ESPECIFICACIONES TÉCNICAS

RED CORPORATIVA EDIFICIO 323

Santo Domingo, Distrito Nacional
República Dominicana

Junio 2025

Importancia de la adquisición de equipos de red – Edificio 323, INDOTEL

La adquisición de los equipos y soluciones listadas es fundamental para garantizar la conectividad, seguridad y escalabilidad de la red tecnológica del nuevo edificio 323 del INDOTEL. Esta infraestructura es clave para el correcto funcionamiento de los servicios institucionales, incluyendo la gestión de datos, comunicaciones internas, acceso a internet, seguridad perimetral, administración centralizada y cumplimiento de estándares modernos de redes corporativas.

Ítem	Equipos Requeridos	Cantidad
1	Access Point Wi-Fi 7 (densidad media)	37
2	Access Point Wi-Fi 7 (densidad alta)	23
3	Switches Multigigabit de 24 puertos	32
4	Switches de acceso de 24 puertos	6
5	Switches de acceso de 48 puertos	20
6	Switches CORE	2
7	Firewalls	2
8	Solución de Almacenamiento de Logs	1
9	Solución de Secure Access Servie Edge	1
10	Solución de Administración Centralizada	1
11	Solución de Network Access Control	1
12	Instalación y configuración de todos los componentes	1
13	Soporte y mantenimiento para Hardware y Software por 3 años	1

Los equipos propuestos deben permitir:

- Implementar una red de alta disponibilidad, rendimiento y cobertura inalámbrica Wi-Fi 7.
- Garantizar una estructura de switches de acceso, distribución y CORE capaz de soportar operaciones fluidas y seguras.
- Fortalecer la seguridad perimetral mediante firewalls avanzados y soluciones de acceso seguro (NAC y SA).
- Asegurar la visibilidad, gestión y almacenamiento centralizado de logs, permitiendo trazabilidad y cumplimiento normativo.
- Consolidar una administración eficiente desde una plataforma de gestión centralizada.

Contar con esta infraestructura desde la fase inicial del edificio es crucial para minimizar riesgos operativos y asegurar que todas las áreas cuenten con servicios tecnológicos de calidad desde el primer día.

Especificaciones técnicas de los equipos requeridos

Los equipos tecnológicos requeridos deben de cumplir con las siguientes características y especificaciones técnicas, las cuales se establecen como mínimas para el presente proyecto.

Ítem 1. Access Point Wi-Fi 7 (densidad media)

Numeral	Especificaciones técnicas
1.1	Cantidad: 37
1.2	El equipo debe soportar WiFi7
1.3	Debe soportar al menos 8 SSID simultáneos
1.4	Debe contar con al menos 3 radios, y soportar al menos 512 usuarios
1.5	Debe tener un radio dedicado al escaneo de frecuencia
1.6	Debe ser de tipo indoor con antenas internas
1.7	Debe soportar tasas de transferencias en la banda 5ghz superiores a 8Gbps
1.8	Debe tener las siguientes antenas internas: x4 Dual band Wi-Fi + x4 Tri-band Wi-Fi and Scanning + 1 2.4GHz BLE/ ZigBee + 1 GPS antena
1.9	Debe tener al menos 41 Watts de consumo de energía
1.10	Debe soportar los siguientes protocolos de autenticación WPA™, WPA2™, and WPA3™ with 802.1x or Preshared key, WEP, Web Captive Portal, MAC blocklist and allowlist
1.11	Debe soportar MIMO Chain 4x4 en los tres radios.
	Características generales
1.12	Punto de acceso (AP) que permita el acceso de los dispositivos a la red a través de la Wireless y que posea todas sus configuraciones centralizadas en controlador inalámbrico;
1.13	Debe soportar el modo de operación centralizado, o sea, su operación depende del controlador inalámbrico en premisas que es responsable de gestionar las políticas de seguridad, calidad de servicio (QoS) y monitoreo de la radiofrecuencia;
1.14	Debe identificar automáticamente el controlador inalámbrico al que se conectará;
1.15	Debe permitir administrarse remotamente a través de links WAN;
1.16	Debe poseer capacidad dual-band con radios 2.4GHz y 5GHz operando simultáneamente, además de permitir configuraciones independientes para cada radio;

1.17	El tráfico de los dispositivos conectados a la red inalámbrica debe realizarse de forma centralizada a través del túnel establecido entre el punto de acceso y el controlador inalámbrico. En este modo todos los paquetes deben ser encapsulados hasta el controlador inalámbrico; Cuando sea encapsulado, el tráfico debe ser encriptado a través de DTLS o IPSEC;
1.18	Debe permitir el tráfico de los dispositivos conectados a la red inalámbrica de forma distribuida (local switching), o sea, el tráfico debe ser conmutado localmente en la interfaz LAN del punto de acceso y no necesitará ser encapsulado hasta el controlador inalámbrico;
1.19	Cuando el tráfico sea distribuido y la autenticación con PSK, en caso de fallo en la comunicación entre los puntos de acceso y el controlador inalámbrico, los usuarios asociados deben permanecer asociados a los puntos de acceso y al mismo SSID. Debe permitirse la conexión de nuevos usuarios a la red inalámbrica;
1.20	En conjunto con el controlador inalámbrico, debe optimizar el rendimiento y la cobertura inalámbrica (RF), realizando automáticamente el ajuste de potencia y la distribución adecuada de canales a ser utilizados;
1.21	Deberá soportar la funcionalidad de ajuste automático de potencia para extender la cobertura en caso de falla del punto de acceso vecino gerenciado por la misma controladora;
1.22	Debe soportar mecanismos para la detección y mitigación de puntos de acceso no autorizados, también conocidos como Rogue APs;
1.23	En conjunto con el controlador inalámbrico, debe implementar mecanismos de protección para identificar ataques a la infraestructura inalámbrica (wIDS / wIPS);
1.24	En conjunto con el controlador inalámbrico, debe permitir la creación de múltiples dominios de movilidad (SSID) con configuraciones distintas de seguridad y red;
1.25	En conjunto con el controlador inalámbrico, debe implementar los siguientes métodos de autenticación: WPA (TKIP) y WPA2 (AES);
1.26	En conjunto con el controlador inalámbrico, debe implementar el protocolo IEEE 802.1X con la asociación dinámica de VLAN para los usuarios en función de los atributos proporcionados por los servidores RADIUS;
1.27	Debe admitir los siguientes métodos de autenticación EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS y PEAP;
1.28	Debe implementar el estándar IEEE 802.11r para acelerar el proceso de roaming de los dispositivos a través de la función conocida como Fast Roaming;
1.29	Debe implementar el estándar IEEE 802.11k para permitir que un dispositivo conectado a la red inalámbrica identifique rápidamente otros puntos de acceso disponibles en su área para que ejecute el roaming;

1.30	Debe implementar el estándar IEEE 802.11v para permitir que la red influya en las decisiones de roaming del cliente conectadas mediante el suministro de información complementaria, como la carga de utilización de los puntos de acceso cercanos;
1.31	Debe implementar el estándar IEEE 802.11e;
1.32	Debe implementar el estándar IEEE 802.11h;
1.33	El punto de acceso deberá soportar agregación de paquetes A-MPDU y A-MSDU;
1.34	El punto de acceso deberá soportar (LPDC) - Low Density Parity Check;
1.35	El punto de Acceso deberá soportar (MLD) - Maximum Likelihood Demodulation;
1.36	El Punto de Acceso deberá soportar método de diversidad (MRC) Maximum Ratio Combining;
1.37	Debe tener indicadores luminosos (LED) para indicación de estado;
1.38	Debe permitir su alimentación a través de Power Over Ethernet (PoE) conforme los estándares 802.3bt;
1.39	El punto de acceso debe ser compatible y ser administrado por los controladores inalámbricos de este proceso;
1.40	Cualquier licencia y / o software necesario para la plena ejecución de todas las características descritas en este término de referencia deberá ser suministrada;
1.41	Debe poseer un certificado emitido por la Wi-Fi Alliance;
1.42	El controlador de la red inalámbrica debe permitir la creación de políticas de firewalls para los SSID con las siguientes funcionalidades de seguridad:
1.43	- IPS
1.44	- Antivirus
1.45	- Web Filter
1.46	- SSL Inspection
1.47	- Application Control
1.48	El controlador de la red inalámbrica no debe licenciar la cantidad de puntos de acceso que se desplieguen.
1.49	Deberá soportar administración centralizada en premisas (single pane of glass) para manejar el NGFW, Wireless Controller y Switch Controller.

