Partida "B"
Sistema Integral de Comunicación con Enlaces Inalámbricos para el Poder Judicial del Estado de Yucatán.

Se deberá enlazar punto a punto en una red tipo Anillo las Oficina Principales (Av. Canek) y los Edificios de las Salas de Oralidad Penal ubicados en los municipios de Umán y Kanasín

La solución deberá incluir los siguientes elementos así como la instalación, configuración y puesta en marcha de la solución completa.

1) Equipo Inalámbrico

- Arquitectura tipo IDU (Unidad Interna) o dispositivo POE y ODU (Unidad externa) con antena integrada de 23dBi, con polarización y diversidad espacial, interconectados a través de cable externo Cat-5e. Rendimiento neto agregado de 200 Mbps
- Soporte Interface TDM y Ethernet de manera simultánea. Interface TDM: que soporte hasta 16 puertos tipo E1/T1 que puedan ser configurado con el software de administración del enlace, entramado no estructurado (transparente), sincronización independiente por puerto Tx y Rx, Conector RJ-45, cumple los estándares ITU-T G.703 y G.826, código de línea E1: HDB3 @ 2.048 Mbps y T1: B8ZS/AMI @ 1.544 Mbps, latencia configurable: 5-20 mseg (defecto: 8mseg), impedancia de 120Ω balanceado para E1 y 100Ω balanceado para T1, y Oscilación y Corrimiento (Jitter & Wander) de acuerdo con ITU-T G.823 y G.824. Puerto Ethernet: 10/100/1000 Base-T con Auto Negociación (Norma IEEE 802.3u), conector RJ-45, soporte VLANs de manera transparente, la velocidad de la información pueda configurarse en pasos de 1Kbps, tamaño máximo de trama 2048 bytes, y latencia de 3 mseg.
- Soporte redundancia 1+1 provista por el mismo radio (sin unidades externas), múltiples bandas de frecuencia (4.9 a 6.0 GHz) en el mismo equipo y sin cambio de Antenas, dichas frecuencias deberán ser configurables vía software (se entregara configurado en 4.9 Ghz), soporte ancho de banda del canal de 10/20 y 40 MHz, potencia TX maximo de 25 dBm, alcance de hasta 120 Km, mecanismos internos para disminuir la interferencia, selección automática de canal, encriptación AES 128 y corrección de errores FECk= 1/2, 2/3, 3/4, 5/6, tecnología dúplex TDD, Modulación 2x2 MIMO, OFDM
- Soporte calidad se servicio QOS IEEE 802.1P, IEEE 802.1Q y 4 niveles de QOS, así como Protocolo SNMP, Telnet y HTTP
- Deberá entregarse con la configuración de ODU y POE con Ethernet (sin IDU)
- Software de administración basado en Windows, de la misma marca del fabricante del equipo.

2) Conmutador de Datos. Se deberá incluir uno (1) por cada sitio de la solución.

- Incluya 48 puertos Ethernet Gigabit 10/100/1000BASE-T capa 3, 4 puertos combo SFP para soporte de medios de fibra, 2 SFP Transceiver 1000BASE-SX con conector LC, 256 MB de CPU SDRAM, 32 MB de memoria flash y Kit para montaje en rack de 1U
- Soporte Módulos de enlace ascendente Ethernet 10 Gigabit, Módulo de apilamiento de 48 Gbps, Negociación automática de velocidad, de los modos dúplex y del control de flujo; MDI/MDIX automático; Espejeado de puertos basado en flujo y Control de tormentas de difusión.
- Capacidad de switcheo de 184 Gbps con tasa de reenvío de hasta de 131 Mpps y hasta 8.000 direcciones MAC
- Protocolos de enrutamiento de nivel 3: Rutas estáticas, Protocolo de información de enrutamiento (RIP) v1/v2, Open Shortest Path First (Protocolo de encaminamiento jerárquico de pasarela interior, OSPF) v1/v2/v3, Classless Inter-Domain Routing (Encaminamiento Inter-Dominios sin Clases, CIDR), Internet Control Message Protocol (Protocolo de control de mensajes de Internet, ICMP), ICMP Router Discover Protocol (Protocolo de descubrimiento de enrutador ICMP, IRDP), Virtual Redundant Routing Protocol (Protocolo de redundancia de enrutador virtual, VRRP), Address Resolution Protocol (Protocolo de resolución de direcciones, ARP), Internet Group Management Protocol (Protocolo de administración de

grupos de Internet, IGMP) v2, Distance-Vector Multicast Routing Protocol (Protocolo de enrutamiento de multidifusión por vector de distancia, DVMRP), DHCP

