ABM SG3010LA
Dell Inc.	Inspiron 410
Dell Inc.	Latitude D630
Dell Inc.	OptiPlex 740
Dell Inc.	OptiPlex 740 Enhanced
Dell Inc.	OptiPlex 9010
Dell Inc.	PowerEdge R220
Dell Inc.	Precision WorkStation T3400
Hewlett-Packard	21-h005la
Hewlett-Packard	23-h055la
Hewlett-Packard	6200 PRO
Hewlett-Packard	6200 pro sff
Hewlett-Packard	AT496AV
Hewlett-Packard	HO Compaq 6200 Pro MT
Hewlett-Packard	HP 100B All-in-One PC
Hewlett-Packard	HP 2230s
Hewlett-Packard	HP 430 Notebook PC
Hewlett-Packard	HP Compaq 6000 Pro MT PC
Hewlett-Packard	HP Compaq 6005 Pro SFF PC
Hewlett-Packard	HP Compaq 6200 Pro MT
Hewlett-Packard	HP Compaq 6200 Pro MT PC
Hewlett-Packard	HP Compaq 6200 Pro SFF
Hewlett-Packard	HP Compaq 6200 Pro SFF PC
Hewlett-Packard	HP Compaq 6200 Pro Small Form Factor
Hewlett-Packard	HP Compaq 6530b (FS745LA#ABM)
Hewlett-Packard	HP Compaq 8100 Elite CMT
Hewlett-Packard	HP Compaq 8100 Elite CMT PC
Hewlett-Packard	HP Compaq 8100 Elite SFF PC
Hewlett-Packard	HP Compaq 8200 Elite AiO Business PC
Hewlett-Packard	HP Compaq dc5100 MT(EW749LA)
Hewlett-Packard	HP Compaq dc5100 SFF(PM215AV)
Hewlett-Packard	HP Compaq dc5700 Microtower
Hewlett-Packard	HP Compaq dc5800 Microtower
Hewlett-Packard	HP Compaq dc5800 Small Form Factor
Hewlett-Packard	HP Compaq dc5850 Microtower
Hewlett-Packard	HP Compaq dc7600 Small Form Factor
Hewlett-Packard	HP Compaq Elite 8300 Touch All-in-One PC

**SOLICITUD DE COTIZACIÓN DE UNA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL PARA PROTEGER LA RED LAN Y WAN DEL INSTITUTO NACIONAL DE VIAS**

Hewlett-Packard	HP Compaq Pro 4300 AiO PC
Hewlett-Packard	HP Compaq Pro 6300 SFF
Hewlett-Packard	HP dx2000 MT (PP826A)
Hewlett-Packard	HP dx2000 MT (PW999AA)
Hewlett-Packard	HP dx5150 SFF
Hewlett-Packard	HP Elite 7100 Microtower PC
Hewlett-Packard	HP ENVY 15 Notebook PC
Hewlett-Packard	HP Pavilion dv2000 (RX563LA#ABM)
Hewlett-Packard	HP Pavilion dv6000 (GM695LA#ABM)
Hewlett-Packard	HP Pro 3000 Microtower PC
Hewlett-Packard	HP ProBook 4530s
Hewlett-Packard	HP ProBook 4720s
Hewlett-Packard	HP ProDesk 600 G1 SFF
Hewlett-Packard	HP ProOne 400 G1 AiO
Hewlett-Packard	HP xw8600 Workstation
Hewlett-Packard	HP Z210 Workstation
Hewlett-Packard	LK599LT
Hewlett-Packard	LK599LT#ABM
Hewlett-Packard	PPPPP-CCC#MMMMMMMMM
HP Pavilion 06	D5468AT-ABA ALONPAV
HP-Pavilion	FK963AA-ABM IQ510la
HP-Pavilion	GN656AA-ABM a6210la
HP-Pavilion	NP120AA-ABM s5130la
IBM	8188KSE
INTEL_	DH55HC__
LENOVO	20351
Sony Corporation	VPCM120AL

**Tabla No. 3: Computadores de escritorio**

## **2.6. Tablet**

La entidad cuenta con un promedio de 20 dispositivos IPAD y dos tablet con sistema operativo Android.