Ítem 2. Access Point Wi-Fi 7 (densidad alta)

Numeral	Especificaciones técnicas
2.1	Cantidad: 23
2.2	El equipo debe soportar WiFi7
2.3	Debe soportar al menos 24 SSID simultáneos
2.4	Debe contar con al menos 3 radios, y soportar al menos 512 usuarios
2.5	Debe tener un radio dedicado al escaneo de frecuencia
2.6	Debe ser de tipo indoor con antenas internas
2.7	Debe soportar tasas de transferencias superiores a 2.56 Gbps en la banda 5ghz
2.8	Debe tener las siguientes antenas internas: 6. x2 Dual band Wi-Fi + x2 6GHz band Wi-Fi + x1 BLE/ ZigBee antena + x1 GPS antena
2.9	Debe tener al menos 15.2 Watts de consumo de energía
2.10	Debe soportar los siguientes protocolos de autenticación WPA™, WPA2™, and WPA3™ with 802.1x or Preshared key, WEP, Web Captive Portal, MAC blocklist and allowlist
2.11	Debe soportar MIMO Chain 2x2 en los tres radios.
	Características generales
2.12	Punto de acceso (AP) que permita el acceso de los dispositivos a la red a través de la Wireless y que posea todas sus configuraciones centralizadas en controlador inalámbrico;
2.13	Debe soportar el modo de operación centralizado, o sea, su operación depende del controlador inalámbrico en premisas que es responsable de gestionar las políticas de seguridad, calidad de servicio (QoS) y monitoreo de la radiofrecuencia;
2.14	Debe identificar automáticamente el controlador inalámbrico al que se conectará;
2.15	Debe permitir administrarse remotamente a través de links WAN;
2.16	Debe poseer capacidad dual-band con radios 2.4GHz y 5GHz operando simultáneamente, además de permitir configuraciones independientes para cada radio;
2.17	El tráfico de los dispositivos conectados a la red inalámbrica debe realizarse de forma centralizada a través del túnel establecido entre el punto de acceso y el controlador inalámbrico. En este modo todos los paquetes deben ser encapsulados hasta el controlador inalámbrico; Cuando sea encapsulado, el tráfico debe ser encriptado a través de DTLS o IPSEC;

2.18	Debe permitir el tráfico de los dispositivos conectados a la red inalámbrica de forma distribuida (local switching), o sea, el tráfico debe ser conmutado localmente en la interfaz LAN del punto de acceso y no necesitará ser encapsulado hasta el controlador inalámbrico;
2.19	Cuando el tráfico sea distribuido y la autenticación con PSK, en caso de fallo en la comunicación entre los puntos de acceso y el controlador inalámbrico, los usuarios asociados deben permanecer asociados a los puntos de acceso y al mismo SSID. Debe permitirse la conexión de nuevos usuarios a la red inalámbrica;
2.20	En conjunto con el controlador inalámbrico, debe optimizar el rendimiento y la cobertura inalámbrica (RF), realizando automáticamente el ajuste de potencia y la distribución adecuada de canales a ser utilizados;
2.21	Deberá soportar la funcionalidad de ajuste automático de potencia para extender la cobertura en caso de falla del punto de acceso vecino gerenciado por la misma controladora;
2.22	Debe soportar mecanismos para la detección y mitigación de puntos de acceso no autorizados, también conocidos como Rogue APs;
2.23	En conjunto con el controlador inalámbrico, debe implementar mecanismos de protección para identificar ataques a la infraestructura inalámbrica (wIDS / wIPS);
2.24	En conjunto con el controlador inalámbrico, debe permitir la creación de múltiples dominios de movilidad (SSID) con configuraciones distintas de seguridad y red;
2.25	En conjunto con el controlador inalámbrico, debe implementar los siguientes métodos de autenticación: WPA (TKIP) y WPA2 (AES);
2.26	En conjunto con el controlador inalámbrico, debe implementar el protocolo IEEE 802.1X con la asociación dinámica de VLAN para los usuarios en función de los atributos proporcionados por los servidores RADIUS;
2.27	Debe admitir los siguientes métodos de autenticación EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS y PEAP;
2.28	Debe implementar el estándar IEEE 802.11r para acelerar el proceso de roaming de los dispositivos a través de la función conocida como Fast Roaming;
2.29	Debe implementar el estándar IEEE 802.11k para permitir que un dispositivo conectado a la red inalámbrica identifique rápidamente otros puntos de acceso disponibles en su área para que ejecute el roaming;
2.30	Debe implementar el estándar IEEE 802.11v para permitir que la red influya en las decisiones de roaming del cliente conectadas mediante el suministro de información complementaria, como la carga de utilización de los puntos de acceso cercanos;
2.31	Debe implementar el estándar IEEE 802.11e;

2.32	Debe implementar el estándar IEEE 802.11h;
2.33	El punto de acceso deberá soportar agregación de paquetes A-MPDU y A-MSDU;
2.34	El punto de acceso deberá soportar (LPDC) - Low Density Parity Check;
2.35	El punto de Acceso deberá soportar (MLD) - Maximum Likelihood Demodulation;
2.36	El Punto de Acceso deberá soportar método de diversidad (MRC) Maximum Ratio Combining;
2.37	Debe tener indicadores luminosos (LED) para indicación de estado;
2.38	Debe permitir su alimentación a través de Power Over Ethernet (PoE) conforme los estándares 802.3bt;
2.39	El punto de acceso debe ser compatible y ser administrado por los controladores inalámbricos de este proceso;
2.40	Cualquier licencia y / o software necesario para la plena ejecución de todas las características descritas en este término de referencia deberá ser suministrada;
2.41	Debe poseer un certificado emitido por la Wi-Fi Alliance;
2.42	El controlador de la red inalámbrica debe permitir la creación de políticas de firewalls para los SSID con las siguientes funcionalidades de seguridad:
2.43	- IPS
2.44	- Antivirus
2.45	- Web Filter
2.46	- SSL Inspection
2.47	- Application Control
2.48	El controlador de la red inalámbrica no debe licenciar la cantidad de puntos de acceso que se desplieguen.
2.49	Deberá soportar administración centralizada en premisas (single pane of glass) para manejar el NGFW, Wireless Controller y Switch Controller.

Ítem 3. Switches Multigigabit de 24 puertos

Numeral	Especificaciones técnicas
3.1	Cantidad: 32
3.2	Tener al menos 24 interfaces 2.5G/1G/100M/10M de cobre
3.3	Tener al menos 6 interfaces 10 Gbps de fibra.
3.4	Soportar al menos 780W de poder para PoE
3.5	Tener al menos 8 puertos PoE++ (802.3 af/at/bt)
3.6	Tener al menos 16 puertos PoE+ (802.3 af/at)
3.7	Throughput de switching de por lo menos 240 Gbps
3.8	Soportar al menos 355 Mbps de paquetes por segundos
3.9	Tener al menos 32k de almacenamiento de MAC Address
3.10	Soportar al menos 4K de VLANS
3.11	Tener al menos 1GB DDR4 de DRAM
3.12	Tener al menos 256 MB de memoria Flash
3.13	Soportar al menos 640 lista de accesos
3.14	Soportar al menos 32 estancias de Spanning Tree
	Funcionalidades de Administración
3.15	El switch deberá poder aceptar actualizaciones de firmware
3.16	Los switches con PoE+ deberán tener la capacidad de habilitar o deshabilitar la función de PoE+
3.17	Deberá soportar detección y notificación de conflictos de direcciones IP
3.18	Deberá soportar administración por IPv4 e IPv6
3.19	Deberá soportar Telnet / SSH para acceso a la consola
3.20	Deberá soportar HTTP / HTTPS
3.21	Deberá soportar SNMP v1/v2c/v3
3.22	Deberá poder configurar su reloj mediante un NTP Server
3.23	Deberá contar con una línea de comandos estándar y con interface para configurar vía Web
3.24	Deberá soportar actualizaciones de Software por: TFTP/FTP/GUI
3.25	Deberá soportar HTTP REST APIs para Configuración y monitoreo
3.26	Deberá soportar configuración de VLAN de forma centralizada. Donde se configure la VLAN una sola vez, y se pueda asignar a distintos switches y puertos.
3.27	La solución debe soportar administración centralizada en la premisa y en la nube, sin necesidad de cambiar modelos de equipos.