- Rendimiento de enrutamiento de nivel 3: RIP (Protocolo de información de enrutamiento), hasta 128 interfaces de enrutamiento, hasta 128 interfaces de enrutamiento OSPF; hasta 128 áreas OSPF; hasta 128 interfaces de enrutamiento por área OSPF; hasta 32 rutas para enrutamiento ECMP; hasta 2 próximos saltos por ECMP, hasta 128 interfaces de enrutamiento por VLAN, hasta 256 entradas en el reenvío de multidifusión, hasta 896 entradas ARP; hasta 512 entradas NDP.
- Calidad del Servicio: Modo de seguridad de nivel 2 (etiquetado IEEE 802.1p), Modo de seguridad de nivel 3 (DSCP), Modo de seguridad de nivel 4 (TCP/UDP), Modo avanzado con directivas basadas en flujos de nivel 2/3/4, incluidas la medición/limitación de velocidad y las garantías de ancho de banda y marca; se puedan utilizar hasta 100 ACL para la identificación de flujo de QoS mediante mapas de clase, 8 colas de prioridad por puerto, Turno rotativo ponderado (WRR) ajustable y programación de prioridad estricta, Modo de servicios QoS basado en puerto, Modo de servicios QoS basado en flujo
- Admita VLAN para el etiquetado y basado en puertos según IEEE 802.1Q. Etiquetado VLAN doble (QinQ). Hasta 1024 VLAN admitidas. VLAN dinámica con el soporte de GVRP y Soporte para Voice VLAN
- Seguridad: Autenticación de la red basada en IEEE 802.1x que admita acceso simple y múltiple al host, acceso de invitado, autorización de voz y Microsoft Active Directory; Protección de la contraseña de acceso al conmutador; Configuraciones definibles por el usuario para la habilitación o deshabilitación de la administración de acceso a Web, SSH, Telnet y SSL; Alerta y bloqueo de dirección MAC basados en puertos; Filtro de dirección IP para acceso de administración a través de Telnet, HTTP, HTTP/SSL, SSH y SNMP; Autenticación remota RADIUS y TACACS+ para el acceso de administración del conmutador; Admita hasta 100 listas de control de acceso (ACL), hasta 12 entradas de control de acceso (ACE) por ACL; Cifrado del SSLv3 y SSHv2 para el tráfico de la administración del conmutador; Filtrado del acceso de administración a través de perfiles
- Agregado de enlaces con soporte hasta para 18 enlaces agregados estáticos, 8 enlaces agregados dinámicos por conmutador y hasta 8 puertos miembros por enlace agregado, soporte LACP (IEEE 802.3ad), LLDP-MED
- Administración: Basada en Web, Interfaz de línea de comandos (CLI) estándar de la industria a la que se acceda a través de Telnet o puerto serial local, Admita SNMPv1, SNMP v2c y SNMPv3, Admita 4 grupos RMON (historia, estadística, alarmas y eventos), Transferencias de TFTP de firmware y archivos de configuración, Doble imagen de firmware incorporada, Admita carga/descarga de archivos de configuración múltiple, Estadística de monitoreo de errores y optimización de rendimiento que incluya cuadros de resumen de puertos, Admita administración de direcciones IP BootP/DHCP, Capacidades de registro remoto Syslog y Sensores de temperatura.

3) Equipo de Seguridad. Se deberá incluir uno (1) por cada sitio de la solución.

El servicio se deberá proporcionar mediante una solución tipo Appliance, no se aceptarán soluciones de software puro.

- Hardware: Al menos Interfaces (7) 10/100/1000 Gigabit de cobre, 2 USB, 1 Consola; Memoria Flash /RAM 32 MB/256 MB; 3G inalámbrico/módem5; Alimentación de entrada 100 a 240 V CA, 50-60 Hz; Certificaciones VPNC, ICSA Firewall 4.1; Cumplimiento de normas FCC Class A, CES Class A, CE, C-Tick, VCCI, Compliance MIC, NOM, UL, cUL, TÜV/GS, CB, NOM, WEEE, RoHS; MTBF de 28 años
- Cortafuego: Al menos un rendimiento dinámico de 500 Mbps, IPS 110 Mbps, GAV 70 Mbps, UTM 60 Mbps, IMIX 110 Mbps, Conexiones 48,000, Conexiones UTM/DPI 32,000, Conexiones nuevas/segundo 1.800 y Soporte Ilimitado de nodos
- VPN: Al menos Rendimientos de 3DES/AES4 130 Mbps; Túneles VPN entre emplazamientos de 15; Licencias GVC de 2 con crecimiento a 25; Licencias SSL VPN de 2 con crecimiento a 10; Cifrado/autenticación/grupo DH DES, 3DES, AES (128, 142, 256 bits), MD5, SHA-1/grupo DH 1, 2, 5, 14; Intercambio de claves IKE, clave manual, certificados (X.509), L2TP sobre

