Anexo Técnico Renovación Equipos de Tecnología e Infraestructura Corporación Ruta N

Medellín, abril de 2023

INDICE

1. OBJETIVO:

Dar a conocer las características técnicas individuales y totales de la solución de infraestructura tecnológica mediante el modelo de renting.

2. ALCANCE:

La información presentada incluye todos los equipos tecnológicos necesarios para la operación, gestión y administración de la infraestructura tecnológica de la Corporación Ruta N,(Equipos de Seguridad Informática ,equipos de conexiones alámbricas (Switch) e inalámbricas (Access Point), Equipos de cómputo portátiles, Equipos de cómputo servidor, solución de telefonía IP, impresoras multifuncionales escáner de alta velocidad y licenciamiento) así como, las configuraciones necesarias, protocolos y licenciamientos que se deben tener en cuenta para la presentación en la convocatoria pública.

En este sentido, este documento servirá como referencia e identificación de todos los equipos solicitados para el proceso de renting tecnológico.

3. DIRIGIDO A:

Esta ficha técnica está dirigida a empresas de Tecnología con altos estándares de calidad y que son partner de los fabricantes de los equipos que se ofrecen y que cuenten con experiencia demostrada en el diseño e implementación de soluciones robustas iguales o similares al objeto, de forma tal que puedan entregar a la Corporación Ruta N respuesta completa a las necesidades planteadas.

Se contempla que la empresa también tenga un equipo de profesionales especializado, los cuales tengas las habilidades para las configuraciones de las diferentes soluciones de ciberseguridad, migración de servidores, configuraciones de redes inalámbricas, migración de plataformas de office 365 entre otros.

4. DEFINICIONES

- **Access Point:** dispositivo de red inalámbrico que permite a los dispositivos móviles conectarse a una red mediante la tecnología Wi-Fi. Básicamente, actúa como un punto de conexión entre los dispositivos inalámbricos y la red cableada.
    - **Firewall:** dispositivo de seguridad que se utiliza para proteger una red de computadoras de accesos no autorizados y posibles amenazas externas, como virus, malware y ataques de hackers.
    - **N.A.C:** herramientas o dispositivos utilizados para controlar el acceso a una red de computadoras y asegurarse de que solo los dispositivos autorizados puedan conectarse y acceder a los recursos de la red.
    - **Servidor:** Un dispositivo o sistema informático que proporciona servicios de red a otros dispositivos y sistemas, como el almacenamiento y procesamiento de datos.

- **Switch:** dispositivo de red que se utiliza para conectar múltiples dispositivos de red, como computadoras, servidores, impresoras y otros switches, en una red de área local (LAN).

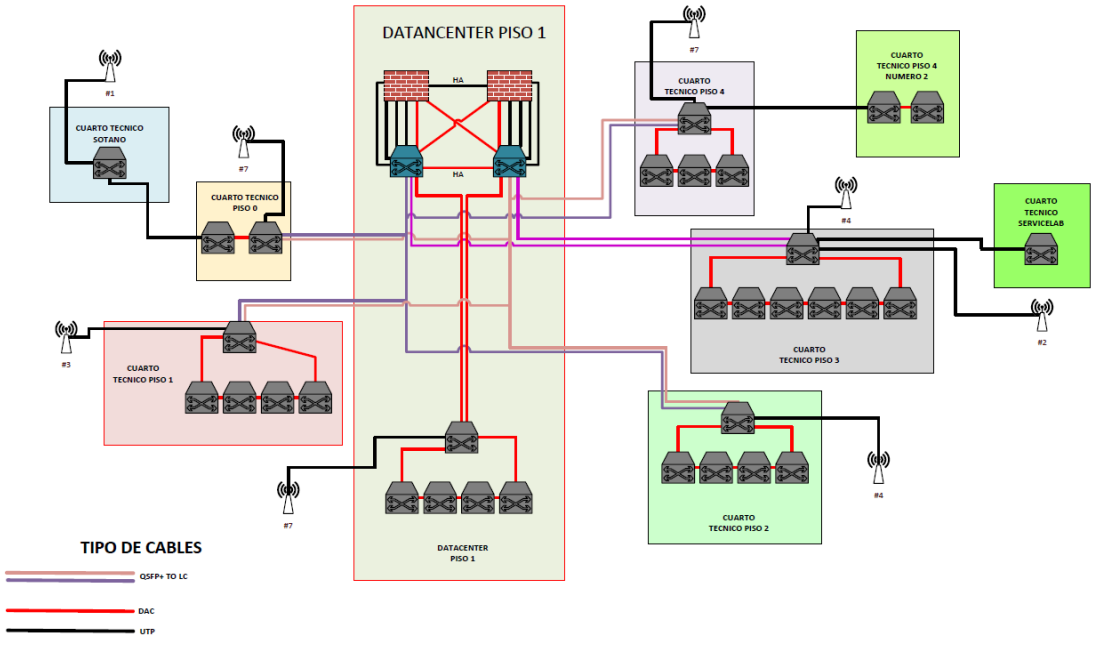
- **Topología:** La topología de red se refiere a la forma en que se conectan los dispositivos en una red de computadoras. Esencialmente, describe la estructura física o lógica de la red y la forma en que los dispositivos se conectan entre sí

- **Virtualización:** La creación de una versión virtual de un recurso informático, como un servidor o un sistema operativo, que se ejecuta en un entorno aislado y separado del hardware físico.

- **VPN:** Red privada virtual que permite a los usuarios conectarse a Internet de forma segura y privada.

5. DESCRIPCIÓN TECNICA

TOPOLOGIA CONSIDERADA PARA LA RENOVACIÓN



CANTIDAD DE EQUIPOS

- Productos de telecomunicaciones

Cantidad	Descripción
2	Equipos de seguridad (Firewall)
34	Equipos para conectividad alámbrica (Switch)
35	Equipos conexión inalámbrica (Access Point)
2	WLC Controladora de red inalámbrica (Integrada en FW)

Servicio de ingeniería instalación, configuración y puesta en marcha de la infraestructura de red, documentación de la solución según lo indicado en los términos de referencia. Además de todo el suministró de los cables y transceptores de alta velocidad para la interconexión de los equipos. La solución inalámbrica incluye network acess control

- Productos equipo de cómputo servidores, equipos de cómputo, impresoras, scanner

Cantidad	Descripción
50	Equipos portátiles gama media
5	Equipos portátiles gama alta
1	Equipo servidor
1	Impresoras Multifuncionales con canon de 5000 páginas de consumo por mes.
1	Kit Dispositivo IOT para Datacenter

Servicio de ingeniería, instalación, configuración y puesta en marcha de la infraestructura según lo indicado en los términos de referencia, migración de información en la nube usuarios OneDrive. Además de migración de máquinas virtuales para el servidor.

- Productos de solución de telefonía IP

Cantidad	Descripción
1	PBX Telefonía IP
20	Teléfonos IP

Servicio de ingeniería instalación, configuración y puesta en marcha de la de la solución de telefonía IP, configuración de teléfonos y entrega en buen funcionamiento. documentación de la solución según lo indicado en los términos de referencia.

EQUIPOS DE SEGURIDAD INFORMÁTICA

FIREWALLS DE PRÓXIMA GENERACIÓN.

Para el tráfico de la red corporativa y red landing se considera dos firewalls que puedan soportar por lo menos 50.000 conexiones simultaneas que se puedan configurar en HA, que soporte la redundancia a nivel WAN. Cada firewall debe permitir configurarse en modo virtual domain, los cuales permitirán tener varios firewalls en el mismo equipo, permitiendo la segmentación de tráfico y políticas de seguridad por separado. Con capacidad para soportar y administrar 45 APS o superior y 34 Switch para la administración y debe soportar las siguientes características.

Por funcionalidades de NGFW se entiende: Firewall, control de aplicaciones, prevención de amenazas, Filtrado de Contenido, Filtrado de DNS, DoS, identificación de usuarios, VPN IPSec, VPN SSL y prevención de fuga de información;

- Las funcionalidades de protección de red que conforman la plataforma de seguridad pueden ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación.
- Los quipos de acceso inalámbrica y switches deben de ser gestionados de forma centralizada desde dispositivo Firewall.
- La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7.
- Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19 ", incluyendo un rail kit (si sea necesario) y los cables de alimentación.
- La gestión de los equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red.
- Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q.
- Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP.
- Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding.
- Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM).
- Los dispositivos de protección de red deben soportar DHCP Relay;
- Los dispositivos de protección de red deben soportar DHCP Server;
- Los dispositivos de protección de red deben soportar sFlow;
- Los dispositivos de protección de red deben soportar Jumbo Frames;
- Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;
- Debe ser compatible con NAT dinámica (varios-a-1);
- Debe ser compatible con NAT dinámica (muchos-a-muchos);
- Debe soportar NAT estática (1-a-1);
- Debe admitir NAT estática (muchos-a-muchos);
- Debe ser compatible con NAT estático bidireccional 1-a-1;
- Debe ser compatible con la traducción de puertos (PAT);
- Debe ser compatible con NAT Origen;
- Debe ser compatible con NAT de destino;
- Debe soportar NAT de origen y NAT de destino de forma simultánea;
- Debe soportar NAT de origen y NAT de destino en la misma política
- Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico.
- Debe ser compatible con NAT64 y NAT46;
- Debe implementar el protocolo ECMP;
- Debe soportar SD-WAN de forma nativa sin requerir equipos o licenciamientos adicionales.

- Debe soportar el balanceo de enlace hash por IP de origen;
- Debe soportar el balanceo de enlace por hash de IP de origen y destino;
- Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe ser compatible con el balanceo en al menos tres enlaces;
- Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales;
- Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red;
- Enviar logs a sistemas de gestión externos simultáneamente;
- Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;
- Debe soporta protección contra la suplantación de identidad (anti-spoofing);
- Implementar la optimización del tráfico entre dos dispositivos;
- Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);
- Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);
- Soportar OSPF graceful restart;
- Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;
- Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;
- Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;
- Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;
- Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;
- Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;
- Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster;
- La configuración de alta disponibilidad debe sincronizar: Sesiones;
- La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;
- La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN;
- La configuración de alta disponibilidad debe sincronizar: Tablas FIB;
- En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;
- Debe soportar la creación de sistemas virtuales en el mismo equipo;
- Para una alta disponibilidad, el uso de clusters virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos;
- Debido que la entidad está buscando una solución de alta calidad, el fabricante de la solución deberá estar como líder en el Cuadrante Mágico de Gartner de Firewall Enterprise.
- Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales.
- Debe permitir la aceleración por hardware de funciones de seguridad, por medio de uno o varios procesadores de propósito especifico de contenido.
- Debe permitir la aceleración por hardware de funciones de Red por medio de uno o varios procesadores de propósito especifico de Red.
- La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso;
- Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos);
- El equipo debe identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas

para mejorar la seguridad general y el rendimiento;

- Debe existir la opción de un Servicio de Soporte que ofrezca a los clientes un chequeo de salud periódico con un informe de auditoría mensual personalizado de sus appliances NGFW;
- La consola de administración debe soportar como mínimo, inglés, español y portugués.
- La solución debe soportar integración con equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.

Control por Política de Firewall

- Debe soportar controles de zona de seguridad;
- Debe contar con políticas de control por puerto y protocolo;
- Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones;
- Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;
- Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad;
- Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;
- Debe soportar automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública.
- Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);
- Debe soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes
- Debe soportar el protocolo estándar de la industria VXLAN;
- La solución debe permitir la implementación sin asistencia de SD-WAN
- En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN;
- La solución debe soportar la integración con solución de sandboxing, protección de correo electrónico, cache y web application firewall.

Control de Aplicación

- Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;
- Detección de miles de aplicaciones en grupos de categorías (por lo menos 15), incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico;
- Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
- Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor;
- Para tráfico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante;
- Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;

- Actualización de la base de firmas de la aplicación de forma automática;
- Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos;
- Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;
- Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante;
- El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;
- Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;
- Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;
- Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo, permitir a Hangouts el chat, pero impedir la llamada de video;
- Debe permitir la diferenciación de aplicaciones proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;
- Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de estas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc);
- Debe ser posible crear grupos dinámicos de aplicaciones basados en características de estas, tales como: Nivel de riesgo de la aplicación;
- Debe ser posible crear grupos estáticos de aplicaciones basadas en características de estas, tales como: Categoría de Aplicación;
- Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente

Prevención de Amenazas

- Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;
- Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);
- Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante;
- Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;
- Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos;
- Deber permitir el bloqueo de vulnerabilidades y exploits conocidos
- Debe incluir la protección contra ataques de denegación de servicio;
- Debe permitir la integración nativa son soluciones de sandbox on-premise.
- Debe contar con un módulo de DoS embebido en el sistema operativo del firewall, el cual no deberá requerir licenciamiento adicional y deberá estar basado en umbrales los cuales podrán ser configurables por puerto.
- Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo;
- Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo;
- Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;
- Debe tener los siguientes mecanismos de inspección IPS: Reensamblado de paquetes TCP;
- Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets);
- Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP,

UDP, etc;

- Detectar y bloquear los escaneos de puertos de origen;
- Bloquear ataques realizados por gusanos (worms) conocidos;
- Debe permitir la inspección profunda del tráfico que se encuentre en TLS 1.3.
- Debe ser posible inspeccionar tráfico SSH y funcionalidades como Exec, Port-Fortward o X11.
- Debe permitir la integración de forma nativa con soluciones de Analista Virtual basado en Inteligencia Artificial, a fin de que se envíen archivos a este último para su análisis por medio de redes neuronales y se obtenga un listado de IP sospechas susceptibles de ser puestas en cuarentena.
- Contar con firmas específicas para la mitigación de ataques DoS y DDoS;
- Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);
- Debe poder crear firmas personalizadas en la interfaz gráfica del producto;
- Identificar y bloquear la comunicación con redes de bots;
- Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo;
- Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;
- Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos;
- Los eventos deben identificar el país que origino la amenaza;
- Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);
- Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;
- Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad;
- En caso de que el firewall pueda coordinarse con software de seguridad en equipo de usuario final (Laptop, DeskTop, etc) deberá contar con un perfil donde pueda realizar análisis de vulnerabilidad en estos equipos de usuario y asegurarse de que estos ejecuten versiones compatibles;
- Proporcionan protección contra ataques de día cero a través de una estrecha integración con componentes del tejido de seguridad, incluyendo NGFW y Sandbox (en las instalaciones y en la nube);
- El Firewall ofertado deberá tener la capacidad de integrarse de forma nativa con soluciones de engaño del tipo Deception, a fin de que se puedan contener amenazas que estén cursando en la red de la entidad.