3.28	Debe soportar auto-discovery para administración centralizada. Es decir, que, al conectar el switch a la red, el controlador debe ser capaz de descubrirlo y administrarlo sin necesidad de configuración alguna en el switch.
3.29	La solución debe ser capaz de hacer agregación de enlaces de forma automática. Es decir, que pueda identificar dos enlaces conectados entre los mismos switches, y en lugar de bloquear un enlace con Spanning Tree, autoconfigure redundancia de enlaces para aprovecharlos al mismo tiempo sin intervención del administrador.
3.30	La solución debe ser capaz de encriptar el tráfico entre enlaces de administración y control.
3.31	Debe soportar Zero-Touch Deployment sobre enlaces capa 2 y capa 3.
3.32	Debe ser capaz de implementar Políticas de Control de Acceso a la red (NAC) que puedan filtrar basado en usuarios, grupos de usuarios del Directorio Activo, Tipo de Dispositivos, Sistema Operativo del dispositivo, Vulnerabilidades de dispositivos de IoT.
	Funcionalidades de Calidad de Servicio
3.33	Deberá soportar priorización de tráfico basada en 802.1p
3.34	Deberá soportar priorización de tráfico basada en IP TOS/DSCP
	Funcionalidades de Capa 2
3.35	Deberá soportar LACP
3.36	Deberá soportar Spanning Tree
3.37	Deberá soportar Jumbo Frames
3.38	Deberá soportar Auto-negociacion para la velocidad de los puertos y para Duplex
3.39	Deberá soportar el estándar IEEE 802.1D MAC Bridging/STP
3.40	Deberá soportar el estándar IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
3.41	Deberá soportar el estándar IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
3.42	Deberá soportar la funcionalidad STP Root Guard
3.43	Deberá soportar STP BPDU Guard
3.44	Deberá soportar Edge Port / Port Fast
3.45	Deberá soportar el estándar IEEE 802.1Q VLAN Tagging
3.46	Deberá poder balancear tráfico Unicast/Multicast sobre un puerto trunk (dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac)
3.47	Deberá soportar el estándar IEEE 802.1AX Link Aggregation
3.48	Deberá soportar instancias de Spanning Tree (MSTP/CST)
3.49	Deberá soportar el estándar IEEE 802.3x Flow Control con Back-pressure
3.50	Deberá soportar el estándar IEEE 802.3 10Base-T
3.51	Deberá soportar el estándar IEEE 802.3u 100Base-TX
3.52	Deberá soportar el estándar IEEE 802.3z 1000Base-SX/LX

3.53	Deberá soportar el estándar IEEE 802.3ab 1000Base-T
3.54	Deberá soportar el estándar IEEE 802.3 CSMA/CD como metodo de acceso y las especificaciones de la capa fisica
3.55	Deberá contar con la funcionalidad de Control de Tormentas (Storm Control)
3.56	Deberá soportar la creación de VLANs por MAC, IP y Ethertype-based
3.57	Deberá soportar Time-Domain Reflectometer (TDR)
3.58	Deberá soportar 4064 VLANs simultáneas
3.59	Deberá soportar IGMP Snooping
3.60	Deberá soportar IGMP proxy y querier
3.61	Deberá soportar emgency location identifier numbers (ELINs) en LLDP-MED
3.62	Deberá permitir limitar la cantidad de MACs aprendidas por puerto
3.63	Deberá permitir un mínimo de 15 instancias de MSTP
3.64	Deberá permitir controlar tormentas de broadcast independientemente en cada puerto
3.65	Deberá soportar un mecanismo de detección y prevención de loops
3.66	Deberá soportar SPAN
3.67	Admite conmutación de velocidad de cable y modo de envío Store and Forward
	Funcionalidades de Capa 3
3.68	Deberá soportar Layer 3 routing.
3.69	Deberá soportar DHCP Relay.
	Funcionalidades estandar soportadas (RFCs)
3.70	Deberá soportar Port Mirroring
3.71	Deberá soportar Admin Authentication Via RFC 2865 RADIUS
3.72	Deberá soportar el estándar IEEE 802.1x authentication Port-based
3.73	Deberá soportar el estándar IEEE 802.1x Authentication MAC-based
3.74	Deberá soportar el estándar IEEE 802.1x Guest and Fallback VLAN
3.75	Deberá soportar el estándar IEEE 802.1x MAC Access Bypass (MAB)
3.76	Deberá soportar el estándar IEEE 802.1x Dynamic VLAN Assignment
3.77	Deberá soportar Radius CoA (Change of Authority)
3.78	Deberá soportar el estándar IEEE 802.1ab Link Layer Discovery Protocol (LLDP)
3.79	Deberá soportar el estándar IEEE 802.1ab LLDP-MED
3.80	Deberá soportar Radius Accounting
3.81	Deberá soportar EAP pass-through
3.82	Deberá soportar detección de dispositivos
3.83	Deberá soportar ACLs
3.84	Deberá soportar scheduling de ACLs

3.85	Deberá soportar DHCP Snooping
3.86	Deberá soportar listas de servidores DHCP permitidos
3.87	Deberá soportar bloqueo de DHCP
3.88	Deberá permitir Dynamic ARP Inspection (DAI)
3.89	Deberá permitir Access VLANs
	Funcionalidades de Seguridad y Visibilidad
3.90	Deberá soportar Syslog
3.91	Debe soportar Energy-Efficient Ethernet (EEE)

Ítem 4. Switches de acceso de 24 puertos

Numeral	Especificaciones técnicas
4.1	Cantidad: 6
4.2	Tener al menos 24 interfaces 1GE de cobre
4.3	Tener al menos 4 interfaces 10 Gbps de fibra.
4.4	Soportar al menos 420W de poder para PoE
4.5	Tener al menos 24 puertos PoE+ (802.3 af/at)
4.6	Throughput de switching de por lo menos 128 Gbps
4.7	Soportar al menos 160 Mbps de paquetes por segundos
4.8	Tener al menos 32k de almacenamiento de MAC Address
4.9	Soportar al menos 4K de VLANS
4.10	Tener al menos 1GB DDR4 de DRAM
4.11	Tener al menos 256 MB de memoria Flash
4.12	Soportar al menos 1k lista de accesos
4.13	Soportar al menos 1k entradas de rutas
4.14	Soportar al menos 32 estancias de Spanning Tree
4.15	Soportar al menos 5k de entradas de host.
	Funcionalidades de Administración
4.16	El switch deberá poder aceptar actualizaciones de firmware
4.17	Los switches con PoE+ deberán tener la capacidad de habilitar o deshabilitar la función de PoE+
4.18	Deberá soportar detección y notificación de conflictos de direcciones IP
4.19	Deberá soportar administración por IPv4 e IPv6
4.20	Deberá soportar Telnet / SSH para acceso a la consola
4.21	Deberá soportar HTTP / HTTPS
4.22	Deberá soportar SNMP v1/v2c/v3
4.23	Deberá poder configurar su reloj mediante un NTP Server
4.24	Deberá contar con una línea de comandos estándar y con interface para configurar vía Web
4.25	Deberá soportar actualizaciones de Software por: TFTP/FTP/GUI
4.26	Deberá soportar HTTP REST APIs para Configuración y monitoreo
4.27	Deberá soportar configuración de VLAN de forma centralizada. Donde se configure la VLAN una sola vez, y se pueda asignar a distintos switches y puertos.
4.28	La solución debe soportar administración centralizada en la premisa y en la nube, sin necesidad de cambiar modelos de equipos.

4.29	Debe soportar auto-discovery para administración centralizada. Es decir, que, al conectar el switch a la red, el controlador debe ser capaz de descubrirlo y administrarlo sin necesidad de configuración alguna en el switch.
4.30	La solución debe ser capaz de hacer agregación de enlaces de forma automática. Es decir, que pueda identificar dos enlaces conectados entre los mismos switches, y en lugar de bloquear un enlace con Spanning Tree, autoconfigure redundancia de enlaces para aprovecharlos al mismo tiempo sin intervención del administrador.
4.31	La solución debe ser capaz de encriptar el tráfico entre enlaces de administración y control.
4.32	Debe soportar Zero-Touch Deployment sobre enlaces capa 2 y capa 3.
4.33	Debe ser capaz de implementar Políticas de Control de Acceso a la red (NAC) que puedan filtrar basado en usuarios, grupos de usuarios del Directorio Activo, Tipo de Dispositivos, Sistema Operativo del dispositivo, Vulnerabilidades de dispositivos de IoT.
	Funcionalidades de Calidad de Servicio
4.34	Deberá soportar priorización de tráfico basada en 802.1p
4.35	Deberá soportar priorización de tráfico basada en IP TOS/DSCP
	Funcionalidades de Capa 2
4.36	Deberá soportar LACP
4.37	Deberá soportar Spanning Tree
4.38	Deberá soportar Jumbo Frames
4.39	Deberá soportar Auto-negociacion para la velocidad de los puertos y para Duplex
4.40	Deberá soportar el estándar IEEE 802.1D MAC Bridging/STP
4.41	Deberá soportar el estándar IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
4.42	Deberá soportar el estándar IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
4.43	Deberá soportar la funcionalidad STP Root Guard
4.44	Deberá soportar STP BPDU Guard
4.45	Deberá soportar Edge Port / Port Fast
4.46	Deberá soportar el estándar IEEE 802.1Q VLAN Tagging
4.47	Deberá poder balancear tráfico Unicast/Multicast sobre un puerto trunk (dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac)
4.48	Deberá soportar el estándar IEEE 802.1AX Link Aggregation
4.49	Deberá soportar instancias de Spanning Tree (MSTP/CST)
4.50	Deberá soportar el estándar IEEE 802.3x Flow Control con Back-pressure
4.51	Deberá soportar el estándar IEEE 802.3 10Base-T
4.52	Deberá soportar el estándar IEEE 802.3u 100Base-TX
4.53	Deberá soportar el estándar IEEE 802.3z 1000Base-SX/LX