## **2.7. Impresoras**

La entidad cuenta con un promedio de 102 impresoras con direccionamiento IP, en su gran mayoría marca Lexmark, distribuidas así:

- Setenta y dos (72) impresoras en Bogotá.

## SOLICITUD DE COTIZACIÓN DE UNA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL PARA PROTEGER LA RED LAN Y WAN DEL INSTITUTO NACIONAL DE VIAS

- Treinta (30) impresoras en las sedes territoriales.

### 2.8. Televisores

Existe un promedio de 20 televisores Smart TV e industriales, conectados a la red LAN brindando el servicio de carteleras digitales, despliegue de turnos en la zona de atención al ciudadano y para presentaciones en las salas de reuniones con que cuenta la entidad.

### 2.9. servicios

La entidad ofrece los siguientes servicios tecnológicos:

- Servicio de directorio, LDAP y Radius instalado bajo sistema operativo Windows Server 2016.
- Servicio de ofimática en la nube Office365, incluye correo electrónico, Word, Excel, Power Point, Project, Skype y One Drive, entre otros.
- Alrededor de 30 sistemas de información y aplicaciones.
- Sistemas de bases de datos Oracle, Sqlserver y Mysql.
- Servicio de antivirus para cada uno de los equipos con sistema operativo de Microsoft.

## 3. REQUISITOS TÉCNICOS Y FUNCIONALES DE LA SOLUCIÓN A COTIZAR

Teniendo en cuenta que la seguridad informática hace parte de la política institucional del **INVIAS**, la entidad solicita a las empresas idóneas en proveer soluciones que garanticen la seguridad perimetral, presentar una cotización de una **INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL CON ALTA DISPONIBILIDAD PARA PROTEGER LA RED LAN Y WAN DEL INSTITUTO NACIONAL DE VIAS** que cumpla con los siguientes requisitos técnicos y funcionales mínimos:

<b>Componentes de la solución perimetral</b>
<p>La solución de seguridad perimetral debe estar compuesta por:</p> <p>a) Dos (2) equipos firewall de nueva generación NGFW (Next Generation Firewall) en conexión activo-activo.</p> <p>b) Un (1) dispositivo para almacenamiento y procesamiento de registros de auditoría.</p> <p>c) Dos (2) switch de veinticuatro (24) puertos estacables para integración de la solución.</p>
<b>Requisitos generales de la solución</b>
<p>a) Los componentes que integran la solución no deben aparecer en listas end-of-life ó end-of-sale del fabricante.</p> <p>b) Vinculación de usuarios y dispositivos, no solo direcciones IP con las políticas protección de los servicios que operan sobre la infraestructura tecnológica del INVIAS o en la nube (Microsoft Azure y Amazon).</p> <p>c) Los dispositivos deben ser tipo appliance (hardware y software integrados en un solo equipo) accesibles a través de SSH e interfaz web usando SSL.</p> <p>d) El firmware y sistema operativo de los equipos que conformen la solución deben ser compatibles con protocolo IPv4 e IPv6. No se aceptarán equipos con sistema operacional de uso genérico.</p> <p>e) Mínimo 90.000 conexiones por segundo.</p>

**SOLICITUD DE COTIZACIÓN DE UNA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL PARA PROTEGER LA RED LAN Y WAN DEL INSTITUTO NACIONAL DE VIAS**