Filtrado de Contenido

- Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora);
- Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito;
- Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;
- Debe tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL;
- Tener por lo menos 75 categorías de URL;
- Debe tener la funcionalidad de exclusión de URLs por categoría;
- Permitir página de bloqueo personalizada;
- Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado,

informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio);
- Además del Explicit Web Proxy, soportar proxy web transparente;

Identificación de Usuarios

- Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local;
- Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / controles basados en usuarios y grupos de usuarios;
- Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/controles basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc;
- Debe tener integración con RADIUS para identificar a los usuarios y grupos que permitan granularidad de las políticas de control basados en usuarios y grupos de usuarios;
- Debe tener integración LDAP para la identificación de los usuarios y grupos que permitan granularidad en la política de control basados en usuarios y grupos de usuarios;
- Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autentificación residente en el equipo de seguridad (portal cautivo);
- Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios;
- Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;
- Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;
- Debe permitir la integración con Azure AD por medio de SAML

QoS Traffic Shaping

- Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming;
- Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;
- Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;
- Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;
- Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;
- Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;
- En QoS debe permitir la definición de tráfico con ancho de banda garantizado;
- En QoS debe permitir la definición de tráfico con máximo ancho de banda;
- En QoS debe permitir la definición de colas de prioridad;
- Soportar marcación de paquetes DiffServ, incluso por aplicación;
- Soportar la modificación de los valores de DSCP para Diffserv;
- Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);

- Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes;

Prevención de Fuga de Información

- Deberá contar con un módulo de prevención de Fuga de información o DLP de Red, embebido en la solución, sin requerir ningún licenciamiento o dispositivo adicional.
- Debe Permitir la creación de filtros para archivos y datos predefinidos;
- Los archivos deben ser identificados por tamaño y tipo;
- Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones;
- Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;
- Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;
- Permitir identificar y opcionalmente prevenir la transferencia de información sensible, incluyendo, pero no limitado a, número de tarjeta de crédito, permitiendo la creación de nuevos tipos de datos a través de expresiones regulares;

Geolocalización

- Soportar la creación de políticas por geolocalización, permitiendo bloquear el tráfico de cierto País/Países;
- Debe permitir la visualización de los países de origen y destino en los registros de acceso;
- Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas;

Red Privada Virtual VPN

- Soporte VPN de sitio-a-sitio y cliente-a-sitio;
- Soportar VPN IPSec;
- Soportar VPN SSL basadas en TLS 1.3;
- La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512
- La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;
- La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);
- La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);
- Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall, Huawei;
- Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;
- Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting;
- Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy;
- Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL;
- Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;
- Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;
- Deberá mantener una conexión segura con el portal durante la sesión;

- El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS.

Virtualización

- El dispositivo deberá poder virtualizar los servicios de seguridad mediante “Virtual Systems”, “Virtual Firewalls” “Contextos” o “Virtual Domains”
- 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.
- Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual
- Se debe poder ver el consumo de CPU y memoria de cada instancia virtual.

SDWAN

- Debe soportar microsegmentación de tráfico donde sea posible, aplicar políticas de IPS y Antivirus entre segmentos de LAN
- Debe admitir NAT en el contexto de salida (NAT Outbound) a un grupo de IP públicos
- Debe proveer la capacidad de realizar inspección SSL para el tráfico https, bloqueo de malware y reconocimiento en capa 7 de aplicaciones en cada una de las sedes.
- Debe proveer gestión centralizada en Cloud propia, generar reportes tanto en el equipo como en la nube de por los menos durante los últimos 7 días.
- Debe ser capaz de ofrecer una gestión multi-tenan en la plataforma de Cloud propia
- Debe ser capaz de proporcionar Zero Touch provisioning
- La funcionalidad de Zero Touch provisioning debe ser capaz de admitir direccionamiento estático y dinámico y que se admite en varios vínculos WAN
- La funcionalidad de Zero Touch debe ser escalable, soportando un mínimo de 15 dispositivos en una misma comunidad VPN
- Debe admitir RFC7018 - ADVPN entre la sede central y las remotas con autenticación basada en estándar x.509 - Certificados digitales y también PSK
- Debe ser capaz de crear VPN "Full-Mesh" en la interfaz gráfica, de forma automática, y sin que el administrador necesite configurar sitio por sitio.
- La configuración VPN IPSEC debe admitir la versión IKE v2.0
- La configuración VPN IPSEC debe admitir DH Group: 14 y 15
- Debe ser capaz de proveer una arquitectura de Auto Discovery VPN - ADVPN (RFC 7018) donde sea posible el uso de máquinas virtuales en Cloud Pública (AWS, Azure, etc) en una topología HUB x Spoke con sus respectivas sedes
- Debe ser capaz de proveer una arquitectura de comunicación entre las sedes, de tal manera que puedan utilizar su canal local de internet para establecer una VPN con cualquier elemento de SD-WAN
- La solución, independiente en su modalidad física o virtual, debe soportar los siguientes requisitos:
  IPv6
  VRRP o Equivalente
  VRF
  BGP
  OSPF
  RIPv2
  Dy
  ic Multipath
  Policy Based Routing

Reconocimiento en capa 7
Debe, de forma alternativa, contar con una base de datos interna, donde sea posible atar una aplicación a un determinado IP / rango de IPs de destino

- El reconocimiento de aplicaciones debe actualizarse de forma dinámica y totalmente transparente en el dispositivo
- El reconocimiento de aplicaciones debe realizarse independientemente de puerto y protocolo
- Debe proporcionar el reconocimiento por defecto en la capa 7, de al menos 4000 aplicaciones ampliamente utilizadas en contextos de SaaS, Aplicaciones en la nube, aplicaciones multimedia (Vimeo, YouTube, Facebook, etc)
- La solución, en su modalidad física y / o virtual, debe considerar los siguientes:
- 802.1Q
- BFD para BGP
- Debe admitir Enrutamiento dinámico BGP con compatibilidad con IPv6
- Debe ser capaz de medir el estado de salud del enlace basándose en criterios mínimos de: Latencia, Jitter y Packet Loss, donde sea posible configurar un valor de Threshold para cada uno de estos ítems, donde será utilizado como factor de decisión en las reglas de SD-WAN
- Debe ser capaz de medir el estado de salud con soporte para múltiples servidores.
- Debe permitir modificar la configuración del tiempo de chequeo en segundos para cada uno de los enlaces
- Debe permitir la configuración de reglas donde el Failback (retorno a la condición inicial) sólo ocurrirá cuando el enlace principal recuperado sea X% (con X variando de 10 a 50) de su valor de Salud mejor que el enlace actual
- Debe permitir la configuración de reglas donde el Failback (retorno a la condición inicial) sólo ocurra dentro de un espacio de tiempo de X segundos…
- Debe permitir la configuración de políticas de QoS en la capa 7, asociadas porcentualmente al ancho de banda de la interfaz SD-WAN
- Debe permitir la configuración de políticas de QoS en valores donde el máximo corresponda a la totalidad del ancho de banda disponible en el equipo
- Debe permitir la consulta vía SNMPv2 / v3 referente a los siguientes datos:
  Estado actual de los enlaces SD-WAN
  Latencia
  Jitter
  Packet Loss
  Paquetes enviados / paquetes recibidos
  Link Bandwitdh
  VRF asociado
- Debe posibilitar la distribución de peso en cada uno de los enlaces que componen el SD-WAN, a criterio del administrador, de forma que el algoritmo de equilibrio utilizado pueda basarse en:
  Número de sesiones,
  Volumen de tráfico,
  IP de origen y destino
  desbordamiento de Enlace (Spillover)
- Debe ser capaz de admitir una arquitectura de transporte multidifusión IPv4 e IPv6 a través de túneles VPN IPSEC construidos en ADVPN.
- Debe tener la capacidad de autenticar a los usuarios para la administración del equipo a través de la base de datos:
  Local
  Integrada en el servidor TACACS +
  Integrada en el servidor Ldap
  Alternativamente debe soportar base de datos centralizada propia, donde toda la arquitectura SD-WAN converge a ella

- La Alta Disponibilidad proporcionada por La funcionalidad de SD-WAN, deberá cumplir los siguientes criterios:
  Soporta Balanceo Activo - Activo
  Soporta Balanceo Activo - Pasivo
  Soporta Balanceo de hasta 4 peers
  Soporta Balanceo Distribuido Geográficamente
- La funcionalidad SD-WAN debe ofrecer solución de problemas en la consola de línea de comandos o gráfica, donde sea posible:
  Ejecutar Packet sniffer del tráfico interesante, filtrando por: IP y Puerto
  Realizar depuración detallada de las fases de negociación VPN
- La funcionalidad SD-WAN debe ofrecer una visualización gráfica de:
- Aplicaciones más utilizadas con su ancho de banda
- Shaping de tráfico SD-WAN
- IP de destino más utilizados con su número de sesiones y ancho de banda asociados
- La funcionalidad SDWAN debe admitir la marcación de paquetes DSCP en las definiciones y reglas para el tráfico SDWAN.

Control de acceso a la red (N.A.C)

Incluye herramienta de control de acceso a la red en base a roles y a dispositivos para empleados, trabajadores eventuales y visitantes a través de cualquier infraestructura cableada, inalámbrica, donde se pueda configurar de la siguiente manera.

Especificaciones de Hardware

ESPECIFICACIONES DEL HARDWARE	DESCRIPCION
Total, interfaces de red	16 GE/RJ45 ports, 8x SFP ports and 4x 10 GE SFP+ ports
Puerto de consola	1
USB Puerto	1
Gestion dedicada 10/100/1000 Puerto	1
Factor de forma	1 montaje en rack RU
Onboard Storage	1x 480 GB SSD
Puertos de alimentación a través de Ethernet (Poe)	N/A
Presupuesto de alimentación Poe	N/A
ESPECIFICACIONES DEL SISTEMA	
IPS Troughput	5 Gbps
NGFW Throughput	3.5 Gbps
Threat Protection Throughput	3 Gbps
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	27 / 27 / 11Gbps
Firewall Latency (64 byte, UDP)	4.78 µs
Firewall Throughput (Packet per Second)	16.5 Mpps
Concurrent Sessions (TCP)	3 Millones
New Sessions/Second (TCP)	280,000
Firewall Policies	10,000
IPsec VPN Throughput (512 byte)	13 Gbps

Gateway-to-Gateway IPsec VPN Tunnels	2000
Client-to-Gateway IPsec VPN Tunnels	16,000
SSL-VPN Throughput	2 Gbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	500
SSL Inspection Throughput (IPS, avg. HTTPS)	4 Gbps
SSL Inspection CPS (IPS, avg. HTTPS)	3,500
Application Control Throughput (HTTP 64K)	300,000
CAPWAP Throughput (HTTP 64K)	13 Gbps
Virtual Domains (Default / Maximum)	10 |10
Maximum Number of Switches Supported	64
Maximum Number of APs (Total / Tunnel)	256 |128
Maximum Number of Tokens	5,000
High Availability Configurations	Active-Active, Active-Passive, Clustering
DISPOSITIVOS REQUERIDOS 2	

Cables de Conexión alta velocidad:

Los equipos de seguridad de red deben incluir los cables DAC y transceptores de alta velocidad como mínimo de 10 GE o la tecnología que según aplique y que permita realizar las conexiones necesarias entre ellos y cumpla el diseño de la topología planteada.

Licenciamiento

El equipo debe incluir las licencias necesarias para el funcionamiento de los módulos Antivirus, Seguridad IP/dominio de botnet, Seguridad móvil, Sandbox Cloud, Protección contra brotes de virus y Desarmado y reconstrucción de contenido.

Garantía: Soporte técnico hardware o software 24/7 de fábrica y garantía y actualizaciones durante la vigencia del contrato.

Ingeniería

El servicio de ingeniería que incluye instalación de los equipos en el lugar donde el supervisor del contrato lo solicite, configuración y entregada funcionando según lo requerido a todo costo.