4.54	Deberá soportar el estándar IEEE 802.3ab 1000Base-T
4.55	Deberá soportar el estándar IEEE 802.3 CSMA/CD como metodo de acceso y las especificaciones de la capa fisica
4.56	Deberá contar con la funcionalidad de Control de Tormentas (Storm Control)
4.57	Deberá soportar la creación de VLANs por MAC, IP y Ethertype-based
4.58	Deberá soportar Time-Domain Reflectometer (TDR)
4.59	Deberá soportar 4064 VLANs simultáneas
4.60	Deberá soportar IGMP Snooping
4.61	Deberá soportar IGMP proxy y querier
4.62	Deberá soportar emgency location identifier numbers (ELINs) en LLDP-MED
4.63	Deberá permitir limitar la cantidad de MACs aprendidas por puerto
4.64	Deberá permitir un mínimo de 15 instancias de MSTP
4.65	Deberá permitir controlar tormentas de broadcast independientemente en cada puerto
4.66	Deberá soportar un mecanismo de detección y prevención de loops
4.67	Deberá soportar SPAN
4.68	Admite conmutación de velocidad de cable y modo de envío Store and Forward
	Funcionalidades de Capa 3
4.69	Deberá soportar Layer 3 routing.
4.70	Deberá soportar DHCP Relay.
	Funcionalidades estandar soportadas (RFCs)
4.71	Deberá soportar Port Mirroring
4.72	Deberá soportar Admin Authentication Via RFC 2865 RADIUS
4.73	Deberá soportar el estándar IEEE 802.1x authentication Port-based
4.74	Deberá soportar el estándar IEEE 802.1x Authentication MAC-based
4.75	Deberá soportar el estándar IEEE 802.1x Guest and Fallback VLAN
4.76	Deberá soportar el estándar IEEE 802.1x MAC Access Bypass (MAB)
4.77	Deberá soportar el estándar IEEE 802.1x Dynamic VLAN Assignment
4.78	Deberá soportar Radius CoA (Change of Authority)
4.79	Deberá soportar el estándar IEEE 802.1ab Link Layer Discovery Protocol (LLDP)
4.80	Deberá soportar el estándar IEEE 802.1ab LLDP-MED
4.81	Deberá soportar Radius Accounting
4.82	Deberá soportar EAP pass-through
4.83	Deberá soportar detección de dispositivos
4.84	Deberá soportar ACLs
4.85	Deberá soportar scheduling de ACLs

4.86	Deberá soportar DHCP Snooping
4.87	Deberá soportar listas de servidores DHCP permitidos
4.88	Deberá soportar bloqueo de DHCP
4.89	Deberá permitir Dynamic ARP Inspection (DAI)
4.90	Deberá permitir Access VLANs
	Funcionalidades de Seguridad y Visibilidad
4.91	Deberá soportar Syslog
4.92	Debe soportar Energy-Efficient Ethernet (EEE)

Ítem 5. Switches de acceso de 48 puertos

Numeral	Especificaciones técnicas
5.1	Cantidad: 20
5.2	Tener al menos 48 interfaces 1GE de cobre
5.3	Tener al menos 4 interfaces 10 Gbps de fibra.
5.4	Soportar al menos 770W de poder para PoE
5.5	Tener al menos 48 puertos PoE (802.3 af/at)
5.6	Throughput de switching de por lo menos 176 Gbps
5.7	Soportar al menos 260 Mbps de paquetes por segundos
5.8	Tener al menos 32k de almacenamiento de MAC Address
5.9	Soportar al menos 4K de VLANS
5.10	Tener al menos 1GB DDR4 de DRAM
5.11	Tener al menos 256 MB de memoria Flash
5.12	Soportar al menos 1.5k lista de accesos
5.13	Soportar al menos 8k entradas de rutas
5.14	Soportar al menos 32 estancias de Spanning Tree
5.15	Soportar al menos 16k de entradas de host.
	Funcionalidades de Administración
5.16	El switch deberá poder aceptar actualizaciones de firmware
5.17	Los switches con PoE+ deberán tener la capacidad de habilitar o deshabilitar la función de PoE+
5.18	Deberá soportar detección y notificación de conflictos de direcciones IP
5.19	Deberá soportar administración por IPv4 e IPv6
5.20	Deberá soportar Telnet / SSH para acceso a la consola
5.21	Deberá soportar HTTP / HTTPS
5.22	Deberá soportar SNMP v1/v2c/v3
5.23	Deberá poder configurar su reloj mediante un NTP Server
5.24	Deberá contar con una línea de comandos estándar y con interface para configurar vía Web
5.25	Deberá soportar actualizaciones de Software por: TFTP/FTP/GUI
5.26	Deberá soportar HTTP REST APIs para Configuración y monitoreo
5.27	Deberá soportar configuración de VLAN de forma centralizada. Donde se configure la VLAN una sola vez, y se pueda asignar a distintos switches y puertos.
5.28	La solución debe soportar administración centralizada en la premisa y en la nube, sin necesidad de cambiar modelos de equipos.

5.29	Debe soportar auto-discovery para administración centralizada. Es decir, que, al conectar el switch a la red, el controlador debe ser capaz de descubrirlo y administrarlo sin necesidad de configuración alguna en el switch.
5.30	La solución debe ser capaz de hacer agregación de enlaces de forma automática. Es decir, que pueda identificar dos enlaces conectados entre los mismos switches, y en lugar de bloquear un enlace con Spanning Tree, autoconfigure redundancia de enlaces para aprovecharlos al mismo tiempo sin intervención del administrador.
5.31	La solución debe ser capaz de encriptar el tráfico entre enlaces de administración y control.
5.32	Debe soportar Zero-Touch Deployment sobre enlaces capa 2 y capa 3.
5.33	Debe ser capaz de implementar Políticas de Control de Acceso a la red (NAC) que puedan filtrar basado en usuarios, grupos de usuarios del Directorio Activo, Tipo de Dispositivos, Sistema Operativo del dispositivo, Vulnerabilidades de dispositivos de IoT.
	Funcionalidades de Calidad de Servicio
5.34	Deberá soportar priorización de tráfico basada en 802.1p
5.35	Deberá soportar priorización de tráfico basada en IP TOS/DSCP
	Funcionalidades de Capa 2
5.36	Deberá soportar LACP
5.37	Deberá soportar Spanning Tree
5.38	Deberá soportar Jumbo Frames
5.39	Deberá soportar Auto-negociacion para la velocidad de los puertos y para Duplex
5.40	Deberá soportar el estándar IEEE 802.1D MAC Bridging/STP
5.41	Deberá soportar el estándar IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
5.42	Deberá soportar el estándar IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
5.43	Deberá soportar la funcionalidad STP Root Guard
5.44	Deberá soportar STP BPDU Guard
5.45	Deberá soportar Edge Port / Port Fast
5.46	Deberá soportar el estándar IEEE 802.1Q VLAN Tagging
5.47	Deberá poder balancear tráfico Unicast/Multicast sobre un puerto trunk (dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac)
5.48	Deberá soportar el estándar IEEE 802.1AX Link Aggregation
5.49	Deberá soportar instancias de Spanning Tree (MSTP/CST)
5.50	Deberá soportar el estándar IEEE 802.3x Flow Control con Back-pressure
5.51	Deberá soportar el estándar IEEE 802.3 10Base-T
5.52	Deberá soportar el estándar IEEE 802.3u 100Base-TX
5.53	Deberá soportar el estándar IEEE 802.3z 1000Base-SX/LX