IPSec; Soporte de certificados Verisign, Thawte, Cybertrust, RSA Keon, Entrust y Microsoft CA, SCEP; Prestaciones VPN Dead Peer Detection, DHCP a través de VPN, IPSec NAT Traversal, pasarela VPN redundante, VPN basada en enrutamiento; Plataformas Global VPN Client soportadas Microsoft® Windows 2000, Windows XP, Vista 32/64 bits, Windows 7 32/64 bits; Plataformas SSL VPN Microsoft Windows 2000/XP/Vista 32/64 bits/Windows 7, Mac OSX 10.4+, Linux FC3+ / Ubuntu 7+ / OpenSUSE; Plataforma Mobile Connect soportada Apple® iOS 4.2 o superior, Google® Android™ 4.0 o superior

- Servicios de seguridad: Inspección profunda de paquetes Antivirus en pasarela, anti-spyware, prevención de intrusiones, inteligencia y control de aplicaciones; Content Filtering Service (CFS) Rastreo por HTTP URL, HTTPS IP, palabra clave y contenido, bloqueo de ActiveX, Java Applet, y cookies, gestión del ancho de banda según categorías de filtrado, listas de admitidos/bloqueados; Enforced Client Anti-Virus and Anti-Spyware McAfee® o Kaspersky®; Comprehensive Anti-Spam Service Soportado; Inteligencia y control de aplicaciones Visualización del tráfico de aplicaciones, gestión del ancho de banda de las aplicaciones.
- Interconexión: Asignación de direcciones IP Estática, (cliente DHCP, PPPoE, L2TP y PPTP), servidor DHCP interno, relé DHCP; Modos NAT 1:1, 1:muchos, muchos:1, muchos:muchos, NAT flexible (IPs solapadas), PAT, modo transparente; VLANS 20, PortShield; DHCP Servidor interno, relé; Enrutamiento OSPF, RIP v1/v2, rutas estáticas, enrutamiento basado en políticas, multicast; Autenticación XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, base de datos interna, servicios de terminal, Citrix; Base de datos de usuarios local de mínimo 150 usuarios; VoIP Compatibilidad total con H.323v1-5, SIP, Gatekeeper, gestión de ancho de banda saliente, VoIP sobre WLAN, seguridad de inspección profunda, interoperabilidad completa con la mayoría de los dispositivos VoIP de pasarela y de comunicaciones.
- Administración: Soporte Seguridad por zonas; Gestión basada en objetos/grupos; DDNS Proveedores de DNS dinámica (ejemplo): dyndns.org, yi.org, no-ip.com y changeip.com; Gestión y monitoreo CLI local, interfaz gráfica Web (HTTP, HTTPS), SNMP v2 y gestión global a través de software propietario de la marca; Protocolización e informes con visualización en tiempo real; Reconexión de hardware Activa/pasiva; Antispam Soporte para RBL, listas de admitidos/bloqueados; Equilibrio de carga saliente y entrante; Normas TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3 y Soporte de aceleración WAN
- Aplicación de gestión de ancho de banda: Permita asignar ancho de banda para aplicaciones críticas, mientras que se permita limitar el tráfico de aplicaciones improductivas
- Identificación de aplicaciones personalizadas: Permita crear y configurar la identificación de aplicaciones personalizadas basadas en los parámetros de tráfico o en patrones únicos a una aplicación de comunicaciones de la red.
- Análisis de tráfico de las aplicaciones: Que permita observar de manera granular el tráfico de aplicaciones, la utilización de ancho de banda y las amenazas de seguridad, además de la solución de problemas de gran alcance y capacidad de análisis forense.
- Seguimiento de la actividad del usuario: Soporte la identificación del usuario a través de Microsoft ® Active Directory y otros sistemas de autenticación que permitan el seguimiento y la notificación de la identificación de usuarios individuales.
- Geo identificación del tráfico IP: Identificar y controlar el tráfico de red que va o viene de países específicos
- Gateway anti-malware: Motor DPI (deep packet inspection) que escanee todos los puertos y protocolos en busca de virus sin importar el tamaño de archivo o la limitación de longitud de flujo.
- Inspección profunda de paquetes DPI: Permita realizar un seguimiento de malware sin importar el orden de paquetes o el momento en el que los paquetes llegan, dando como resultado una muy baja latencia, mientras que elimina la limitación en tamaño del archivos y proporcionar un mayor rendimiento y seguridad que los diseños de proxy.
- Cloud Anti-Virus (AV): Además de utilizar la base de datos integrada en el equipo, el motor DPI también debe consultar con los servicios en la nube del fabricante.
- Actualización de firmas del motor de escaneo 7x24: El fabricante debe crear y actualizar las bases de datos de firmas que se propagan automáticamente a los servidores de seguridad en