- Configurar las políticas basadas en rutas son necesarias en la corporación para poder enrutar el tráfico hacia internet de cada VLAN dependiendo de su propósito entre los cuatro canales de internet que se tienen disponibles.
- Configurar las rutas basadas en políticas para definir por cual canal de internet saldrá cada una de las redes de Ruta N

- configurar múltiples configuraciones en capa 2, para segmentar las diferentes empresas que en Ruta N se les brinda servicios de acceso
- Múltiples configuraciones en capa 3 para garantizar el enrutamiento y la alcanzabilidad de la red desde cada uno de los pisos del edificio.
- Listas de control de acceso para denegar el acceso a la administración de los equipos desde las redes de landing y otros segmentos de red.
- Todos los centros de cableado alternos están conectados con el principal a través de enlaces dobles de fibra óptica.
- Configurar perfiles optimizados para la protección de la red, estos módulos de protección incluyen; IPS, Antivirus, Antibot y Threat Emulation, las políticas están configuradas para un buen rendimiento de los dispositivos y contemplando una capa de protección.
- Configurar la autenticación de la VPN de los usuarios se hace directamente contra el Firewall y utilizando LDAP para traer los usuarios del directorio activo.
- Configuración de Virtual Firewalls según lo solicitado por el supervisor
- Configurar balanceo de carga de los canales de internet,con un canal de mayor ancho de banda que es manejara mucha más carga; este se configuro con una prioridad del 75% y el segundo canal que se configura con una prioridad del 25% esto con el fin de obtener un mejor balanceo en el consumo de los recursos y en caso de que se presente falla en uno de ellos el otro canal asumirá todo el tráfico, La función de redundancia de ISP funciona con un script que decide la ruta para diferentes conexiones y no más allá. Solo se toman decisiones de enrutamiento.
- Configurar las política y buenas prácticas básicas de firewall recomendadas por el fabricante.
- Configurar el portal cautivo de la red invitados con la herramienta de control de acceso a la red, permitiendo el ingreso que los usuarios invitados, por medio de generación de tokens automáticos para la conexión a la red. El nombre de usuario va a ser el correo registrado con anterioridad y la contraseña será asignada aleatoriamente, la vigencia de la cuenta es de un día y no necesita de una activación previa ya que se efectúa automáticamente, luego de estar haber expirado no se podrá acceder. además configurar para la verificación de la dirección MAC en la base de datos interna de un invitado que previamente fue registrado, con el objetivo de no presentarle el portal cautivo cada vez que se conecte a la red de invitados en diferente espacios, sí y solo sí, aún está activa la cuenta.
- Para la red wifi corporativa configurar teniendo como fuente de autenticación y autorización el directorio activo de la entidad, permitiendo la conexión de los diferentes funcionarios al hacer uso de las credenciales de dominio sobre el SSID corporativo.
- Que pueda detectar dispositivos por LDAP, MAC, entre otros, y asignarle una vlan tanto de forma cableada como inalámbrica, desde la misma plataforma.
- Demas configuraciones solicitadas por el supervisor.

EQUIPOS DE CONEXIÓN ALÁMBRICA (SWITCH)

Capa de distribución:

Para esta capa se necesitan 2 switches de capa 2/3 de alta velocidad y densidad que se integre con la solución de seguridad, es decir que la administración sea centralizada y que proporcione una visibilidad y un control completos de todos los usuarios y dispositivos de la red, independientemente de cómo se conecten, además de que proporcionen enlaces ascendentes de alta velocidad a la red troncal de cara a la capa de acceso y capa Core.

- Las políticas basadas en rutas son necesarias en la corporación para poder enrutar el tráfico hacia internet de cada VLAN dependiendo de su propósito entre los 4 canales de internet que se tienen disponibles.
- Fuentes de Alimentación Duales Intercambiables en Caliente
- Soporte para paquetes Jumbo para mejorar el desempeño de grandes transferencias de datos
- Múltiples configuraciones en capa 2, para segmentar las diferentes empresas que en Ruta N se les brinda servicios de acceso
- Múltiples configuraciones en capa 3 para garantizar el enrutamiento y la alcanzabilidad de la red desde cada uno de los pisos del edificio.
- Listas de control de acceso para denegar el acceso a la administración de los equipos
- desde las VLAN de landing, entre otros
- Balanceo de carga

Seguridad: Switch que proporcione una amplia gama de características de seguridad, como el control de acceso basado en políticas (802.1X), la autenticación de puertos, la detección y prevención de intrusiones (IPS), el filtrado de paquetes y la inspección profunda de paquetes (DPI) y todo lo necesario para proteger contra amenazas de red.

Escalabilidad: Switch que este diseñado para proporcionar una alta escalabilidad y densidad.

Administración de redes: Que pueda ser también administrado a través de una consola de línea de comandos (CLI) y una interfaz web gráfica (GUI) que permite una gestión completa de la red y de los dispositivos conectados a ella.

Interoperabilidad: Que se integra perfectamente con otros productos de la solución, lo que permite una gestión y seguridad completa de la red.

Calidad de servicio: Que admita la priorización del tráfico y la gestión del ancho de banda para garantizar una experiencia de usuario óptima en la red.

Redundancia: Que admita múltiples protocolos de redundancia, como Spanning Tree Protocol (STP), Link Aggregation Control Protocol (LACP) etc, para proporcionar alta disponibilidad y protección contra fallos de red.

En resumen, un switch de capa 2/3 de alta velocidad y densidad con una amplia gama de servicios y capacidades, como seguridad, escalabilidad, administración de redes, interoperabilidad, calidad de servicio y redundancia.

Características de Hardware

ESPECIFICACIONES DEL HARDWARE	DESCRIPCION
Total, interfaces de red	24 GE/RJ45 ports, 4x 10 GE SFP+ ports and 2x 40 GE QSFP+
Puerto de consola serie RJ-45	1
Gestión dedicada 10/100/1000 Puertos	1
Factor de forma	1 montaje en rack RU

Puertos de alimentación a traves de Ethernet (Poe)	N/A
Presupuesto de alimentación PoE	N/A
ESPECIFICACIONES DEL SISTEMA	
Capacidad de conmuntacion (Duplex)	288 Gbps
Paquetes por segundo (Duplex)	428 Mpps
Almacenamiento de direcciones MAC	96K
Latencia de red	< 2µs
VLAN Compatibles	4K
Tamaño del grupo de agregacion de vínculos	24
Total de grupos de agregacion de enlaces	Hasta el número de puertos
búferes de paquetes	4 MB
DRAM	DDR3 de 2GB
FLASH	128 MB
ACL	1k
Spanning tree Instances	32
Ruta de entradas	16k/8k
Multicast Route Entries	8k
Entradas host	24k
SIWTCHES REQUERIDOS 2	

Capa de acceso

Después del análisis realizado previamente se considera utilizar tres tipos de modelos de switches para esta capa.

- Fuentes de alimentación redundantes ventiladores inteligentes para garantizar la operación estable.
- Se debe realizar el apilamiento de los switches de acceso de cada piso con la tecnología que aplique como se logra evidenciar en la topología propuesta
- Administracion centralizada desde la solucion de seguridad o la que aplique
- Se deben conectar los APS en los puertos poe del switch correspondiente y deben quedar trabajando a la maxima velocidad
- Conexiones en F.O de cara a los switches de distribucion
- Deben soportar el protocolo 802.1Q
- Conectividad de alta velocidad
- Administración de VLAN
- Características de QoS
- Seguridad de red
- Redundancia
- Múltiples configuraciones en capa 2, para segmentar las diferentes empresas que en Ruta N se les brinda servicios de acceso

Características de Hardware

ESPECIFICACIONES DEL HARDWARE	DESCRIPCION
Total, interfaces de red	24x GE RJ45 and 4x 10GE SPF+
Puerto de consola serie RJ-45	1
Gestión dedicada 10/100 Puerto	N/A
Factor de forma	1 montaje en rack RU
Puertos de alimentación a través de Ethernet (Poe)	N/A
Presupuesto de alimentación PoE	N/A
ESPECIFICACIONES DEL SISTEMA	
Capacidad de conmutación (Duplex)	128 Gbps
Paquetes por segundo (Duplex)	190 Mpps
Almacenamiento de direcciones MAC	32K
Latencia de red	< 1µs
VLAN Compatibles	4K
Tamaño del grupo de agregación de vínculos	8
Total de grupos de agregación de enlaces	16
búferes de paquetes	2 MB
DRAM	DDR3 de 512 MB
FLASH	64 MB
ACL	768
Spanning tree Instances	16
SIWTCHES REQUERIDOS 7	

ESPECIFICACIONES DEL HARDWARE	DESCRIPCION
Total, interfaces de red	48x GE RJ45 and 4x 10GE SPF+
Puerto de consola serie RJ-45	1
gestión dedicada 10/100 Puerto	N/A
Factor de forma	1 montaje en rack RU
Puertos de alimentación a través de Ethernet (Poe)	N/A
Presupuesto de alimentación PoE	
ESPECIFICACIONES DEL SISTEMA	
Capacidad de conmuntacion (Duplex)	128 Gbps
Paquetes por segundo (Duplex)	190 Mpps
Almacenamiento de direcciones MAC	32K
Latencia de red	< 1µs

VLAN Compatibles	4K
Tamaño del grupo de agregación de vínculos	8
Total, de grupos de agregación de enlaces	16
búferes de paquetes	2 MB
DRAM	DDR3 de 512 MB
FLASH	64 MB
ACL	768
Spanning tree Instances	16
SIWTCHES REQUERIDOS 20	

ESPECIFICACIONES DEL HARDWARE	**DESCRIPCION**
Total, interfaces de red	16x GE RJ45, 8x 2.5 GE RJ45 ports, 2x 5 GE RJ45, and 4x 10 GE SFP+
Puerto de consola serie RJ-45	1
gestión dedicada 10/100 Puerto	1
Factor de forma	1 montaje en rack RU
Puertos de alimentación a través de Ethernet (Poe)	24 (16x 802.3af/at, 8x 802.3af/at/UPOE)
Presupuesto de alimentación PoE	420 W
ESPECIFICACIONES DEL SISTEMA	
Capacidad de conmutación (Duplex)	128 Gbps
Paquetes por segundo (Duplex)	204 Mpps
Almacenamiento de direcciones MAC	16K
Latencia de red	< 1µs
VLAN Compatibles	4K
Tamaño del grupo de agregación de vínculos	8
Total de grupos de agregación de enlaces	Hasta el número de puertos
búferes de paquetes	2 MB
DRAM	DDR4 de 1 GB
FLASH	256 MB
ACL	1k
Spanning tree Instances	16
Entradas de ruta	1000/500
Entradas de host	2k

SIWTCHES REQUERIDOS 6

Cables de Conexión alta velocidad:

Los equipos de red deben incluir los cables DAC y transceptores SFP+ y/o QSFP como mínimo de 10 GE o la tecnología que aplique y todo lo necesario que permita realizar las conexiones entre ellos y cumpla el diseño de la topología planteada.

Garantía: Soporte técnico hardware o software 24/7 de fábrica y garantía y actualizaciones durante la vigencia del contrato.

Ingeniería

Incluye servicio de ingeniería que incluye instalación de los equipos en el lugar donde el supervisor del contrato lo solicite, configuración y entregada funcionando según lo requerido a todo costo.

Controlador de red inalámbrica (WLC)

Se necesitan dos controladoras de equipos inalámbricos (WLC) que estén integradas al firewall de administración principal que permita la gestión de por lo menos 50 AP simultáneos y configurable en HA entre FIREWALL.

- Funciones de alta movilidad con alto rendimiento, proporcionar Wi-Fi seguro de clase empresarial.
- Densidad, movilidad y confiabilidad
- Seguridad y monitoreo de RF
- Soporte para WIFI 6 y los últimos estándares wifi
- Itinerancia sin interrupciones
- **Gestión integrada de acceso de invitados**: portales de invitados alojados en el firewall, o integración con portales de 3rd party, soporte de administrador de invitados / lobby y registro automático de correo electrónico de invitados, protocolo 802.1X.
- **WID integrados:** identificación y gestión de puntos de acceso no autorizados e identificación de ataques por aire (OTA).
- **Huella digital del dispositivo:** identificación de todos los dispositivos cliente por tipo, sistema operativo y otros factores.
- **Solución remota de problemas:** desde la consola de administración se pueda ejecutar fácilmente análisis de espectro o capturas de paquetes desde puntos de acceso asociados, independientemente de la ubicación.
- **Visibilidad y control de aplicaciones de capa 7:** inspección profunda de capa 7 con más de proporcionar garantías de ancho de banda y priorización de aplicaciones críticas
- **Selección automatizada de canales y potencia:** optimizar automáticamente la selección de canales y la potencia AP Tx.