5.54	Deberá soportar el estándar IEEE 802.3ab 1000Base-T
5.55	Deberá soportar el estándar IEEE 802.3 CSMA/CD como metodo de acceso y las especificaciones de la capa fisica
5.56	Deberá contar con la funcionalidad de Control de Tormentas (Storm Control)
5.57	Deberá soportar la creación de VLANs por MAC, IP y Ethertype-based
5.58	Deberá soportar Time-Domain Reflectometer (TDR)
5.59	Deberá soportar 4064 VLANs simultáneas
5.60	Deberá soportar IGMP Snooping
5.61	Deberá soportar IGMP proxy y querier
5.62	Deberá soportar emgency location identifier numbers (ELINs) en LLDP-MED
5.63	Deberá permitir limitar la cantidad de MACs aprendidas por puerto
5.64	Deberá permitir un mínimo de 15 instancias de MSTP
5.65	Deberá permitir controlar tormentas de broadcast independientemente en cada puerto
5.66	Deberá soportar un mecanismo de detección y prevención de loops
5.67	Deberá soportar SPAN
5.68	Admite conmutación de velocidad de cable y modo de envío Store and Forward
	Funcionalidades de Capa 3
5.69	Deberá soportar Layer 3 routing.
5.70	Deberá soportar DHCP Relay.
	Funcionalidades estandar soportadas (RFCs)
5.71	Deberá soportar Port Mirroring
5.72	Deberá soportar Admin Authentication Via RFC 2865 RADIUS
5.73	Deberá soportar el estándar IEEE 802.1x authentication Port-based
5.74	Deberá soportar el estándar IEEE 802.1x Authentication MAC-based
5.75	Deberá soportar el estándar IEEE 802.1x Guest and Fallback VLAN
5.76	Deberá soportar el estándar IEEE 802.1x MAC Access Bypass (MAB)
5.77	Deberá soportar el estándar IEEE 802.1x Dynamic VLAN Assignment
5.78	Deberá soportar Radius CoA (Change of Authority)
5.79	Deberá soportar el estándar IEEE 802.1ab Link Layer Discovery Protocol (LLDP)
5.80	Deberá soportar el estándar IEEE 802.1ab LLDP-MED
5.81	Deberá soportar Radius Accounting
5.82	Deberá soportar EAP pass-through
5.83	Deberá soportar detección de dispositivos
5.84	Deberá soportar ACLs
5.85	Deberá soportar scheduling de ACLs
5.86	Deberá soportar DHCP Snooping

5.87	Deberá soportar listas de servidores DHCP permitidos
5.88	Deberá soportar bloqueo de DHCP
5.89	Deberá permitir Dynamic ARP Inspection (DAI)
5.90	Deberá permitir Access VLANs
	Funcionalidades de Seguridad y Visibilidad
5.91	Deberá soportar Syslog
5.92	Debe soportar Energy-Efficient Ethernet (EEE)

Ítem 6. Switches CORE

Numeral	Especificaciones técnicas
6.1	Cantidad: 2
6.2	Tener al menos 48 interfaces 10G/1G SFP+/ SFP ports y 4 puertos 4x 100G/40G QSFP28/QSFP+
6.3	Throughput de switching de por lo menos 1760 Gbps
6.4	Soportar al menos 1518 Mbps de paquetes por segundos
6.5	Tener al menos 144k de almacenamiento de MAC Address
6.6	Soportar al menos 4K de VLANS
6.7	Tener al menos 8GB DDR3 de DRAM
6.8	Tener al menos 128MB de NOR
6.9	Tener al menos 128GB de SSD para almacenamiento
6.10	Tener al menos 800ns de latencia de switching
6.11	Tener al menos 12MB de buffer de paquetes
6.12	Tiene que ser un switch de 1RU
6.13	Debe incluir los siguientes SFP:
6.14	10 GE SFP+ transceiver module, long range 10km, LC connector, SMF (cantidad: 180 en total)
6.15	100 GE QSFP28 passive direct attach cable, 2m, transceivers included, for systems with QSFP28 slots (cantidad: 6 en total)
	Funcionalidades de Administración
6.16	El switch deberá poder aceptar actualizaciones de firmware
6.17	Los switches con PoE+ deberán tener la capacidad de habilitar o deshabilitar la función de PoE+
6.18	Deberá soportar detección y notificación de conflictos de direcciones IP
6.19	Deberá soportar administración por IPv4 e IPv6
6.20	Deberá soportar Telnet / SSH para acceso a la consola
6.21	Deberá soportar HTTP / HTTPS
6.22	Deberá soportar SNMP v1/v2c/v3
6.23	Deberá poder configurar su reloj mediante un NTP Server
6.24	Deberá contar con una línea de comandos estándar y con interface para configurar vía Web
6.25	Deberá soportar actualizaciones de Software por: TFTP/FTP/GUI
6.26	Deberá soportar HTTP REST APIs para Configuración y monitoreo

6.27	Deberá soportar configuración de VLAN de forma centralizada. Donde se configure la VLAN una sola vez, y se pueda asignar a distintos switches y puertos.
6.28	La solución debe soportar administración centralizada en la premisa y en la nube, sin necesidad de cambiar modelos de equipos.
6.29	Debe soportar auto-discovery para administración centralizada. Es decir, que, al conectar el switch a la red, el controlador debe ser capaz de descubrirlo y administrarlo sin necesidad de configuración alguna en el switch.
6.30	La solución debe ser capaz de hacer agregación de enlaces de forma automática. Es decir, que pueda identificar dos enlaces conectados entre los mismos switches, y en lugar de bloquear un enlace con Spanning Tree, autoconfigure redundancia de enlaces para aprovecharlos al mismo tiempo sin intervención del administrador.
6.31	La solución debe ser capaz de encriptar el tráfico entre enlaces de administración y control.
6.32	Debe soportar Zero-Touch Deployment sobre enlaces capa 2 y capa 6.
6.33	Debe ser capaz de implementar Políticas de Control de Acceso a la red (NAC) que puedan filtrar basado en usuarios, grupos de usuarios del Directorio Activo, Tipo de Dispositivos, Sistema Operativo del dispositivo, Vulnerabilidades de dispositivos de IoT.
	Funcionalidades de Calidad de Servicio
6.34	Deberá soportar priorización de tráfico basada en 802.1p
6.35	Deberá soportar priorización de tráfico basada en IP TOS/DSCP
	Funcionalidades de Capa 2
6.36	Deberá soportar LACP
6.37	Deberá soportar Spanning Tree
6.38	Deberá soportar Jumbo Frames
6.39	Deberá soportar Auto-negociacion para la velocidad de los puertos y para Duplex
6.40	Deberá soportar el estándar IEEE 802.1D MAC Bridging/STP
6.41	Deberá soportar el estándar IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
6.42	Deberá soportar el estándar IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
6.43	Deberá soportar la funcionalidad STP Root Guard
6.44	Deberá soportar STP BPDU Guard
6.45	Deberá soportar Edge Port / Port Fast
6.46	Deberá soportar el estándar IEEE 802.1Q VLAN Tagging
6.47	Deberá poder balancear tráfico Unicast/Multicast sobre un puerto trunk (dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac)
6.48	Deberá soportar el estándar IEEE 802.1AX Link Aggregation
6.49	Deberá soportar instancias de Spanning Tree (MSTP/CST)

6.50	Deberá soportar el estándar IEEE 802.3x Flow Control con Back-pressure
6.51	Deberá soportar el estándar IEEE 802.3 10Base-T
6.52	Deberá soportar el estándar IEEE 802.3u 100Base-TX
6.53	Deberá soportar el estándar IEEE 802.3z 1000Base-SX/LX
6.54	Deberá soportar el estándar IEEE 802.3ab 1000Base-T
6.55	Deberá soportar el estándar IEEE 802.3 CSMA/CD como metodo de acceso y las especificaciones de la capa fisica
6.56	Deberá contar con la funcionalidad de Control de Tormentas (Storm Control)
6.57	Deberá soportar la creación de VLANs por MAC, IP y Ethertype-based
6.58	Deberá soportar Time-Domain Reflectometer (TDR)
6.59	Deberá soportar 4064 VLANs simultáneas
6.60	Deberá soportar IGMP Snooping
6.61	Deberá soportar IGMP proxy y querier
6.62	Deberá soportar emgency location identifier numbers (ELINs) en LLDP-MED
6.63	Deberá permitir limitar la cantidad de MACs aprendidas por puerto
6.64	Deberá permitir un mínimo de 15 instancias de MSTP
6.65	Deberá permitir controlar tormentas de broadcast independientemente en cada puerto
6.66	Deberá soportar un mecanismo de detección y prevención de loops
6.67	Deberá soportar SPAN
6.68	Admite conmutación de velocidad de cable y modo de envío Store and Forward
	Funcionalidades de Capa 3
6.69	Deberá soportar Layer 3 routing.
6.70	Deberá soportar DHCP Relay.
	Funcionalidades estandar soportadas (RFCs)
6.71	Deberá soportar Port Mirroring
6.72	Deberá soportar Admin Authentication Via RFC 2865 RADIUS
6.73	Deberá soportar el estándar IEEE 802.1x authentication Port-based
6.74	Deberá soportar el estándar IEEE 802.1x Authentication MAC-based
6.75	Deberá soportar el estándar IEEE 802.1x Guest and Fallback VLAN
6.76	Deberá soportar el estándar IEEE 802.1x MAC Access Bypass (MAB)
6.77	Deberá soportar el estándar IEEE 802.1x Dynamic VLAN Assignment
6.78	Deberá soportar Radius CoA (Change of Authority)
6.79	Deberá soportar el estándar IEEE 802.1ab Link Layer Discovery Protocol (LLDP)
6.80	Deberá soportar el estándar IEEE 802.1ab LLDP-MED
6.81	Deberá soportar Radius Accounting