el mundo. Dicha actualización de firmas debe tener efecto inmediato sin ningún tipo de reinicio o interrupción del servicio.

- Escaneo basado en firmas: Prevención de intrusiones que analice las cargas útiles de paquetes para las vulnerabilidades y exploits que se dirigen a los sistemas críticos internos.
- Actualización automática de firmas: El fabricante debe mantener actualizada y desplegada continuamente, una base de datos de firmas de IPS. Estas firmas deben tener efecto inmediato en el appliance y no requieren reinicios o cualquier otra interrupción en el servicio.
- Prevención de amenazas de salida: La solución deberá tener la capacidad de inspeccionar el tráfico entrante y saliente, y asegurar la red contra ataques de denegación de servicio y no permitir cualquier comando de control y comunicación Botnet.
- IPSec VPN para conectividad Site-to-site: De alto rendimiento de VPN IPSec que permita que el equipo actúe como un concentrador de VPN para sitios de gran tamaño, sucursales u oficinas en casa.
- SSL VPN o Cliente IPSec de acceso remoto: Permita utilizar la tecnología VPN SSL sin cliente o con cliente IPSec, para facilitar el acceso al correo electrónico, archivos, computadoras, sitios de intranet y aplicaciones de diferentes plataformas
- Ruteo-basado en VPN: La solución debe tener la capacidad de realizar enrutamiento dinámico a través de enlaces VPN para asegurar una máxima disponibilidad en el caso de un fallo temporal en el túnel VPN, de modo que sin problemas pueda volver a enrutar el tráfico entre los puntos finales a través de rutas alternativas.
- Stateful Packet Inspection: Todo el tráfico de la red debe ser inspeccionado, analizado y puesto de conformidad con las políticas de acceso de firewall.
- Protección de ataque de DOS. (denegación de servicio): La solución debe proveer un mecanismo de protección contra ataques de denegación de servicio DOS a nivel de capa 2 y 3 SYN Flood así como mediante tecnologías de listas negras.
- Ruteo basado en Políticas: Mediante la creación de rutas basadas en el protocolo para dirigir el tráfico a una conexión WAN preferida con la posibilidad de no volver a una ruta secundaria WAN en el caso de una interrupción.
- Alta disponibilidad: Soporte el análisis de paquetes de forma Activa/Pasiva/3G Wireless USB.
- Balanceo de carga WAN: Permita el balanceo de carga de al menos 4 interfaces mediante asignación tipo “round robin”, “spillover” o métodos de procentaje.
- Interfaz de administración WEB: Consola de administración intuitiva que permita de forma sencilla hacer ajustes en la configuración.
- SNMP: Compatibilidad con el protocolo SNMP
- Administración Centralizada: Permita la administración y aplicación de políticas desde una consola centralizada del mismo fabricante.

4) Servicios e Infraestructura

- Suministro de equipos, accesorios y todo el material adecuado y necesario para una correcta instalación.
- Suministro e instalación de estructuras metálicas necesarias, así como todo el material adecuado y necesario en las estructuras metálicas para una correcta instalación. Incluyendo Instalaciones de Pararrayos y Tierra Física.
- Se entregara memoria técnica con todos los datos de la solución, así como graficas de las pruebas de tráfico.
- Póliza de servicio por 3 (tres) Años 5x8 con tiempo de respuesta máximo de 4 hrs con reemplazo avanzado de equipos.
- Garantía de tres (3) años de equipos para los incisos 1, 2 y 3
- Licencias y Actualización de software por tres (3) años en todos los equipos para los incisos 1, 2 y 3
- Carta del Fabricante en donde indique que el licitante es Distribuidor autorizado del equipo ofertado para los incisos 1, 2 y 3.
- Carta del Fabricante en donde indique que el licitante cuenta con personal capacitado y certificado para la instalación de los equipos ofertados en los incisos 1, 2 y 3.

- Todas las cartas deberán presentarse en original, no se aceptaran copias fotostáticas o impresas de formatos digitales en esta propuesta tecnica.