- **Gestión de la cobertura de la red inalámbrica:** proporcionar una cobertura de red inalámbrica adecuada y optimizar la cobertura mediante el ajuste de la potencia de transmisión y la optimización de la ubicación y la configuración de los AP.
- **Seguridad de la red inalámbrica:** La WLC debe tener funciones de seguridad para proteger la red inalámbrica empresarial de amenazas externas e internas, como autenticación de dispositivos, autenticación de usuarios, control de acceso a la red, detección de intrusiones y cifrado.
- **Gestión de políticas de red:** La WLC debe permitir la definición y gestión de políticas de red inalámbrica para controlar el acceso a la red, la calidad de servicio (QoS), la asignación de ancho de banda y otras funciones importantes.
- **Escalabilidad:** La WLC debe ser escalable para adaptarse al crecimiento de la red inalámbrica empresarial y ser capaz de manejar un gran número de AP y clientes.
- **Gestión de la movilidad:** La WLC debe ser capaz de gestionar la movilidad de los clientes inalámbricos en la red empresarial, lo que incluye la transferencia de los clientes entre AP sin interrupción en la conectividad.
- **Monitoreo y análisis del rendimiento**: La WLC debe tener herramientas integradas para monitorear y analizar el rendimiento de la red inalámbrica empresarial, como estadísticas de tráfico, información de clientes conectados y análisis de problemas de conectividad.

ACCESS POINT APS

Se necesitan 35 AP de última generación en 2 modelos diferentes, los detalles de estos se pueden observar en la ficha técnica. Los puntos de acceso deben de ser gestionados de forma centralizada por el controlador WLC Con la integración de la funcionalidad del controlador inalámbrico en el dispositivo Firewall.

- Monitoreo continuamente del entorno de RF en busca de interferencias, ruido y señales de AP vecinos
- **Cobertura de red inalámbrica:** Estos deben de ser instalados en las ubicaciones ya definidas o las que consideren teniendo en cuenta proporcionar una cobertura uniforme y una velocidad de conexión alta y estable.
- **Gestión centralizada:** deben permitir la gestión centralizada y la configuración desde un controlador WLAN (WLC).
- **Seguridad de la red inalámbrica:** debe tener funciones de seguridad para proteger la red inalámbrica empresarial de amenazas externas e internas, como autenticación de dispositivos, autenticación de usuarios, control de acceso a la red, detección de intrusiones y cifrado.
- **Funciones de roaming:** debe ser capaz de proporcionar funciones de roaming sin interrupción, lo que permite a los usuarios moverse por la red inalámbrica sin perder la conectividad.
- **Integración con otras soluciones de red:** debe ser capaz de integrarse con otras soluciones de red empresarial, como switches y routers, para proporcionar una gestión unificada y mejorar la eficiencia y la seguridad de la red en su conjunto.
- **Configuración y monitoreo remoto:** debe permitir la configuración y el monitoreo remoto desde un controlador WLAN o una herramienta de gestión remota, lo que permite a los administradores de red configurar y solucionar problemas desde cualquier lugar de la red.

- **Calidad de servicio (QoS):** debe ser capaz de proporcionar QoS para garantizar que las aplicaciones críticas de la empresa reciban el ancho de banda necesario para su correcto funcionamiento.
- **Escalabilidad:** debe ser escalable para adaptarse al crecimiento de la red inalámbrica empresarial y ser capaz de manejar un gran número de dispositivos móviles.

Características mínimas de Hardware

ESPECIFICACIONES	DESCRIPCION
Tipo de Hardware	AP Interior
Numero de radios	3 + 1 BLE
Numero de antenas	5 interno + 1 BLE Interno
Tipo de antena y ganancia máxima	PIFA: 4 dBi para 2,4 GHz, 5 dBi para 5 GHz
Bandas de frecuencia (GHz)	2.400–2.4835, 5.150–5.250, 5.250–5.350, 5.470–5.725, 5.725–5.850
Capacidades de Radio 2	Banda de frecuencia: 2.4 GHz Ancho de canal: 4x4 20/40 MHz Modulación: BPSK, QPSK, QAM64, QAM256 y QAM1024 Cadenas MIMO: servicio 4x4
Capacidades de Radio 2	Banda de frecuencia: 5.0 GHz Ancho de canal: 4x4 20/40/80MHz y 2x2 160MHz contiguos Modulación: BPSK, QPSK, QAM64, QAM256 y QAM1024 Cadenas Mimo: servicio 4x4
Capacidades de Radio 3	Banda de frecuencia: 2.4/5.0 GHz Cadenas MIMO: escaneo de frecuencia 1x1
Velocidad máxima de datos	Radio 1: hasta 1147 Mbps Radio 2: hasta 2402 Mbps Radio 3: solo escaneo
Radio Bluetooth de baja energía	Escaneo Bluetooth y anuncio iBeacon @ 6 dBm Potencia TX máxima
Interfaces	1x 100/1000/2500 Base-T RJ45,1 x 10/100/1000 Base-T RJ45,1x USB tipo A, 1x puerto serie RS-232 RJ45
Alimentación a través de Ethernet (PoE)	802.3at PoE predeterminado 1 puerto alimentado por 802.3at o 2 puertos alimentados por 802.3af - Funcionalidad completa del sistema + soporte USB 1 puerto está conectado a 802.3af - Sin soporte USB, Funciona en modo 2x2 con potencia reducida R1 / R2 17dBm (alimentación Tx)
SSID simultáneos	Hasta 16 (14 si el escaneo en segundo plano está habilitado)
Tipo(s) de EAP	EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST
Autenticación de usuario/dispositivo	WPA™, WPA2 y WPA3™ con 802.1x™ o clave previamente compartida, WEP, Web Captive Portal, MAC blocklist y allowlist

Potencia máxima Tx (conducida)	Radio 1: 2.4 GHz 24 dBm / 251 mW (4 cadenas combinadas) Radio 2: 5 GHz 23 dBm / 200 mW (4 cadenas combinadas)* Radio 3: NA
Cerradura Kensington	Si
Estándares IEEE	802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11w, 802.11ac, 802.11ax (Wi-Fi 6), 802.1Q, 802.1X, 802.3ad,802.3af, 802.3at, 802.3az, 802.3bz
Tipos de SSID compatibles	Puente local, túnel y malla
Capacidad por cliente de radio	Hasta 512 clientes por radio (Radio1 y Radio2)
Coexistencia celular	Si
Botón Restablecer	Si
Modo LED apagado	Si
Funciones avanzadas de 802.11	
OFDMA	Si (UL y DL)
OFDMA de 2,4 GHz	Si
Reutilización espacial (coloración BSS)	Si
Modo UL MU-MIMO 802.11ax	Si
DL-MU-MIMO	Si
HE-MU-MIMO	SI
Tiempo de activación objetivo mejorado (TWT)	Si
Capacidades de monitoreo inalámbrico	
Modos de radio Rogue Scan	Antecedentes, Dedicado
Modos de radio WIPS / WIDS	Fondo, Dedicado (recomendado)
Modo de rastreo de paquetes	Si
Analizador de espectro	Si
DISPOSITIVOS REQUERIDOS 32	

ESPECIFICACIONES	DESCRIPCION
Tipo de Hardware	AP Interior
Numero de radios	3 + 1 BLE
Numero de antenas	3 Wi-Fi interno de doble banda + 1 BLE/ZigBee

Tipo de antena y ganancia maxima	Antena PIFA Doble banda: 4.5dBi para 2.4Ghz y 5.5dBi para antena BLE de 5GHz 4.0dBi a banda de 2.4GHz
Bandas de frecuencia (GHz)	2.400–2.4835, 5.150–5.250, 5.250–5.350, 5.470–5.725, 5.725–5.850
Capacidades de Radio 2	Banda de frecuencia: 2.4GHz Ancho de canal: 20 / 40MHz Modulación: BPSK, QPSK, 64/256/1024 QAM MIMO Cadenas: Servicio 2x2
Capacidades de Radio 2	Banda de frecuencia: 5.0GHz Ancho de canal: 20/40/80MHz Modulación: BPSK, QPSK, 64/256/1024 QAM MIMO Cadenas: Servicio 2x2
Capacidades de Radio 3	Bandas de frecuencia: 2.4GHz y 5.0GHz Cadenas MIMO: 1x1 Escaneo de frecuencia
Velocidad Máxima de datos	Radio 1: hasta 574 Mbps Radio 2: hasta 1201 Mbps Radio 3: solo escaneo de frecuencia
Radio Bluetooth de baja energía	Escaneo Bluetooth y publicidad iBeacon @ 10 dBm max Alimentación TX
Interfaces	2x 10/100/1000 Base-T RJ45, 1x Tipo 2.0 USB, 1x RS-232 Puerto serie RJ45
Alimentación a través de Ethernet (PoE)	1 x 802.3at PoE predeterminado 1 x 802.af PoE sin función USB
SSID simultáneos	Hasta 16 (14 si el escaneo en segundo plano está habilitado)
Tipo(s) de EAP	EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST
Autenticación de usuario/dispositivo	WPA™, WPA2 y WPA3™ con 802.1x™ o clave previamente compartida, WEP, Web Captive Portal, MAC blocklist & allowlist
Potencia máxima Tx (conducida)	Radio 1: 2.4GHz: 23 dBm / 200 mW (2 cadenas combinadas) Radio 2: 5GHz: 22 dBm / 158 mW (2 cadenas combinadas) Radio 3: NA
Cerradura Kensington	Si
Estándares IEEE	802.11a, 802.11b, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11ac, 802.11ax, 802.1Q, 802.1X, 802.3ad, 802.3af, 802.3at, 802.3az
Tipos de SSID compatibles	Puente local, túnel y malla

Capacidad por cliente de radio	Hasta 512 clientes por radio (Radio1 y Radio2)
Coexistencia celular	Si
Botón Restablecer	Si
Modo LED apagado	Si
Funciones avanzadas de 802.11	
OFDMA	Si
Reutilización espacial (coloración BSS)	Si
Modo UL MU-MIMO 802.11ax	Si
DL-MU-MIMO	Si
Tiempo de activación objetivo mejorado (TWT)	Si
Capacidades de monitoreo inalámbrico	
Modos de radio Rogue Scan	Antecedentes, Dedicado
Modos de radio WIPS / WIDS	Fondo, Dedicado (recomendado)
Modo de rastreo de paquetes	Si
Analizador de espectro	Si
DISPOSITIVOS REQUERIDOS 3	

Cables de Conexión alta velocidad:

Los equipos de red deben incluir los cables DAC y transceptores de alta velocidad todo lo necesario que permita realizar las conexiones necesarias entre ellos y cumpla el diseño de la topología planteada.

Garantía: Soporte técnico hardware o software 24/7 de fábrica y garantía y actualizaciones durante la vigencia del contrato.

Ingeniería

Incluye servicio de ingeniería que incluye instalación de los equipos en el lugar donde el supervisor del contrato lo solicite, configuración y entregada funcionando según lo requerido a todo costo.

- Junto con la solución descrita, se debe entregar adicionalmente la siguiente información: Ingeniería de detalle de la solución implementada y las configuraciones realizadas
- Protocolo de pruebas de funcionalidades de la red
- Acta de Entrega.

SOLUCIÓN DE COMUNICACIOES UNIFICADAS DE TELEFONIA IP

Planta Telefonía IP PBX

Se requiere una plataforma de comunicaciones unificadas y colaboración de IP PBXs físico o virtual que proporcione y centralizada, incluyendo voz, videollamadas, videoconferencias, videovigilancia, reuniones web, datos, análisis, movilidad, acceso a instalaciones, intercomunicadores y más.

Que admita hasta 500 usuarios y mínimo de 50 llamadas simultaneas, e incluya una solución integrada de reuniones web y videoconferencias que permite a los empleados conectarse desde los dispositivos y teléfonos IP móviles y de escritorio,

Los teléfonos IP deben conectarse contra la PBX mediante la red interna sobre protocolo SIP estándar. Adicionalmente se debe permitir la utilización de su propio softphone o alguno externo.

Que permita la protección de seguridad avanzada con arranque seguro, certificado único y contraseña predeterminada aleatoria para proteger llamadas y cuentas.

puertos de red Gigabit RJ45 con detección automática con PoE+ integrado y modo Support NAT Router.

Suporta códec de voz Full-Band Opus y códec de video H.264/ H.263/H.263+/VP8, resistencia a la fluctuación de hasta 50% de pérdida de paquetes.