6.82	Deberá soportar EAP pass-through
6.83	Deberá soportar detección de dispositivos
6.84	Deberá soportar ACLs
6.85	Deberá soportar scheduling de ACLs
6.86	Deberá soportar DHCP Snooping
6.87	Deberá soportar listas de servidores DHCP permitidos
6.88	Deberá soportar bloqueo de DHCP
6.89	Deberá permitir Dynamic ARP Inspection (DAI)
6.90	Deberá permitir Access VLANs
	Funcionalidades de Seguridad y Visibilidad
6.91	Deberá soportar Syslog
6.92	Debe soportar Energy-Efficient Ethernet (EEE)

Ítem 7. Firewalls

Numeral	Especificaciones técnicas
7.1	Cantidad: 2
7.2	Throughput de por lo menos 76 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6
7.3	Throughput de al menos 55 Gbps de VPN IPSec
7.4	Soportar al menos 12 Gbps de throughput de IPS
7.5	Soportar al menos 10 Gbps de throughput de NGFW
7.6	Soportar al menos 6 Gbps de throughput de Threat Protection
7.7	Soporte hasta 7.8 Millones conexiones simultaneas
7.8	Soporte hasta 500K de nuevas conexiones por segundo
7.9	Estar licenciado para, o soportar sin necesidad de licencia, 2,000 túneles de VPN IPSec site-to-site simultáneos
7.10	Estar licenciado para, o soportar sin necesidad de licencia, 50,000 túneles de clientes VPN IPSec simultáneos
7.11	Throughput de al menos 3.6 Gbps de VPN SSL
7.12	Soportar al menos 5,000 clientes de VPN SSL simultáneos
7.13	Soportar al menos 8 Gbps de throughput de Inspección SSL
7.14	Soportar al menos 28 Gbps de throughput de Application Control
7.15	Debe soportar 25 sistemas virtuales lógicos (dominios virtuales) por appliance
7.16	Tener al menos 8 interfaces 10Gbps de fibra SFP+.
7.17	Tener al menos 8 interfaces 1Gbps de fibra SFP.
7.18	Tener al menos 18 interfaces 1Gbps de cobre RJ45.
7.19	Debe contar con fuente de poder redundante (Dual Power Supply).
7.2	La solución debe poseer un software centralizado para el monitoreo del performance del equipo a nivel de recursos (CPU, Memoria, sesiones, temperatura, etc…) y a nivel de red (cantidad de tráfico por enlace) que permite conservar el historial de al menos 3 meses.
7.21	La solución debe incluir licencias o features de seguridad que permitan configurar túneles ipsec entre los sitios remotos y el centro de datos principal para proteger el tráfico en la red WAN.
7.22	La solucion debe proveer un sistema de aprovisionamiento central proporcionando una pieza de software que controle todos los nodos de forma interdependiente.
7.23	La solución debe permitir la visibilidad en la WAN.
7.24	La solución debe ser capaz de implementar monitoreo y optimización de aplicaciones en tiempo real.

7.25	La solución debe permitir el aprovisionamiento sin necesidad de intervención, es decir, la configuración del dispositivo de red debe poder realizarse de forma remota. Solo es necesario conectar los equipos. Una vez encendidos los dispositivos se descubren automáticamente, descargan las configuraciones y comienzan a funcionar.
7.26	La solución de administración centralizada debe tener la capacidad de manejar la solución de Firewall, Switches, Wireless y SD-WAN desde una misma consola de gestión.
7.27	La solución debe contar con una herramienta de administración centralizada capaz de crecer hasta al menos 10,000 dispositivos administrado desde un único panel de gestión.
7.28	La solución debe integrarse a la plataforma de management actual.
	Instalación y condiciones físicas
7.29	Los equipos deben soportar temperaturas de hasta 40 grados centígrado y humedad de 10–60% sin afectar el funcionamiento de los mismos.
7.30	La infraestructura propuesta debe ser instalable en gabinetes estándares.
7.31	Los equipos deben quedar atornillados a los gabinetes de red. En caso de que las dimensiones físicas de los equipos no sea la adecuada para instalar en gabinetes el suplidor deberá incluir en su propuesta rack mount kit para realizar la correcta instalación de los equipos. No se permitirán instalación de bandejas.
7.32	La instalación física de los equipos debe de realizar bajo los mejores estándares de la industria.
7.33	Los equipos Firewall a instalar deben de contar con redundancia a nivel de power.
	La solución debe brindar la funcionalidad de SD-WAN permitiendo:
7.34	Dirigir el tráfico de acuerdo a políticas de seguridad definidas centralmente controlando el acceso a las distintas zonas y a Internet. El tráfico crítico se podrá aplicar políticas de calidad de servicio, mientras que el tráfico menos esencial se podrá dirijir a los recursos restantes. La solución debe poder hacer una selección de rutas dinámicas: Permitiendo balanceo de cargas a través de las conexiones WAN.
7.35	La solución debe ser capaz de manejar el tráfico de cada localidad remota de manera eficiente incluyendo tráfico de aplicaciones manejado por los usuarios, tráfico de voz, video, sistemas de gestión y administración.
7.36	Los equipos SD-WAN deben ser capaz de formar conexiones entre los sitios usando
7.37	túneles VPN con cifrado avanzado contando cada appliance con doble módulos de power.
7.38	Debe soportar SD-WAN con multiples tipos de conexiones simultaneas como: MPLS, Internet Broadband, y LTE.

7.39	Si falla un enlace, la solución debe permitir que el tráfico se redireccione automáticamente a los enlaces restantes en un tiempo máximo de 1 segundo.
7.40	La solución de redes SD-WAN se debe poder administrar a través de una consola central con una interfaz de usuario gráfica y moderna. La solución debe poseer un software de gestión vía GUI o WEB para su administración
7.41	El control de ruta o la selección de ruta debe dirigir el tráfico en función de la prioridad de la aplicación a los enlaces de red apropiados.
7.42	Las políticas globales o locales configuradas para SD-WAN deben poder configurarse fácilmente en una consola de administración con reglas simples tales como: enviar tráfico de video a través de los circuitos de mayor capacidad; enviar actualizaciones de software a través de circuitos de banda ancha de Internet; o enviar todo el tráfico de negocio a través de redes privadas virtuales (VPN) seguras.
7.43	La solución debe estar como líder en el último cuadrante de Gartner de WAN Edge Infrastructure.
	Condiciones Técnicas y control de aplicaciones
7.44	Debe soportar protocolos de enrutamiento avanzado como OSPF, BGP, ISIS.
7.45	Debe permitir el filtrado del tráfico en base a políticas de firewalls, webfiltering, y App control.
7.46	Permite acelerar las aplicaciones y minimizar el consumo de ancho de banda de la WAN.
7.47	Los dispositivos de red deben soportar 4064 VLANs Tags 802.1q, DHCP Relay, DHCP Relay, Jumbo Frames.
7.48	Debe contar con políticas de control por puerto y protocolo.
7.49	Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF).
7.50	La solución debe tener la capacidad de ser integrado con una solución utilizando el
7.51	protocolo Netflow.
7.52	La solución debe de ser capaz de identificar el tráfico de red por fuente de origen o destino, tipo de aplicación y usuarios.
7.53	Se deben soportar mecanismos de registros de la actividad de los usuarios en términos de ingreso o salida.
7.54	El sistema debe permitir el ingreso de las credenciales de un usuario, y debe poder permitir integrarse con MS Active Directory, LDAP y RADIUS. Con este mecanismo se puede determinar la identidad del usuario.
7.55	La solución debe tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo.

7.56	Soporte a bloqueo de contraseñas por intentos errados y expiración de contraseñas para cuentas locales.
7.57	La solución y el proveedor cuentan con un procedimiento para detectar vulnerabilidades y para actualización de parches de seguridad.
7.58	Manejo de encriptación, permitiendo que la información crítica y sensible (almacenada y transmitida) se cifre para su seguridad.
7.59	Capacidad de administración de los permisos que tienen los usuarios para realizar configuraciones y cambios en los equipos determinados por perfiles predefinidos.
7.60	La comunicación de interfaces debe contar con cifrado, autenticación y manejos de sesiones.
7.61	Debe contar con protocolos de cifrado SSL y certificados para las conexiones administrativas.
7.62	Debe permitir la inspección de paquetes cifrado para identificar micro aplicaciones.
7.63	La solución debe identificar al menos 2100 aplicaciones.
7.64	La solución debe estar como líder en el último cuadrante de Gartner de Network Firewall.
	QoS Traffic Shaping
7.65	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.
7.66	Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen, destino, usuario, grupo, puerto. Soportar la priorización de protocolo en tiempo real de voz (VoIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype. Debe soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service). En QoS debe permitir la definición de tráfico con ancho de banda garantizado, con máximo ancho de banda y la definición de colas de prioridad.
7.67	Sa solución debe soportar la función "Packet Duplication" para mejorar la experiencia del usuario en caso de fallas en los enlaces.
	Control de Auditoría
7.68	Debe generar logs de ejecución de proceso (usuario, fecha, tarea, etc) y manejo de logs de seguridad.
7.69	Logs deben ser exportables para ser integrados a herramienta SIEM.
7.70	El sistema debe mantener una bitácora de auditoría de cada vez que el usuario ingresa o sale del sistema.