f) Funciones de seguridad básicas como: VPN IPSec y SSL, control de aplicaciones, filtrado URL, IPS, identificación y control de usuarios, administración de ancho de banda (QoS).
<b>Requisitos específicos para el Firewall NGFW</b>
<p>a) Throughput de 5.6 Gbps con la funcionalidad de control de aplicaciones habilitada para todas las firmas que el fabricante posea.</p> <p>b) Throughput de 2.3 Gbps con las siguientes funcionalidades habilitadas simultáneamente para todas las firmas que la plataforma de seguridad posea debidamente activadas y actuando: control de aplicaciones, IPS, Antivirus e Antispyware.</p> <p>c) Soportar como mínimo, 2.000.000 de conexiones simultaneas.</p> <p>d) Soportar como mínimo, 65.000 nuevas conexiones por segundo.</p> <p>e) Fuente redundante de 650 W de CA o CC (180/240).</p> <p>f) Disco Solid State Drive (SSD) como mínimo, de 200 GB para almacenamiento del sistema y Logs.</p> <p>g) Mínimo, diez (10) interfaces de red de 10/100/1000 base-TX.</p> <p>h) Mínimo, seis (6) puertos SFP/SFP+ de 1/10 Gb.</p> <p>i) Un (1) puerto de gestión fuera de banda de 10/100/1000 Gb.</p> <p>j) Dos (2) puertos de 10/100/1000 Gb de alta disponibilidad.</p> <p>k) Un (1) puerto SFP+ de 10 Gb de alta disponibilidad.</p> <p>l) Un (1) puerto de consola RJ-45.</p> <p>m) Un (1) puerto micro-USB.</p> <p>n) Soportar como mínimo, ocho (8) ruteadores virtuales.</p> <p>o) Soportar como mínimo, cincuenta (50) zonas de seguridad.</p> <p>p) Capacidad mínima de mil veinticuatro (24) clientes de VPN SSL simultáneos, sin uso de licenciamiento.</p> <p>q) Capacidad mínima de cuatro mil (4000) túneles VPN IPSEC simultáneos, sin uso de licenciamiento.</p> <p>r) Capacidad de expansión hasta 6 sistemas virtuales lógicos (contextos) en el firewall físico.</p> <p>s) Capacidad de enrutamiento OSPFv2/v3, BGP, RIP y estático.</p> <p>t) Capacidad de multicast PIM-SM, PIM-SSM, IGMP v1, v2 y v3.</p> <p>u) Detección de reenvío bidireccional (BFD).</p> <p>v) Soportar los siguientes tipos de NAT:</p> <ul style="list-style-type: none"> <li>o NAT dinámico.</li> <li>o NAT estático</li> <li>o IP dinámico y puerto (traducción de la dirección del puerto).</li> <li>o NAT64, NPTv6.</li> </ul> <p>w) Modos de interfaz: L2, L3, tap, virtual wire (modo transparente).</p> <p>x) Alta Disponibilidad: activo/activo, activo/pasivo.</p> <p>y) Detección de fallas: monitoreo de ruta, monitoreo de interfaz.</p> <p>z) Identificación de la aplicación independientemente del puerto, el cifrado (SSL o SSH) o técnica evasiva empleada.</p> <p>aa) Utilización de la aplicación, no el puerto, como base para todas sus decisiones de políticas de habilitación segura: permitir, denegar, programar, inspeccionar y aplicar la configuración del tráfico.</p> <p>bb) Clasificación de las aplicaciones no identificadas para control de políticas, análisis forense de</p>



**SOLICITUD DE COTIZACIÓN DE UNA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL PARA PROTEGER LA RED LAN Y WAN DEL INSTITUTO NACIONAL DE VIAS**

amenazas o desarrollo de tecnología App-ID. cc) Identificación de malware desconocido para su análisis en función de cientos de comportamientos maliciosos para crear y ofrecer protección automáticamente. dd) Limitación de la transferencia no autorizada de archivos y datos confidenciales y habilitar de forma segura la navegación web no relacionada con el trabajo.
<b>Requisitos específicos Switch 24 puertos</b>
a) Switch tipo stackable. b) Veinticuatro puertos 10/100/1000. c) Cuatro puertos SFP+. d) Soportar mínimo 64000 rutas IPv4. e) Tabla de direcciones MAC 48000. f) Soportar mínimo 4000 VLANs. g) Flow Control: IEEE 802.3x. h) VLAN Tagging: IEEE 802.3ac. i) Spanning Tree Protocol: IEEE 802.1D. j) Rapid Spanning Tree: IEEE 802.1w. k) Multiple Spanning Tree: IEEE 802.1s. l) Link Aggregation Protocol: IEEE 802.1AX. m) Fabric Virtualization Services: IEEE 802.1aq. n) DHCP Snooping. o) SNMP v3. p) Remote Port Mirroring. q) VLAN Stacking. r) DPI ( Deep Packet Inspection).
<b>Generación de reportes</b>
a) El almacenamiento y procesamiento de registros de auditoria (logs) debe hacerse en un dispositivo independiente inmerso en la solución, con una capacidad de retención de 1 Terabyte. b) Dependiendo de las restricciones de cada fabricante, la entidad abre la posibilidad de hacer uso del servidor MANAGEMENT PANORAMA con que cuenta a la fecha (ver el numeral 2.2 – Seguridad perimetral).
<b>Análisis de comportamientos en caja de arena</b>
Se requiere prevención contra malware, zero day o amenazas desconocidas, dirigidas o APTs (Advanced Persistent Threats), con un máximo de respuesta de 24 horas.
<b>Software para proteger los servicios instalados en infraestructura de nube (Microsoft Azure y Amazon)</b>
a) Número máximo de sesiones 100.000 b) Mínimo 500 interfaces de túnel/túneles y vpn ipsec. c) Globalprotect (ssl vpn) 200 sesiones de descifrado ssl 1.024. d) Certificados para ssl entrante 25. e) Routers virtuales 3. f) Zonas de seguridad 20. g) Número máximo de políticas 2.000. h) Objetos de direcciones 4.000.