	PLANTA TELEFONIA IP FISICA
CARACTERISTICAS	**Descripción**
Puerto RJ11	Puertos FXS para Teléfono Analógico 1
Interfaces de Red	Tres puertos Gigabit auto adaptativos (conmutados, enrutados o en modo de tarjeta dual) con PoE+
NAT Router	Sí (soporta modo enrutado y modo conmutado)
Puertos Periféricos	1 Puerto USB 3.0, 1 interfaz de tarjeta SD
Interruptor de Reinicio	Sí, pulsación larga para restablecimiento de fábrica y pulsación corta para reinicio
Códecs de Voz y Fax	Opus, G.711 A-law/U-law, G.722, G722.1, G722.1C, G.723.1 5.3K/6.3K, G.726-32, G.729A/B, iLBC, GSM; T.38
Códecs de Video	H.264, H.263, H263+, VP8
QoS	Layer 2 QoS (802.1Q, 802.1p) y Layer 3 (ToS, DiffServ, MPLS) QoS
API	API completa disponible para la integración de plataformas y aplicaciones de terceros
Protocolos de Red	SIP, TCP/UDP/IP, RTP/RTCP, IAX, ICMP, ARP, DNS, DDNS, DHCP, NTP, TFTP, SSH, HTTP/HTTPS, PPPoE, STUN, SRTP, TLS, LDAP, HDLC, HDLC-ETH, PPP
Cifrado de Medios	SRTP, TLS, HTTPS, SSH, 802.1X
Funciones de Llamada	Estacionamiento de llamadas, desvío de llamadas, transferencia de llamadas, llamada en espera, identificador de llamadas, registro de llamadas, historial de llamadas, tono de llamada, IVR, música en espera, rutas de llamadas, DID, DOD, DND, DISA, grupo de extensiones, timbre de llamada simultáneo, calendario, grupos PIN, cola de llamadas, grupo de captura de llamadas, radiolocalización/intercomunicación, correo de voz, despertador, SCA, BLF, correo

	de voz a email, fax a email, marcación rápida, devolución de llamada, marcación por nombre, llamada de emergencia, modo de llamada Sígueme, lista negra/lista blanca, conferencia de voz, videoconferencia, lista de eventos, códigos de funciones, función Busy Camp-on/Call Completion, control de voz, informes posteriores a las reuniones, envío/recepción de fax virtual, email a fax
Estándares de protocolo de Internet	RFC 3261, RFC 3262, RFC 3263, RFC 3264, RFC 3515, RFC 3311, RFC 4028. RFC 2976, RFC 3842, RFC 3892, RFC 3428, RFC 4733, RFC 4566, RFC 2617, RFC 3856, RFC 3711, RFC 4582, RFC 4583, RFC 5245, RFC 5389, RFC 5766, RFC 6347, RFC 6455, RFC 8860, RFC 4734, RFC 3665, RFC 3323, RFC 3550
DISPOSITIVOS REQUERIDOS 1	

Cables de Conexión

Los equipos deben incluir todos los cables necesarios que permita realizar las conexiones para el buen funcionamiento de la solución.

Ingeniería

Incluye servicio de ingeniería que incluye instalación de los equipos en el lugar donde el supervisor del contrato lo solicite, licencia necesaria configuración y entregada funcionando según lo requerido a todo costo.

- Junto con la solución descrita, se debe entregar adicionalmente la siguiente información: Ingeniería de detalle de la solución implementada y las configuraciones realizadas
- Protocolo de pruebas de funcionalidades de la red
- Acta de Entrega.

TELEFONOS IP GAMA ALTA

teléfono IP de nivel empresarial ideal para el manejo de alto volúmenes de llamadas. hasta 12 teclas de línea/apariciones de línea y 6 cuentas de SIP utilizando LCD de pantalla a color de 4.3 pulgadas (480 x 272) y audio Full HD. El GXP2170 soporta las velocidades de conexión más rápidas posibles con puertos de red duales de Gigabit. Cuenta con PoE integrado y Bluetooth incorporado para la sincronización con dispositivos móviles y auriculares Bluetooth, así como la capacidad de conectar/alimentar hasta 4 módulos de extensión en cascada con pantalla LCD para acceder marcación rápida/contacto BLF de hasta 160.

	TELEFONOS IP GAMA ALTA
CARACTERISTICAS	**Descripción**
Protocolos/Normas	SIP RFC3261, TCP/IP/UDP, RTP/RTCP, HTTP/HTTPS, ARP, ICMP, DNS(un registro, SRV, NAPTR), DHCP, PPPoE, SSH, TELNET, TFTP, NTP, STUN, SIMPLE, LLDP, LDAP, TR- 069, 802.1x, TLS, SRTP, IPV6, CDP/SNMP/RTCP-XR
Interfaces de Red	Puertos Gigabit Ethernet de doble encendido y autodetección de 10/100/1000 Mbps con PoE integrado.
Visualización gráfica	LCD a color de 4.3 pulgadas (480x272) TFT
Bluetooth	Si, integrado
Teclas de función	12 teclas de línea con hasta 6 cuentas de SIP, 5 XML de contexto sensible programable teclas de función, 5 teclas de navegación/menú, 11 teclas de función dedicadas para: MENSAJE (con indicador LED), AGENDA, TRANSFERENCIA, CONFERENCIA, RETENCIÓN, AURICULARES, MUDO, ENVIAR/REMARCAR

Códecs voz	Soporte para G7.29A/B, G.711µ/ley a, G.726, G.722 (banda ancha), G723.1, iLBC, Opus, DTMF dentro de banda y fuera de banda (en audio, RFC2833, SIP INFO), VAD, CNG, AEC, PLC, AJB, AGC
Características de telefonía	Retener, transferir, reenviar, conferencia de 5 vías, detener llamadas, capturar llamadas, aparición de llamada compartida (SCA)/aparición de línea en puente (BLA), agenda telefónica descargable (XML, LDAP, hasta 2000 artículos) llamada en espera, registro de llamadas (hasta 500 registros), personalización de XML de la pantalla, marcado automático al descolgar, respuesta automática, clic para marcar, plan de marcado flexible, escritorio rápido, tonos de llamada de música personalizados y música de espera, redundancia del servidor y conmutación por error
Audio HD	Sí, auricular y altavoz HD con soporte para audio de banda ancha
Módulo de extensión	Sí, puede alimentar hasta 4 módulos
QoS	QoS de la capa 2 (802.1Q, 802.1P) y QoS de la capa 3 (ToS, DiffServ, MPLS)
Seguridad	Contraseñas del usuario y del administrador, autenticación basada en MD5 y MD5-sess Archivo de configuración de cifrado AES de 256 bits, SRTP, TLS, control de acceso de medios de 802.1x
Idiomas múltiples	Inglés, alemán, italiano, francés, español, portugués, ruso, croata, chino, coreano, japonés
Adicional	auricular con cable, soporte de base, fuente de alimentación universal, cable de red, guía de instalación rápida, licencia GPL
DISPOSITIVOS REQUERIDOS 1	

Módulo de Extensión

ofrece funcionalidad, versatilidad y flexibilidad adicionales a los teléfonos IP cuenta con una pantalla gráfica LCD de 128 x 384 y 20 botones programables (cada uno con LED bicolor). Permite hasta 40 extensiones por módulo usando las dos teclas de cambio de página.

	Módulo de Extensión
CARACTERISTICAS	**Descripción**
Líneas	20 (Hasta 40 con 2 teclas de cambio de página
Soporte de Características	Interfaz Gráfica de Usuario local accionada desde el teléfono base
Energía	Los módulos de expansión son activados por el teléfono base
Actualizaciones de Firmware	Proporcionadas por el teléfono base.
DISPOSITIVOS REQUERIDOS 1	

TELEFONOS IP GAMA MEDIA

teléfono IP de gama media con funciones de telefonía avanzadas. Este teléfono IP de rango medio viene equipado con 8 líneas, 4 cuentas SIP, 8 teclas de línea bicolor y 4 teclas XML programables, sensibles al contexto en una pantalla LCD de 200 x 80 pixeles (3.3") con luz de fondo. Para personalización tono de llamada/tono de espera con música personalizada e integración con aplicaciones Web y empresariales avanzadas, soporta las velocidades de conexión más rápidas posibles con dos puertos de red Gigabit con detección automática, como funciones de aprovisionamiento automático con control de acceso a medios.

	TELEFONOS IP GAMA MEDIA
CARACTERISTICAS	**Descripción**

Protocolos/Normas	SIP RFC3261, TCP/IP/UDP, RTP/RTCP, HTTP/HTTPS, ARP, ICMP, DNS (A record, SRV, NAPTR), DHCP, PPPoE, SSH, TELNET, TFTP, NTP, STUN, SIMPLE, LLDP, LDAP, TR-069, 802.1x, TLS, SRTP, IPV6
Interfaces de Red	Puertos Gigabit Ethernet de doble encendido y autodetección de 10/100/1000 Mbps con PoE integrado.
Visualización gráfica	Pantalla LCD de 200 x 80 pixeles (3.3'') con luz de fondo
Bluetooth	No
Teclas de función	8 teclas de línea con hasta 4 cuentas SIP, 4 teclas XML programables, sensibles al contexto, 5 teclas de navegación/menú, 8 teclas de función dedicada para: DIRECTORIO TELEFÓNICO, TRANSFERENCIA, CONFERENCIA, AURICULAR, SILENCIO, ENVIAR/REMARCAR, ALTAVOZ, VOLUMEN
Códecs voz	Soporte para G.729A/B, G.711µ/a-law, G.726, G.722 (banda ancha), G.723, iLBC, OPUS, DTMF en banda y fuera de banda (audio de entrada, RFC2833, SIP INFO), VAD, CNG, AEC, PLC, AJB, AGC
Características de telefonía	Retención, transferencia, desvío, conferencia de 5 participantes, estacionamiento de llamadas, recuperación de llamadas, estado de llamada compartida (SCA)/estado de línea en puente (BLA), directorio telefónico descargable (XML, LDAP, hasta 2000 contactos), llamada en espera, registro de llamadas (hasta 500 registros), personalización XML de la pantalla, marcación automática al descolgar, respuesta automática, hacer clic para marcar, plan de marcación flexible, hot desking (estaciones de trabajo compartidas), tonos de llamada con música personalizada y música en espera, redundancia de servidores y conmutación por error
Audio HD	Sí, auricular y altavoz HD con soporte para audio de banda ancha
QoS	Layer 2 QoS (802.1Q, 802.1P) y Layer 3 (ToS, DiffServ, MPLS) QoS
Seguridad	Contraseñas a nivel del usuario y administrador, autenticación basada en MD5 y MD5-sess, archivo de configuración cifrado con AES de 256 bits, SRTP, TLS, 802.1x Media Access Control, soporte de conector de seguridad Kensington (Kensington Lock)
Idiomas múltiples	Inglés, alemán, italiano, francés, español, portugués, ruso, croata, chino, coreano, japonés
Energía	Adaptador de corriente universal incluido: Entrada:100-240V; Salida: +5V, 1A; Power-over-Ethernet Integrado (802.3af); consumo máximo de energía: 5W
DISPOSITIVOS REQUERIDOS 20	

Cables de Conexión

Los equipos deben incluir todos los cables necesarios que permita realizar las conexiones para el buen funcionamiento de la solución.

Garantía: la solución de telefonía (planta, teléfonos y accesorios) deben tener soporte técnico y garantía durante la vigencia del contrato.

Ingeniería

Incluye servicio de ingeniería que incluye instalación de los equipos en el lugar donde el supervisor del contrato lo solicite, licencias necesarias, configuración y entregada funcionando según lo requerido a todo costo.

EQUIPOS DE COMPUTO

Equipo de cómputo Servidor

Requisitos mínimos de hardware

	SERVIDORES ON PREMISE
CARACTERISTICAS	**Descripción**
Chasis Dimensiones	Rackeable Tiene un chasis adaptable, que incluye las nuevas opciones de configuración de bahías de unidades modulares Chasis de factor formato reducido: 4,29 x 43,46 x 70,7 cm, Chasis de factor formato grande: 4,29 x 43,46x 74,98 cm
Procesador	Procesador (16 núcleos)
	Frecuencia básica del procesador 2,40 GHz, Frecuencia turbo máxima 3,40 GHz, cache 24 Mb
Memoria	Cantidad total 96 GB DDR4 (32 GB cantidad 3) , Memoria persistente 3 TB (24 X 128 GB) LRDIMM 6 TB (12 X 512 GB
Disco Duro	Cantidad total 7.2 TB 2.4 TB SAS 12g, Mission Critical, 10K rpm, small form factor, (CANTIDAD 3)
Tarjeta de Red	Adaptador Ethernet PCIe x8 Gen2 de 2 puertos a 10 Gb
Controladora de almacenamiento	Smart Array P408i-a SR Gen10 (8 Internal Lanes/2GB Cache) 12G SAS Modular Controller
Fuente	Fuente de alimentación hot-plug de bajo contenido en halógenos y ranura flexible de 800 W (cantidad 2)
Administración de infraestructura	iLO (Integrated Lights-Out) Advanced
Evaluación Ambiental	Energy Star EPEAT Gold ROHS
Servicio de garantía	4 años de garantía. Duración certificada por el fabricante. Cobertura de mano de obra, partes y atención en sitio al siguiente día laboral. El servicio debe incluir una herramienta para la detección predictiva (no reactiva) con notificación de fallas.
DISPOSITIVOS REQUERIDOS 1	

Generalidades

EQUIPOS DE CÓMPUTO PORTÁTILES

Equipos portátiles corporativos de alto rendimiento, delgado los cuales puedan soportar tareas informáticas intensivas, como análisis de datos o diseño gráfico con facilidad y gráficos potentes. altavoces Dolby Audio orientados al usuario, Dolby Voice AI La tecnología de supresión de ruido mejora la experiencia del usuario durante las videoconferencias. además, debe tener variedad de puertos incluidos como Thunderbolt 4, Rj45 integrado. Además de contar con certificaciones ambientales que puedan reducir la huella de carbono.