Ítem 8. Solución de Almacenamiento de Logs

Numeral	Especificaciones técnicas
8.1	Cantidad: 1
8.2	La solucion propuesta debe ser una máquina virtual la cual debe soportar 20GB/logs por dia y debe ser desplegables sobre arquitecturas VMware, Hyper-V, AWS o Azure
8.3	La solucion propuesta debe incluir los licenciamientos de Indicators of Compromise Service, Security Automation Service, Outbreak Service.
8.4	Debe soportar acceso vía SSH, WEB (HTTPS) para la gestion de la solución
8.5	Contar con comunicación cifrada y autenticación con usuario y contraseña para la obtención de reportes, tanto en interface gráfica (GUI) como vía linea de comandos en consola de gestión.
8.6	Permitir acceso simultáneo de administración, así como permitir crear por lo menos 2 (dos) perfiles para administración y monitoreo.
8.7	Soporte SNMP versión 2 y 3
8.8	Permitir virtualizar la gestión y administración de los dispositivos, donde cada administrador solo tenga acceso a los equipos autorizados.
8.9	Debe permitir la creación de administrador general, que tenga acceso general a todas las instancias de virtualización de la solución.
8.10	Debe permitir activar y desactivar para cada interface de la plataforma, los permisos de acceso HTTP, HTTPS, SSH
8.11	Autenticación de usuarios de acceso a la plataforma via LDAP
8.12	Autenticación de usuarios de acceso a la plataforma via Radius
8.13	Autenticación de usuarios de acceso a la plataforma via TACACS+
8.14	Generación de informes en tiempo real de tráfico, en formato de gráfica de mapas geográficos
8.15	Generación de informes en tiempo real de tráfico, en formato de gráfica de burbuja.
8.16	Generación de informes en tiempo real de tráfico, en formato de gráfica tabla
8.17	Definición de perfiles de acceso a consola con permiso granulares, tales como: acceso de escritura, de lectura, de creación de nuevos usuarios y cambios en configuraciones generales.
8.18	Debe contar con un asistente gráfico para agregar nuevos dispositivos, usando la dirección IP, usuario y contraseña del mismo.
8.19	Debe ser posible ver la cantidad de logs enviados desde cada dispositivo supervisado
8.2	Contar con mecanismos de borrado automático de logs antiguos.

8.21	Permitir la importación y exportación de reportes
8.22	Debe contar con la capacidad de crear informes en formato HTML
8.23	Debe contar con la capacidad de crear informes en formato PDF
8.24	Debe contar con la capacidad de crear informes en formato XML
8.25	Debe contar con la capacidad de crear informes en formato CSV
8.26	Debe permitir exportar los logs en formato CSV
8.27	Generación de logs de auditoría, con detalle de la configuración realizada, el administrador que realizó el cambio y hora del mismo.
8.28	Los logs generados por los dispositivos administrados deben ser centralizados en los servidores de la plataforma, pero la solución debe ofrecer también la posibilidad de utilizar un servidor externo de Syslog o similar.
8.29	La solución debe contar con reportes predefinidos
8.30	Debe poder enviar automáticamente los logs a un servidor FTP externo a la solución
8.31	Debe ser posible la duplicación de reportes existentes para su posterior edición.
8.32	Debe tener la capacidad de personalizar la portada de los reportes obtenidos.
8.33	Permitir centralmente la visualización de logs recibidos por uno o más dispositivos, incluido la capacidad de uso de filtros para facilitar la búsqueda dentro de los mismos logs.
8.34	Los logs de auditoría de cambios de configuración de reglas y objetos deben ser visualizados en una lista distinta a la de los logs relacionados a tráfico de datos.
8.35	Tener la capacidad de personalización de gráficas en los reportes, tales como barras, líneas y tablas
8.36	Debe poseer mecanismo de “Drill-Down” para navegar en los reportes de tiempo real.
8.37	Debe permitir descargar de la plataforma los archivos de logs para uso externo.
8.38	Tener la capacidad de generar y enviar reportes periódicos automáticamente.
8.39	Permitir la personalización de cualquier reporte preestablecido por la solución, exclusivamente por el Administrador, para adoptarlo a sus necesidades.
8.40	Permitir el envío por email de manera automática de reportes.
8.41	Debe permitir que el reporte a enviar por email sea al destinatario específico.
8.42	Permitir la programación de la generación de reportes, conforme a un calendario definido por el administrador.
8.43	Debe ser posible visualizar gráficamente en tiempo real la tasa de generación de logs por cada dispositivo gestionado.
8.44	Debe permitir el uso de filtros en los reportes.
8.45	Debe permitir definir el diseño de los reportes, incluir gráfico, añadir texto e imágenes, alineación, saltos de página, fuentes, colores, entre otros.

8.46	Permitir especificar el idioma de los reportes creados
8.47	Generar alertas automáticas vía email, SNMP y Syslog, basado en eventos especiales en logs, severidad del evento, entre otros.
8.48	Debe permitir el envío automático de reportes a un servidor externo SFTP o FTP.
8.49	Debe ser capaz de crear consultas SQL o similar dentro de las bases de datos de logs, para uso en gráficas y tablas en reportes.
8.50	Tener la capacidad de visualizar en GUI de reportes de información del Sistema, como licencias, memoria, disco duro, uso de CPU, tasa de logs por segundo recibidos, total de logs diarios recibidos, alertas del sistema, entre otros.
8.51	Debe contar con una herramienta que permita analizar el rendimiento en la generación de reportes, con el objetivo de detectar y arreglar problemas en generación de los mismos.
8.52	Que la solución sea capaz de importar archivos con logs de dispositivos compatibles conocido y no conocidos por la plataforma, para posterior generación de reportes.
8.53	Debe ser posible poder definir el espacio que cada instancia de virtualización puede utilizar para almacenamiento de logs.
8.54	Debe proporcionar la información de cantidad de logs almacenados y la estadística de tiempo restante de almacenado.
8.55	Debe ser compatible con autenticación de doble factor (token) para usuarios administradores de la plataforma.
8.56	Debe permitir aplicar políticas para el uso de contraseñas para los administradores de la plataforma, como tamaño mínimo y caracteres permitidos
8.57	Debe permitir visualizar en tiempo real los logs recibidos.
8.58	Debe permitir el reenvío de logs en formato syslog.
8.59	Debe permitir el reenvío de logs en formato CEF (Common Event Format).
8.60	Debe incluir dashboard para operaciones SOC que monitorea las principales amenazas de seguridad para su red
8.61	Debe incluir dashboard para operaciones SOC que monitorea comprometimiento de usuarios y uso sospechoso de la web en su red.
8.62	Debe incluir dashboard para operaciones SOC que monitorea el tráfico en su red.
8.63	Debe incluir dashboard para operaciones SOC que monitorea el tráfico de aplicaciones y sitios web en su red
8.64	Debe incluir dashboard para operaciones SOC que monitorea detecciones de amenazas de día cero en su red (sandboxing).
8.65	Debe incluir dashboard para operaciones SOC que monitorea actividad de endpoints en su red.