**SOLICITUD DE COTIZACIÓN DE UNA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL PARA PROTEGER LA RED LAN Y WAN DEL INSTITUTO NACIONAL DE VIAS**

- i) Capacidad de prevención contra amenazas 600 mbps.
- j) Rendimiento de vpn ipsec 250 mbps.
- k) Número de sesiones nuevas por segundo 8.000.
- l) Licencias threat prevention y wildfire.

**Licenciamiento**

Suministrar todo el licenciamiento requerido para la puesta en marcha de la solución y todas las actualizaciones que pueden surgir durante un periodo de tres años.

**Soporte y mantenimiento**

- a) Servicio de soporte técnico que permita resolver cualquier requerimiento o incidente relacionado con los componentes que conforman la solución, durante de tres años a partir de la puesta en producción. El esquema de soporte debe ser atendido mediante los siguientes tiempos de respuesta, dependiendo de la prioridad:

Prioridad	Tiempo de respuesta	Descripciones de los niveles de servicios
1	1 hora (en horario 7*24)	"Caída del sistema" o situación del producto inoperativo que afecta a un entorno de producción.
2	2 horas en jornada laboral	Situación con repercusiones importantes para el negocio que probablemente pone en peligro un entorno de producción. El software puede funcionar, pero de forma muy limitada.
3	4 horas en jornada laboral	Situación con repercusiones poco importantes para el negocio con la mayoría de las funciones de software en funcionamiento. Sin embargo, puede ser necesaria algún tipo de estrategia para poder ofrecer el servicio.
4	1 día laboral	Problema o cuestión menor que no afecta al funcionamiento de la plataforma.

- b) Servicio de mantenimiento a los dispositivos en sitio, una vez al año, por un periodo de tres años (3) contados a partir de la puesta en producción.
- c) El servicio de soporte deberá incluir configuraciones y actualizaciones del firmware y sistema operativo a la última versión de todos los equipos que conforman la solución, por un periodo de tres (3) años contados a partir de la puesta en producción.
- d) Asesoría en la revisión de archivos LOG de eventos registrados en el sistema, con el fin de detectar y evaluar los errores no reportados.
- e) Suscripción por tres años para:
- f) Prevención de amenazas, Exploits, ataques de comando y control en la red.
- g) Filtrado que permita determinar los sitios web a los cuales puede ir la navegación de la organización, obteniendo aquellos sitios maliciosos o con contenido que debe ser restringido.
- h) El derecho a nuevas aplicaciones y categorías, así como mejoras y actualización de versiones de software.
- i) Asesoría en el afinamiento de políticas de firewall principal y firewall secundario.

**SOLICITUD DE COTIZACIÓN DE UNA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL PARA PROTEGER LA RED LAN Y WAN DEL INSTITUTO NACIONAL DE VIAS**