Requisitos de Hardware

Referencia	PORTÁTILES – ADMINISTRATIVO GAMA MEDIA
CARACTERISTICAS	Descripción
Chasis	Slot para cable de seguridad Kensington/noble.
	Equipo Tipo dockeable con soluciones de tipo USB tipo C que permitan la transmisión de energía, video y datos a través de la solución.
	Chip TPM 2.0 discreto/integrado
	Certificación de durabilidad MIL-STD-810H
Pantalla	14 pulgadas en diagonal
	Bisel estrecho
Peso	Máximo 1.39kg
Sistema Operativo	Windows 11 Professional Downgrade Windows 10 Professional
Recuperación de Sistema Operativo	Vía Nube, para evitar ocupar espacio en el disco duro, descargable vía USB.
BIOS	BIOS, propietario del fabricante o con derechos reservados para su uso. En español o inglés UEFI BIOS. De la misma marca del fabricante del equipo.
	BIOS con funcionalidad de auto recuperación a través de copia de reserva alojada en chip o disco duro del sistema en caso de ataques y que permite verificar la integridad de la BIOS a través de fuentes externas.
	De la misma marca del fabricante del equipo con marca troquelada o grabada en la tarjeta.
Procesador	Intel Core i5-1235U. 10 núcleos (2 núcleos de desempeño y 8 núcleos de eficiencia, frecuencia turbo de desempeño/eficiencia de 4.4 GHz/3.3 GHz cada una, frecuencia base de desempeño/eficiencia de 1.3 Ghz/0.9 GHz cada una)
	La fecha de lanzamiento del procesador no debe ser anterior al año 2022.
Memoria	16GB (1x16GB) DDR4 3200MHz
Disco D uro	256 GB M.2 PCIe NVMe M.2 2242
Tarjeta Wifi	Wireless card 802.11ax con Bluetooth 5.1
Audio	2 parlantes de 2W con certificación Dolby® Audio™ y arreglo dual de micrófonos far-field Dolby Voice
Puertos	2 USB 3.2 Gen 1 tipo A o superior al menos uno con tecnología de Carga

	1 puerto USB-C 3.2 Gen 1 con soporte a transferencia de datos, paso de carga y DisplayPort 1.4
	1 puerto Thunderbolt 4 Tipo C
	1 puerto HDMI integrado
	1 puerto RJ-45 integrado
	1 puerto Audio Jack
	Cámara web FHD con obturador de privacidad mecánico.
Batería	Batería con capacidad de mínimo 42Wh con soporte a carga rápida.
Adaptador de corriente	Adaptador externo USB-C
Display	Pantalla de 14" con resolución FHD (1920x1080).
Teclado	Integrado con resistencia a derrames y salpicaduras.
Touchpad	Touchpad en chasis del equipo.
Evaluación Ambiental	ENERGY STAR
	Registrado en EPEAT en mínimo categoría Gold.
	Sin BFR/PVC9
Servicio de garantía	4 años de garantía Prestada por el fabricante. Duración certificada por el fabricante. Cobertura de mano de obra, partes y atención en sitio al siguiente día laboral.
	El equipo debe poder ser administrado con herramientas de Gestión mediante el protocolo Simples equipos deben contener herramienta tecnológica que haga uso de las nuevas tecnologías de predicción de fallas de hardware. Dicha herramienta debe tener consola única en para consultar u operar en línea, que monitoree en tiempo real de manera predictiva los componentes de los equipos como: procesador, memoria, discos, baterías, placa principal, crashes de sistema operativo (pantalla azul) con detalles del incidente y recomendaciones de remediación. La plataforma debe enlazar con la solicitud de tiquets de soporte de garantía del fabricante de manera automática. Esta herramienta deberá ser nativa del fabricante de los equipos. anexar certificación. la funcionalidad de la plataforma no deberá ser menor a un periodo de la garantía solicitada para los equipos.
EQUIPOS REQUERIDOS: 50	

Programas y configuraciones

- Instalación de semilla de sistema operativo y actualización.
- Instalación de Programas básicos según lo indicado por el supervisor del contrato.
- Migración de OneDrive a los nuevos equipos corporativos.
- Acta de Entrega.

Equipos portátiles diseño

Referencia	PORTÁTILES – GAMA ALTA
CARACTERISTICAS	**Descripción**
Pantalla	Pantalla Liquid Retina XDR de 14,2 pulgadas (diagonal)1; resolución nativa de 3024 x 1964 a 254 pixeles por pulgada
Peso	Máximo 1.6 kg
Sistema Operativo	Mac OS última versión
AUDIO	Sistema de sonido de seis parlantes de alta fidelidad con woofers con cancelación de fuerza Amplio sonido estéreo.
	Sistema de tres micrófonos con calidad de estudio, alta relación señal/ruido y tecnología beamforming direccional
Procesador	CPU de 10 núcleos con 6 núcleos de rendimiento y 4 de eficiencia Chip M2 Pro, GPU de 16 núcleos Neural Engine de 16 núcleos, 200 GB/s de ancho de banda de memoria
Memoria	Memoria unificada de 16 gb
Disco Duro	SSD de 512 GB
Cámara	Cámara FaceTime HD de 1080p
Tarjeta Wifi	Conexión inalámbrica Wi-Fi 6 802.11ax, Bluetooth 5.3
Reproducción de video	Los formatos compatibles incluyen HEVC, H.264 y ProRes HDR con Dolby Vision, HDR10 y HLG
Reproducción de audio	Los formatos compatibles incluyen AAC, MP3, Apple Lossless, FLAC, Dolby Digital, Dolby Digital Plus y Dolby Atmos
Puertos	Puerto HDMI Entrada de 3,5 mm para audífonos Puerto MagSafe 3 Ranura para tarjeta SDXC
	Tres puertos Thunderbolt 4 (USB-C) compatibles con: Carga , DisplayPort , Thunderbolt 4 (hasta 40 Gb/s), USB 4 (hasta 40 Gb/s)
Batería **Adaptador de corriente**	Batería de polímero de litio de 70 Wh3 , Adaptador de corriente USB-C de 67 W Adaptador de corriente USB-C de 67 W
Teclado	Keyboard retroiluminado con 65 (EE.UU.) o 66 (ISO) teclas, incluidas 4 teclas de flecha en forma de “T” invertida
Touchpad	Touch ID
Servicio de garantía	Garantía durante la vigencia del contrato por cobertura de mano de obra, partes y atención en sitio al siguiente día laboral.

DISPOSITIVOS REQUERIDOS 5

Programas y configuraciones

- Instalación de semilla de sistema operativo y actualización.
- Instalación de Programas básicos según lo indicado por el supervisor del contrato.
- Migración de OneDrive a los nuevos equipos corporativos.

IMPRESORA MULTIFUNCIONAL

Impresoras multifuncional con canon de 5000 página por mes.

Referencia	IMPRESORA MULTIFUNCIONAL
CARACTERISTICAS	**Descripción**
Resolución	1200 x 1200 ppp
Dimensiones A x P x H	18.7 "x 17.4" x 20.1 "(476 mm x 442 mm x 510 mm)
Peso	67.24 lbs. (30.5 kg)
Pesos de papel admitidos	Bandejas: 14 - 58 lb. Bond (52 - 220 g / m²) Derivación: 14 - 68 lb. Bond (52 - 256 g / m²) Dúplex: 14 - 43 lb. Bond (52 - 162 g / m²)
Panel de control	10.1 "panel de operación inteligente
Cantidad máxima de copias	Hasta 999 copias.
Capacidad de salida estándar	250 hojas
Tamaños de papel admitidos	Bandejas de papel estándar: 5.5 "x 8.5" - 8.5 "x 14" (A6-A4, B6-B5) Bandejas de papel opcionales: 5.5 "x 8.5" - 8.5 "x 14" (A6-A4 , B6-B5) Bandeja bypass: 5.5 "x 8.5" - 8.5 "x 14" (A6-A4, B6-B5) Tamaños personalizados - Ancho: 2.36 "- 8.5" (60 - 216 mm), Longitud: 5.0 " - 35.43 "(127 - 900 mm)
Memoria del sistema	2 GB de RAM / 320 GB HDD
Tipos de papel admitidos	Liso, Reciclado, Especial, Coloreado, Papel con membrete, Cartulina, Preimpreso, Bond, Revestido, Sobre, Etiqueta, OHP
Velocidad de salida Copiar / Imprimir	45 ppm (formato carta)
Capacidad máxima de papel	2,100 hojas
Capacidad de papel estándar	500 hojas

Interfaces	Estándar: Ethernet 10 base-T / 100 base-TX / 1000 base-T, USB Host 2.0 Opcional: LAN inalámbrica (IEEE 802.11a / b / g / n), NIC adicional (2do puerto), placa USB extendida, archivo Convertidor de formato
Especificaciones del escáner	
Modos de escaneo	E-mail, Carpeta, USB, Tarjeta SD
Velocidad de escaneo BW a todo colo	45.7 ipm
Formatos de archivo	TIFF de una sola página, JPEG de una sola página, PDF de una sola página, PDF de alta compresión de una sola página, PDF / A de una sola página, TIFF de múltiples páginas, PDF de varias páginas, PDF de alta compresión de varias páginas, PDF de varias páginas / A
Resolución de escaneo	600 dpi
Garantía	Garantía durante la vigencia del contrato por cobertura de mano de obra, partes y atención en sitio al siguiente día laboral.
Canon impresión	Debe incluir un canon de 5000 páginas impresas por mes
DISPOSITIVOS REQUERIDOS 1	

SISTEMA IOT PARA DATACENTER

Suministro e instalación de dispositivo interfaz IoT para vincular de forma inteligente el Datacenter con el objetivo de gestionar las condiciones de temperatura, humedad relativa, acceso y gestión energética, a través de sensores para ejecutar órdenes de mando y la alimentación/regulación de energía.

Con el fin de contar con administración remota del DataCenter, se debe de contar con un dispositivo interfaz IoT que permita vincular de forma inteligente soluciones, sensores, integración de interfaces y protocolos para la recopilación y transmisión de datos a sistemas TI superiores o a sistemas para el control local de los estados de las máquinas.

Debe permitir la digitalización y la interconexión de forma sencilla, la interfaz debe permitir la conexión de soluciones de climatización y sensores para el control de condiciones ambientales físicas tanto para DataCenter tipo office, como para entornos industriales 4.0, sin interferir en la lógica de automatización.

Debe ser una solución Plug and run: la configuración y puesta en marcha del dispositivo interfaz IoT se realiza de forma rápida, con sensores del mismo fabricante, de tal forma que permitan la integración plug and play, permitiendo poder crecer en la solución sin desarrollo de terceros.

Debe estar fabricado en material UL 94-V0 que garantice la seguridad ante inflamabilidad.

Debe soportar Cable USB conector USB

Borne de conexión con sistema push-in (24 V c.c.)

Debe contar con redundancia, debe soportar al menos 2 x RJ45 CAN-Bus

"Debe contar con conexión de red, debe soportar Ethernet IPv4/IPv6 10/100/1000

Debe de soportar mínimo 32 Sensores"

"Debe contar con mínimo

1 Micro USB tipo B (dispositivo) para USB 2.0 1 ranura para tarjeta micro SD para SD 2.0

1 USB 2.0 de alta velocidad (EHCI)

1 botón de confirmar

1 borne de conexión con sistema push-in para sensor NTC

2 conectores adicionales a los de Red y CAN-Bus RJ45 para interfaz RS 485 (interfaz refrigerador)"

La solución de monitoreo no debe usar unidades de Rack, debe funcionar de forma transversal, e integrarse a la solución existente.

"Debe soportar los protocolos. OPC-UA SNMPv1 SNMPv2c SNMPv3 Modbus/TCP TCP/IPv4 TCP/IPv6 Radius Telnet

SSH FTP SFTP HTTP HTTPS NTP DHCP DNS SMTP Syslog LDAP"

Debe contar con amplio rango de funcionamiento de temperatura, entre 0 y 70°C

Se debe de contar con una Fuente de alimentación que no consuma unidades de rack, que sea tipo Door Control con conector tipo DataCenter C13

Debe soportar humedad de entre 5 y 95%

Se debe de contar con al menos un sensor de temperatura y un sensor de humedad

El sensor debe de contar con Conector 2xRJ45 y debe de soportar protocolo CAN bus

Debe contar con certificación UL + C-UL, EAC

Protección IP 30 - IEC 60 529

Debe contar con sensores antivandálicos

El sensor debe de contar con Conector 2xRJ45 y debe de soportar protocolo CAN bus

Debe ser liviano, con un peso no mayor a 200gr para uso flotante

Debe contar con todos los cables y accesorios requeridos para poner en funcionamiento la solución

Debe de contar con Iluminación LED de 11W, Iluminación de 4000 K (blanco neutro), debe de contar con IP20, Debe de contar con luminaria: aluminio extrusionado, Cubierta de la iluminación: policarbonato

demás material en PC-ABS"

Debe de contar con accesorios de tal forma que permita el encendido de iluminación automático al detectar la apertura de las puertas

Se debe de contar con un sistema de control de acceso

El sensor debe de contar con Conector 2xRJ45 y debe de soportar protocolo CAN bus

Debe de contar con conector Rj12, Debe de contar con Sensor de Acceso IR integrado para detección de puerta abierta y/o cerrada

Debe soportar interfaz Web y administración remota, con soporte de Dashboard para administración vía HTTPS, con envío de alertas vía email en caso de detección de alertas.

Todos los elementos de la solución IOT deben tener soporte y garantía durante la vigencia del contrato

DISPOSITIVO IOT DATACENTER	
Estribo para gestión de cableado 6 UA	1
DK POWERBOX DIN 43880	1
IoT Interface	1
CMC III Fuente de alimentación	1
CABLE DE UNION C13/C14	1
CMCIII Sensor térmico/de humedad	1
CMCIII Sensor actos vandálicos	1
Cable de conexión CMC III CAN-Bus RJ 45	2
CMCIII CABLE CONEXION CAN-BUS RJ45, 1,5	2
CMCIII Cable de conexión CAN-Bus RJ 45,	1
CS CILINDRO MEDIO	2
CMC III Access Control	2
CMC III Lector transponder VX RAL 9005	1
SZ Luminaria LED 900 S/Enchufe 100-240V	1

SZ Cable de conexión para iluminación LE	1
SZ Interruptor de puerta, cable 800mm	1
Guía de deslizamiento 150kg prof. 600-90	1
Kit para DET-AC Plus y EFD Plus	1
CMC-TC SENSOR DE ACCESO	1
Juego de estanqueidad para TS IT y LCP e	1

LICENCIAMIENTO

Cantidad	Descripción	Duración
1	Licenciamiento software de monitoreo de infraestructura (48 meses) mínimo 500 sensores.	48 meses
100	licencia de Backup office 365	48 meses
100	Solución de seguridad endpoint	48 meses
2	Virtualización de Sistemas Operativos	48 meses
2	licencias Windows Server Standard última versión	48 meses
100	Licencias cal por dispositivo	48 meses

Licenciamiento software de monitoreo de infraestructura (1): La corporación cuenta con una herramienta de monitoreo de red y sistemas altamente efectiva y personalizable que proporciona una visibilidad completa de la infraestructura de TI y ayuda a los administradores de TI a detectar y solucionar problemas, esta herramienta actualmente se encuentra instalada en la nube del proveedor, también se cuenta con una sonda remota para monitorear los dispositivos que se encuentren en la red lan. se requiere monitorear por lo menos 50 dispositivos y 500 sensores, la herramienta debe contar con las siguientes características y funciones.

Características:

- Mapas y paneles de control
- Informes personalizables
- Alertas y notificaciones personalizables
- Monitoreo distribuido
- múltiples interfaces de usuario
- Descubrimiento automático de red
- Compatible con las principales tecnologías
- Ping,snmp, WMI, SSH, solicitudes HTTP y más
- Protocolos de flujo (IPFIX, jFlow, sFlow y NetFlow)
- Monitoreo de LAN, WAN, servidores y más
- Supervisión sitios web, aplicaciones, servicios y más
- El tráfico total

- El tráfico web (HTTP, HTTPS)
- El tráfico de correo (IMAP, POP3, SMTP)
- File transfer traffic (FTP, P2P)
- La infraestructura del tráfico (DHCP, DNS, ICMP, SNMP)
- El control remoto (RDP, SSH, VNC)
- Otro tráfico UDP y TCP
- Monitoreo de servicios Microsoft 365
- métodos de notificación integrados (correo electrónico, push, solicitudes HTTP y demás)
- umbrales personalizados para el monitoreo
- Debe contar con una API
- Acciones activadas por eventos
- Alerta de limites

Funcionalidades:

- **Monitoreo de red:** monitoreo todo el tráfico de red, incluyendo el ancho de banda, los paquetes de datos, los errores y las interrupciones.
- **Monitoreo de servidores:** monitoreo del rendimiento de los servidores, incluyendo el uso de CPU, memoria y disco duro.
- **Monitoreo de aplicaciones:** monitoreo del rendimiento de las aplicaciones en tiempo real, lo que permite detectar problemas antes de que afecten a los usuarios finales.
- **Monitoreo de dispositivos:** monitoreo de una amplia gama de dispositivos de red, incluyendo routers, switches, firewalls, impresoras y más.
- **Alertas en tiempo real:** envió de alertas por correo electrónico, SMS o notificaciones push en caso de que se detecte un problema.
- **Un panel de control único**: el cual monitorea todos los sistemas, dispositivos, aplicaciones, tráfico y más de su infraestructura de TI en una herramienta de monitoreo central.
- **Mapas de red personalizados:** permite crear mapas de red personalizados para visualizar la topología de la red y el estado de los dispositivos.
- **Integración de SNMP:** compatible con el Protocolo Simple de Administración de Red (SNMP) para recopilar y analizar datos de dispositivos de red.
- **Integración de APIs:** se integra con APIs de diferentes proveedores y aplicaciones para recopilar y analizar datos específicos.
- **Análisis histórico:** almacena los datos históricos de la red y los sistemas, lo que permite a los usuarios realizar análisis y comparaciones a largo plazo
- **Interfaz de usuario fácil de usar:** interfaz intuitiva y fácil de usar que permite a los usuarios monitorear y analizar datos de manera eficiente.
- **Personalización:** se puede personalizar para satisfacer las necesidades específicas de los usuarios, lo que permite monitorear solo lo que es importante.
- **Informes detallados:** generar informes detallados sobre el rendimiento de la red y los sistemas, lo que permite a los usuarios analizar datos de manera efectiva.

- **Escalabilidad:** escalable y puede manejar grandes redes y sistemas.
- **Integración con otros sistemas:** se integra con una amplia gama de sistemas y herramientas, lo que lo hace altamente compatible con otras soluciones de TI.

licencia de copia de seguridad para office 365 (100): solución de respaldo y recuperación de datos para entornos de Office 365. Protege datos de herramientas de Microsoft Teams, Exchange Online, OneDrive for Business y SharePoint.

- **Solución de seguridad endpoint CLOUD para 100 usuarios**

Actualmente se cuenta con una solución de seguridad basada en la nube que ofrece una serie de características y funcionalidades para proteger los sistemas de la organización contra amenazas cibernéticas. Algunas de sus características y funcionalidades son:

- **Protección de endpoints:** protege los endpoints, como computadoras portátiles y de escritorio, servidores y dispositivos móviles, contra virus, malware, ransomware y otras amenazas.
- **Análisis de comportamiento:** La solución utiliza análisis de comportamiento para detectar y bloquear amenazas que intentan aprovechar vulnerabilidades en el sistema.
- **Prevención de la pérdida de datos:** incluye funciones de prevención de la pérdida de datos para evitar que la información confidencial se filtre fuera de la red.
- **Protección de la navegación web:** La solución bloquea el acceso a sitios web maliciosos conocidos y protege contra ataques de phishing.
- **Seguridad móvil:** también protege los dispositivos móviles, incluidos teléfonos inteligentes y tabletas, contra amenazas y ofrece funciones como el control de acceso remoto y la eliminación remota de datos.
- **Actualizaciones automáticas:** La solución se actualiza automáticamente con las últimas definiciones de virus y parches de seguridad para garantizar una protección óptima contra las amenazas más recientes.
- **Firewall personal:** incluye un firewall personal que controla el tráfico de entrada y salida de la red, y protege los dispositivos contra ataques de red.
- **Prevención de intrusiones:** utiliza tecnología de prevención de intrusiones para bloquear ataques de día cero y otras amenazas avanzadas.
- **Control de dispositivos:** permite a los administradores de TI controlar el acceso a dispositivos externos, como unidades USB y discos duros externos, para prevenir la pérdida de datos.
- **Control web:** permite a los administradores de TI controlar el acceso a sitios web, filtrar contenido web y bloquear sitios web maliciosos.
- **Protección de correo electrónico:** incluye protección de correo electrónico para filtrar correos electrónicos maliciosos y correo no deseado.
- **Protección contra phishing:** utiliza tecnología antiphishing para proteger a los usuarios de ataques de phishing que intentan robar información confidencial.
- **Protección de archivos:** utiliza la tecnología de protección de archivos para proteger los archivos críticos del sistema contra ataques de malware y ransomware.
- **Análisis en tiempo real:** analiza en tiempo real todos los archivos y procesos que se ejecutan en los dispositivos para detectar y bloquear amenazas.

- **Gestión centralizada:** se puede gestionar y configurar de forma centralizada desde una consola de administración, lo que facilita la administración de la seguridad en toda la empresa. La consola Garantiza la visibilidad en tiempo real de todos los endpoints así como la gestión completa de la seguridad y la creación de informes para todos los sistemas operativos
  Compatibilidad: debe ser compatible con la mayoría de los sistemas operativos
- **Soporte para XDR:** Para mejorar aún más el conocimiento de la situación y proporcionar visibilidad a través de su red
- **Motor de detección:** El motor de detección brinda protección contra ataques maliciosos al sistema mediante el control de la comunicación de archivos, correo electrónico e Internet.
- **exploración avanzada mediante AMSI:** permite a los desarrolladores de las aplicaciones habilitar nuevas defensas de malware
- **Protección del sistema de archivos en tiempo real:** La protección del sistema de archivos en tiempo real controla todos los archivos del sistema para detectar código malicioso al abrirlos, crearlos o ejecutarlos
- **Exploración del equipo:** Se usa para realizar la exploración de los archivos y las carpetas del equipo
- **Control del dispositivo:** proporciona el control del dispositivo automático (CD/DVD/USB/...).
- **Sistema de prevención de intrusiones basado en el host (HIPS):** protege su sistema contra malware y actividades no deseadas que intentan perjudicar el equipo
- **Modo de presentación:** característica para los usuarios que requieren utilizar el software en forma ininterrumpida
- **Exploración en el inicio:** Se realizará de forma automática durante el inicio del sistema
- **Protección de documentos:** explora los documentos de Microsoft Office antes de que se abran, así como los archivos descargados automáticamente por Internet Explorer
- **Creación de Varios tipos de Exclusiones:** Las Exclusiones permiten excluir objetos del motor de detección, debe permitir exclusiones de rendimiento, Exclusiones de la detección, exclusiones de procesos, Exclusiones Hips, Etc.
- **Firewall Bidireccional:** El firewall controla todo el tráfico de red que sale del sistema y que ingresa a él.
- **Protección contra ataques de red:** Analiza el contenido del tráfico de la red y protege de ataques en la red.
- **Protección contra Botnet:** detecta y bloquea la comunicación con los servidores maliciosos de comando y control según patrones típicos usando el equipo está infectado y un bot está tratando de comunicarse.
- **Creación de Zona de confianza:** Permite crear perfiles de confianza para la creación de reglas de comunicación local.
- **Filtrado de protocolos:** Habilitar el filtrado del contenido de los protocolos de aplicación.
- **Protección del cliente de correo electrónico:** La integración con los clientes de correo electrónico incrementa el nivel de protección activa frente a los códigos maliciosos en los mensajes de correo electrónico.
- **Protección del acceso a la Web:** Monitorear la comunicación entre los navegadores Web y los servidores remotos, según las disposiciones normativas de HTTP.
- **Protección anti-phishing:** bloquea las páginas web conocidas por distribuir este tipo de contenido.

- **Control Web:** permite bloquear páginas Web que puedan contener material potencialmente ofensivo.
- **Actualización del programa:** El módulo de actualización garantiza que el programa esté
- siempre al día de dos maneras: actualizando el motor de detección y los componentes del sistema.
- **Archivos de registro:** Los archivos de registro contienen información sobre todos los sucesos importantes del programa.
- **Tareas programadas:** Desde la sección de tareas programadas, se gestionan y
- ejecutan tareas programadas según la configuración y las propiedades predefinidas.
- **Estadísticas de protección:** ver un gráfico de datos estadísticos relacionados con los módulos de protección.
- **Observar la actividad: I**ínea de tiempo que registra la actividad del sistema de
- archivos en tiempo real.
- **SysInspector:** Inspecciona minuciosamente su equipo, recopila información detallada sobre los componentes del sistema como las aplicaciones y los controladores, las conexiones de red o las entradas de registro importantes, y evalúa el nivel de riesgo de cada componente.
- **Protección basada en la nube:** Protección de comunicación en la nube Informe de seguridad Esta función proporciona una descripción general de las estadísticas.
- **Envío de muestras para su análisis:** Si encuentra un archivo de conducta sospechosa en su equipo o un sitio sospechoso en Internet.
- **Cuarentena:** La principal función de la cuarentena es almacenar de forma segura los objetos informados (como malware, archivos infectados o aplicaciones potencialmente no deseadas).
- **Navegador Seguro:** Activa protección de memoria, protección del teclado, protección basada en listas de URL para la ejecución automática del Navegador

Tecnologías que debe soportar

- Antivirus
- Antispyware
- Detección de redes de confianza
- Firewall personal
- Anti-Spam
- Self Defence
- HIPS
- Web Control
- Navegador seguro
- Control de dispositivos
- MDM IOS, Android
- Análisis UEFI
- Detecciones ADN
- Machine Leaning
- Reputación y Cache
- Bloqueo de Exploits
- Análisis avanzado de memoria
- Escudo contra ransomware
- Protección contra ataques de red
- Protección contra botnets

- Sandbox
- Full disk encryption

Funcionalidades:

- La consola de gestión es muy fácil de usar y con una interfaz de usuario muy intuitiva y con muchas características útiles lo que facilita enormemente el trabajo y la localización de amenazas en los ordenadores de los usuarios.
- podemos obtener informes detallados sobre todas y cada una de las PC que se ejecutan en nuestra organización en un solo panel, lo cual ayuda a tener una mejor administración de los endpoints y facilidad de actualización de estos a través de la administración,
- las políticas se pueden definir por perfil. En lo personal la gestión de la nube funciona bien y podemos realizar todas las tareas de operaciones con la política correcta y suficiente información si ocurre un incidente.
- La implementación es sumamente sencilla. el agente se puede desplegar por la red o
- por medio del directorio activo.
- La administración es fácil y automatizada, La consola permite a nosotros los administradores, ejecutar tareas, hacer cumplir las políticas de seguridad, monitorear el estado del sistema y responder rápidamente a problemas o detecciones en terminales administrados en todas las plataformas, incluidos equipos de escritorio, servidores, máquinas virtuales e incluso dispositivos móviles.
- Su cliente ligero es realmente ligero, no afecta al rendimiento de los equipos de forma drástica o notable. No consume tantos recursos, sin interferencias con otras aplicaciones cuando funciona en segundo plano
- esta solución tiene la opción de generar informes personalizados, por ejemplo, cuales
- fueron los usuarios más atacados durante el mes, cual fue tipo de evento, la remediación
- Podemos obtener también la información de las características del hardware de los dispositivos finales
- Capacidad para generar alertas o notificaciones a un administrador en caso de que se detecte una infección.
- El Agente es bastante completo para prevenir amenazas, Las capacidades automatizadas de detección y respuesta de la solución son bastante buenas esto también depende mucho de lo agresivos que queramos ser con las políticas.
- El agente es a prueba de manipulaciones ya que este solo se puede desinstalar o
- cerrar mediante el uso de una contraseña.
- La Solución de monitoreo e informes en tiempo real que nos ayuda a investigar cualquier incidente de seguridad, código malicioso o anomalías
- no hay impacto mayor en el rendimiento de la red.
- La función de extracción de amenazas que escanea archivos en tiempo real, el sandboxing es capaz de prevenir amenazas que el antimalware no detecta.
- Genera automáticamente informes forenses que proporcionan detalles y conocimientos procesables sobre un incidente.

- **2 licencias VMware vSphere Standard:**

La corporación Ruta N requiere de un sistema operativo VMware vSphere para alojar máquinas virtuales en sus servidores. Esta licencia de virtualización de servidores ofrece una amplia gama de características y funcionalidades avanzadas para mejorar la eficiencia, la disponibilidad y la seguridad de los sistemas de TI de la Corporación, esta licencia cuenta con las siguientes características.

- **Virtualización de servidores:** vSphere Standard permite virtualizar los servidores de una empresa, lo que significa que varios sistemas operativos y aplicaciones pueden funcionar en un solo servidor físico, lo que ayuda a reducir el costo total de propiedad y aumentar la utilización de recursos.
- **Balanceo de carga:** esta característica permite distribuir el trabajo de manera uniforme entre los servidores virtuales, lo que ayuda a mejorar el rendimiento y la disponibilidad de las aplicaciones.
- **Migración en vivo:** vSphere Standard permite a las empresas migrar servidores virtuales de un servidor físico a otro sin interrupciones en el servicio, lo que ayuda a minimizar el tiempo de inactividad y mejorar la disponibilidad de los sistemas.
- **Alta disponibilidad:** la licencia vSphere Standard incluye la función de alta disponibilidad, que automáticamente reinicia las máquinas virtuales en caso de fallo del hardware, ayudando a minimizar el tiempo de inactividad y reducir el impacto en el negocio.
- **Seguridad:** vSphere Standard incluye características de seguridad avanzadas como la autenticación de dos factores y la encriptación de datos, lo que ayuda a proteger los sistemas y los datos de la empresa contra posibles amenazas.
- Consolide el hardware para mejorar la utilización de la capacidad.
- Optimice la administración de TI mediante una gestión centralizada.
- Reduzca la inversión en capital y los gastos operativos.
- Reduzca al mínimo los recursos de hardware necesarios para ejecutar el hipervisor, lo que se traduce en una mayor eficiencia.
- Formato compacto para minimizar las amenazas a la seguridad del hipervisor

2 licencias Windows Server Standard última versión

La Corporación Ruta N requiere de dos licencias de Windows Server Estándar última versión, para el Directorio Activo Principal y Secundario, con estas licencias, la Corporación puede ejecutar las aplicaciones de servidor necesarias y asegurar la estabilidad y el rendimiento de la infraestructura de TI.

Características que por lo general están disponibles	Windows Server Standard ultima version
Red extendida de Azure	No
Analizador de procedimientos recomendados	Sí
Contenedores	Sí
Direct Access	Sí
Memoria dinámica (en virtualización)	Sí
RAM de agregado o reemplazo en caliente	Sí
Aplicación de revisiones en caliente	No

Microsoft Management Console	Sí
Interfaz de servidor básica	Sí
Network Load Balancing	Sí
Windows PowerShell	Sí
Opción de instalación Server Core	Sí
Administrador de servidores	Sí
SMB directo y SMB sobre RDMA	Sí
Compresión de SMB	Sí
SMB a través de QUIC	No
Redes definidas por software	No
Servicio de migración de almacenamiento	Sí
Réplica de almacenamiento	Sí, (1 asociación y 1 grupo de recursos con un volumen único de 2 TB)
Compresión de réplica de almacenamiento	No
Espacios de almacenamiento	Sí
Espacios de almacenamiento directos	No
Volumen Activación Services	Sí
Integración de VSS (Servicio de instantáneas de volumen)	Sí
Windows Server Update Services	Sí
Registro de licencias del servidor	Sí
Activación heredada	Como invitado si se hospeda en el centro de datos
Carpetas de trabajo	Sí
Número Máximo de usuarios	Depende de las cal

Nota: Se necesitan 100 licencias CAL por dispositivo Windows Server para otorgar a los usuarios y dispositivos los derechos de acceso al sistema operativo de Windows Server que se está ejecutando en el servidor.

Nota 1: Todo el licenciamiento debe tener las últimas versiones durante toda la vigencia del contrato

ANALISIS DE NIVEL DE SERVICIO TECNOLOGICOS:

Apoyar a la mesa de servicio interna con el soporte técnico a toda la infraestructura en modalidad de renting, atendiendo, gestionando o dando solución a los incidentes que le sean informados, garantizando la normal operación de los servicios y productos según los tiempos descritos a continuación.

- **Requerimiento:** Un requerimiento es una descripción formal de algo que un sistema, producto o proceso debe proporcionar o cumplir. Puede ser una necesidad funcional, de rendimiento, de seguridad, de calidad o de cualquier otro tipo que deba ser satisfecha para que un proyecto tenga éxito.

- **Incidente:** Un incidente en TI es un evento no planificado que interrumpe o reduce la calidad de un servicio TI. Puede ser causado por una falla en el hardware, software, red o cualquier otro componente del sistema. Un incidente puede afectar la disponibilidad, integridad o confidencialidad de los datos o la capacidad de un usuario para acceder a los servicios TI.

  PRIORIDAD CRITICA: incidentes que tienen un impacto severo en la operación crítica y requieren una respuesta inmediata para minimizar el impacto.

  Los eventos o servicios que aplican en esta categoría son:

  - Indisponibilidad general de internet en toda la corporación.
  - Fallas en servidores que impidan el acceso a internet o a sus aplicativos o los archivos almacenados en ellos.
  - Fallas simultaneas en todos los equipos de cómputo, equipos de telecomunicaciones
  - Ataques a la seguridad informática e indisponibilidad.
  - Fallas en las redes inalámbricas.
  - Una falla masiva es una interrupción significativa en un sistema o servicio, que afecta a un gran número o a todos los usuarios o componentes.

  PRIORIDAD ALTA: incidentes que tienen un impacto moderado en la operación y requieren una respuesta oportuna para resolver el problema.

  Los eventos o servicios que aplican en esta categoría son:

  - Indisponibilidad de la Suit de Office 365.
  - Indisponibilidad del ERP – SAFIX
  - Fallas en los sistemas de información
  - Fallas en los sistemas de monitoreo y consolas de administración.
  - Fallas sistema de telefonía IP general

  PRIORIDAD MEDIA: incidentes que tienen un impacto limitado en la operación y requieren una respuesta apropiada para resolver el problema.

  Los eventos que aplican en esta categoría son:

  - Indisponibilidad o falla en sistemas de información como intranet.
  - Servicios de apoyo de sistemas de inventario, sistemas de seguimiento de tareas y proyectos.
  - Fallas en Servicio de impresoras.
  - Fallas en algunos equipos de cómputo.
  -

- **PRIORIDAD BAJA:** incidentes que tienen un impacto mínimo en la operación y requieren una respuesta apropiada, pero no necesariamente de forma inmediata.

Los eventos que aplican en esta categoría son:

- Servicios secundarios o menos utilizados, como sistemas de encuestas o aplicaciones de mensajería.
- Servicios de aprendizaje o entrenamiento, como plataformas de formación en línea.
- Actualizaciones de sistemas operativos.
- Fallas en teléfonos IP

NIVEL	TIEMPO DE ATENCION	TIEMPO DE SOLUCIÓN (HORAS HÁBILES)
Crítico	0-2 horas	0 – 8 horas
Alto	2-4 horas	8 horas y 1 minuto – 16 horas
Medio	4-8 horas	16 horas y 1 minuto y 24 horas
Bajo	8 – 16 horas	48 horas

- **Tarea Programada:** Puede ser una tarea de mantenimiento, una copia de seguridad, una actualización de software, una ejecución de un script, realizar un inventario, entre otros.

Servicio	Descripción	Aplica
Mantenimiento preventivo	Se entiende por mantenimiento preventivo a la labor periódica y programada de limpieza del hardware contratado.	SI
Soporte	Se entiende por soporte la atención de incidentes relacionados con la ausencia parcial o total del servicio que presta la infraestructura de Seguridad perimetral.	SI

Monitoreo	El servicio de monitoreo consiste en apoyar el seguimiento del comportamiento de los diferentes elementos de la infraestructura de Seguridad perimetral, a través de herramientas especializadas, para conocer su desempeño y poder tomar acciones proactivas ante cualquier evento que pueda afectar o afecte el normal funcionamiento de estos; Adicionalmente, permite tener históricos para analizar el desempeño y la disponibilidad de los servicios en el tiempo.	SI
Administración	Se entiende por administración la atención de actividades y tareas relacionadas con la gestión de aspectos como la configuración, el rendimiento y la disponibilidad, de los servicios que presta la infraestructura de conectividad, de servidores, de aplicaciones y de protocolos establecidos para el normal cumplimiento de las exigencias propias del cliente	SI
Calidad	Se entiende como aquellas actividades de gestión que son asociadas a los servicios anteriormente mencionados y que tienen como propósito la mejora continua y aseguramiento de la calidad de los servicios.	SI

Actividades

Servicio	Actividad
Monitoreo	Monitoreo estado del dispositivo mediante ping.
	Monitoreo utilización de CPU.
	Monitoreo utilización de memoria.
	Monitoreo del estado de puertos TCP específicos.
	Monitoreo del tiempo que el dispositivo ha estado encendido.
	Definición de umbrales para las anteriores variables.
	Generación de alarmas según los umbrales definidos.
	Monitoreo utilización ancho de banda.
	Monitoreo del tiempo que el dispositivo ha estado encendido.
	Definición de umbrales para las anteriores variables.

Soporte	Escalamiento de incidentes ante fabricantes
	Tramite de garantías ante fabricante
	Manejo de los casos de soporte mediante herramienta de Gestión de solicitudes.
	Diagnóstico y solución de fallas hardware y partes
	Soporte de conexiones físicas.
	Diagnóstico y solución de fallas relacionadas con el sistema operativo.
	Diagnostico a problemas de rendimiento.
	Soporte de configuración y protocolos de red.
Administración	Gestión de reglas Gestión de Listas de acceso Gestión de NATs Gestión de grupos
Calidad	Presentar informe de gestión mensual.
	Mantener actualizada y realizar la gestión del riesgo.
	Mantener un plan de calidad para el servicio
Mantenimiento	Limpieza física del hardware contratado empleando las herramientas adecuadas.

NOTA: Cuando la solución de un incidente demore más de 24 horas hábiles, el futuro contratista deberá reemplazar el equipo que presenta fallas por uno de similares características mientras es solucionado el incidente.

Los tiempos de soporte y mantenimiento empiezan a contar una vez LA CORPORACION RUTA N MEDELLIN notifica el incidente o problema, mediante la mesa de servicios o telefónicamente.

Definición incidente crítico: Son aquellos incidentes de software y/o hardware, que no permiten la utilización del equipo.

Definición incidente bajo: Son aquellos incidentes de software y/o hardware, que afectan la utilización del equipo en condiciones normales.

Los casos que sean reportados por teléfono deberán quedar inscritos en la mesa de servicios dispuesta para el este caso, indicando la fecha y hora de recepción de la comunicación telefónica.