<p>j) Documentación de los servicios de soporte técnico y/o mantenimiento que contengan como mínimo los siguientes ítems:</p> <ul style="list-style-type: none"> <li>• Causas del incidente que provocó la solicitud de soporte.</li> <li>• Procedimientos preventivos y/o correctivos aplicados.</li> <li>• Recomendaciones.</li> </ul>
<b>Entrega, instalación y puesta en producción</b>
<p>a) La entrega e instalación deberá hacerse en un plazo no mayor a un mes contado a partir de la orden de inicio de un eventual contrato.</p> <p>b) Se deberá estructurar y ejecutar un protocolo de pruebas de funcionamiento de cada uno de los equipos, antes de la puesta en producción.</p> <p>c) Instalación, configuración y alistamiento de la plataforma a la última versión estable aprobada por el fabricante, teniendo en cuenta los parámetros de seguridad de la red.</p> <p>d) Implementación y puesta en producción de la solución de acuerdo con las mejores prácticas del fabricante, teniendo en cuenta una arquitectura de red segura.</p> <p>e) Suministrar todos los elementos que sean necesarios para la instalación y correcto funcionamiento de la solución: tornillos, cables, software, ...etc.</p> <p>f) Migración y afinamiento de las políticas a partir de la solución de seguridad perimetral existente, con el fin de identificar las reglas y objetos ocultos, obsoletos, no usados, redundantes y/o traslapados.</p> <p>g) Definición de aplicaciones críticas del negocio.</p> <p>h) Filtrado de URL.</p> <p>i) Plan de pruebas de la configuración realizada (ATP).</p>
<b>Documentación</b>
<p>a) Documentación de la instalación y configuración de la solución, que abarque:</p> <ul style="list-style-type: none"> <li>• Manuales de los fabricantes de los equipos.</li> <li>• Informe de la instalación que incluya diagramas de conexión, pasos para la instalación, configuración y puesta en producción.</li> <li>• Documento de garantía de cada uno de los equipos instalados.</li> <li>• Manuales de administración.</li> <li>• Manuales de operación.</li> <li>• Documentación de licenciamiento.</li> <li>• Catálogos de la herramienta ofrecida.</li> </ul> <p>b) Documentación de cada servicio de soporte, mantenimiento o actualización de la solución instalada.</p> <p>c) La documentación (guías de administración, manuales y/o guías técnicas) de los equipos que integran la solución debe ser de acceso público a través del sitio web del fabricante.</p>
<b>Capacitación</b>
<p>a) Capacitación certificada por el fabricante a dos personas que designe el INVIAS en la instalación, configuración y administración de la solución, acompañada del boucher que los habilite para la presentación del examen de certificación.</p> <p>b) Capacitación de 16 horas, a cuatro (4) personas designadas por el INVIAS, en la configuración de la solución implementada.</p>

**SOLICITUD DE COTIZACIÓN DE UNA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL PARA PROTEGER LA RED LAN Y WAN DEL INSTITUTO NACIONAL DE VIAS**

<b>Garantía y reemplazo de partes</b>
a) Garantía de cada uno de los componentes que conforman la solución por un periodo de tres (3) años a partir de la puesta en producción. b) Para que no exista interrupciones en el servicio, en caso de falla de alguno de los equipos que hacen parte de la solución, se deberá suministrar un equipo con las mismas características o superior sin costo alguno para la entidad. c) En caso de reemplazar partes o suministrar repuestos para los dispositivos que conforman la solución, estos deben ser nuevos, no remanufacturados y de iguales o superiores características a los originales, sin costo alguno para la entidad. Los repuestos deberán tener la modalidad del siguiente día hábil (NBD next business day).
<b>Confidencialidad</b>
Mantener la confidencialidad de la información suministrada por la entidad, excepto en aquellos casos en que la información sea de dominio público.
<b>Certificaciones que acreditan al cotizante</b>
a) Contar con una certificación vigente expedida por el fabricante, acreditando que el cotizante es como mínimo, un canal GOLD. b) Ofrecer un equipo de trabajo conformado, como mínimo, por dos (2) ingenieros con tarjeta profesional vigente, y certificados por el fabricante de los equipos como personas calificadas para adelantar la implementación.

**Tabla No. 4: Características técnicas mínimas**

#### **4. PRESENTACIÓN DE LA COTIZACIÓN**

La cotización debe ser presentada a través del **Sistema Electrónico de Contratación Pública (SECOP II)** hasta el 20 de marzo de 2019, indicando el valor de **UNA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL PARA PROTEGER LA RED LAN Y WAN DEL INSTITUTO NACIONAL DE VIAS** que cumpla con todos los requisitos técnicos y funcionales mínimos del numeral 3.

Por otra parte, el **INVIAS** solicita presentar una descripción de los equipos que conforman la solución, indicando marca, modelo y cualquier aspecto técnico relevante.

**Fecha de elaboración del documento:** 14 de marzo de 2019