8.66	Debe incluir dashboard para operaciones SOC que monitorea actividad VPN ren su red.
8.67	Debe incluir dashboard para operaciones SOC que monitorea puntos de acceso WiFi y SSIDs
8.68	Debe incluir dashboard para operaciones SOC que monitorea rendimiento de recursos local de la solución (CPU, Memoria)
8.69	Debe permitir crear dashboards personalizados para monitoreo de operaciones SOC
8.70	Debe soportar configuración de alta disponibilidad Master/Slave en la capa 3
8.71	Debe permitir generar alertas de eventos a partir de logs recibidos
8.72	Debe permitir crear incidentes a partir de alertas de eventos para endpoint
8.73	Debe permitir la integración al sistema de tickets ServiceNow
8.74	Debe soportar servicio de Indicadores de Compromiso (IoC) del mismo fabricante, que muestre las sospechas de comprometimiento de usuarios finales en la web, debiendo informar por lo menos: dirección IP de usuario, hostname, sistema operativo, veredicto (clasificación general de la amenaza), el número de amenazas detectadas.
8.75	Debe permitir respaldar logs en nube publica de Amazon S3
8.76	Debe permitir respaldar logs en nube publica de Microsoft Azure
8.77	Debe permitir respaldar logs en nube publica de Gooogle Cloud
8.78	Debe soportar el estándar SAML para autenticación de usuarios administradores
	Firewall Reports
8.79	Debe contar con reporte de cumplimiento de PCI DSS
8.80	Debe contar con reporte de utilización de aplicaciones SaaS
8.81	Debe contar con reporte de prevención de perdida de datos (DLP)
8.82	Debe contar con reporte de VPN
8.83	Debe contar con reporte de Sistema de prevención de intrusos (IPS)
8.84	Debe contar con reporte de reputación de cliente
8.85	Debe contar con reporte de análisis de seguridad de usuario
8.86	Debe contar con reporte de análisis de amenaza cibernética
8.87	Debe contar con reporte de breve resumen diario de eventos e incidentes de seguridad
8.88	Debe contar con reporte de tráfico DNS
8.89	Debe contar con reporte tráfico de correo electrónico
8.90	Debe contar con reporte de Top 10 de Aplicaciones utilizadas en la red
8.91	Debe contar con reporte de Top 10 de Websites utilizadas en la red
8.92	Debe contar con reporte de uso de redes sociales
	Email Reports
8.93	Debe contar con reporte de evaluación de riesgo para correo electrónico

	Wireless Reports
8.94	Debe contar con reporte de cumplimiento PCI de Wireless.
8.95	Debe contar con reporte de AP´s y SSID´s autorizados, así como clientes WIFi
	Endpoint Reports
8.96	Debe contar con reporte de vulnerabilidades de solución gestionada de seguridad de equipo terminal.
	WAF Reports
8.97	Debe contar con reporte de aplicaciónes web, si se cuenta con plataforma de seguridad web

Ítem 9. Solución de Secure Access Servie Edge

Numeral	Especificaciones técnicas
9.1	Cantidad: 1
9.2	Se requiere de una solución (SaaS) del tipo Secure Access Service Edge (SASE) que proporcione visibilidad, cumplimiento, seguridad de datos y protección contra amenazas para servicios basados en la nube.
9.3	La solución debe ser soportada para 200 usuarios.
9.4	La solución propuesta debe proveer capacidades de Secure Web Gateway y Firewall as a Service (FWaaS) para dispositivos con o sin agente.
9.5	La solución propuesta debe permitir acceso granular por aplicación pudiéndose realizar dinámicamente un cambio de critico de confianza implícita a explicita con el uso de ZTNA.
9.6	La solución propuesta debe brindar capacidades de Deep Inspección SSL para el análisis de tráfico encriptado.
9.7	La solución propuesta debe analizar el comportamiento de los usuarios para detectar comportamientos sospechosos o irregulares y generar alertas por comportamiento malicioso.
9.8	La solución propuesta debe realizar análisis activos de detección de virus y malware.
	Funcionalidades Especificas de SASE
9.9	La solución propuesta debe permitir la inspección de tráfico encriptado usando TLS 1.3.
9.10	La solución propuesta debe soportar la implementación con agente y sin agente.
9.11	La solución propuesta debe brindar reconocimiento de al menos 4800 aplicaciones.
9.12	La solución propuesta debe poseer la capacidad de antivirus/antimalware en línea con soporte de sandbox cloud u on-premise.
9.13	La solución propuesta debe proveer control de navegación a través del uso de categorización de sitios web, patrones específicos de URL y filtrado de contenido.
9.14	La solución propuesta debe brindar protección de DNS a través del uso de categorías, así de patrones personalizados, también debe reconocer y bloquear conexiones a sitios de Bonet y CsC.
9.15	La solución propuesta debe proporcionar capacidades de Intrusion Prevention (IPS) para la detección y mitigación de ataques de red.
9.16	La solución propuesta debe provee capacidades de filtrado de archivos basados en el tipo de archivo.

9.17	La solución propuesta debe permitir la autenticación de usuarios de locales, así como remotos de Active Directory/LDAP, RADIUS y Azure AD.
9.18	La solución propuesta debe permitir el uso de dos dispositivos con o sin agente por usuario licenciado.
9.19	La solución propuesta debe brindar capacidades de escaneo de vulnerabilidades de los dispositivos.
9.20	La solución propuesta debe soportar conectividad a través de auto túneles, como de navegador web.
9.21	La solución propuesta debe proveer la capacidad de monitorear los siguientes parámetros de uso: Orígenes
9.22	de conexión, Destinos de conexión, Aplicaciones, Aplicaciones de nube, Sitios web, Uso de políticas, Sesiones y Amenazas.
9.23	La solución propuesta debe proveer la capacidad de generar reportes bajo demanda o programados tales
9.24	como: Reporte de amenazas, Reporte de uso Web, Eventos e incidentes de seguridad, Uso de ancho de banda de aplicaciones y Nivel de riesgo de aplicaciones.
9.25	La solución propuesta debe soportar la creación de políticas usando Zero Trust Tags para la creación de políticas hacia a internet y hacia premisas.
9.26	La solución debe permitir integrarse con la solución actual de Firewall para poder compartir los perfiles de IPS, Filtrado Web, Perfil de Antivirus y control de aplicaciones.
9.27	La solución propuesta debe permitir la integración con los Firewall actuales sin necesidad de appliance virtual o físico.
9.28	La solución propuesta debe permitir la integración de un ZTNA Proxy gateway con el firewall actual para enviar tráfico directo hacia las aplicaciones en premisas sin necesidad de ir a un Point of Presence.
9.29	La solución propuesta debe soportar al menos cuatro (4) Point of Presence (PoP) en diferentes regiones alrededor del mundo.
9.30	La solución propuesta debe incluir ip publicas dedicadas para la organización.
9.31	La solución propuesta debe permitir el monitoreo en tiempo real de las aplicaciones(Jitter, Delay) SaaS como Office 365, tanto en los Point of Precense o en los dispositivos finales.
9.32	La solución propuesta no debe limitar el ancho de banda de los usuarios.
9.33	La solución propuesta debe incluir al menos tres dispositivos por licenciamiento de usuario.

Ítem 10. Solución de Administración Centralizada

Numeral	Especificaciones técnicas
10.1	Cantidad: 1
10.2	Si la solución es virtualizada, debe ser compatible con el ambiente VMware ESXi 5.0/5.1/5.5/6.0/6.5/6.7; Microsoft Hyper-V 2008 R2 / 2012 / 2012 R2/2016; Citrix XenServer 6.0+; Open Source Xen 4.1+; KVM on Redhat 6.5+ and Ubuntu 17.04; Amazon Web Services (AWS); Microsoft Azure; Google Cloud (GPC); Oracle Cloud Infraestructure (OCI); Alibaba Cloud (AliCloud).
10.3	No debe haber límites a la cantidad de múltiples vCPU si el aparato es virtual;
10.4	No debe haber límites a la expansión de memoria RAM si el aparto es virtual;
10.5	Si la solución es virtualizada, debe tener capacidades de Alta disponibilidad (HA)
10.6	Debe tener la capacidad de permitir provisionar y monitorear configuración de SD-WAN de todos los dispositivos gestionados desde una sola consola.
10.7	Como parte de la visibilidad SD-WAN de los dispositivos gestionados centralmente, la solución debe contar con visibilidad de estado de enlace, desempeño de aplicación, utilización de ancho de banda y cumplimiento de SLA objetivo.
10.8	Debe tener la capacidad de automatizar flujos de trabajo y configuraciones para los dispositivos gestionados desde una sola consola
10.9	La solución debe tener la capacidad Multi-tenancy para separar los datos de gestión de infraestructura de manera lógica o geográfica y permitir despliegue zerotouch para un aprovisionamiento masivo rápido.
10.10	La solución debe ser capaz de realizar respaldos automáticos de configuración hasta en 5 nodos, conteniendo updates de todos los dispositivos gestionados.
10.11	Debe tener la capacidad de permitir provisionar comunidades VPN y monitorear conexiones VPN de todos los dispositivos gestionados desde una sola consola y mostrar su geolocalización en un mapa.
10.12	La solución debe permitir utilización de API RESTful para permitir interacción con portales personalizados en la configuración de objetos y políticas de seguridad.
10.13	Permitir integración de intercambio y compartición de datos con terceros mediante pxGrid, OCI, Esxi .
10.14	En la fecha de la propuesta, ninguno de los modelos de la oferta puede estar en el sítio del fabricante en listados de end-of-life o end-of-sales;
10.15	La gestión de la solución debe soportar acceso por SSH, cliente o WEB (HTTPS) y API abierta;

10.16	Debe permitir accesos concurrentes de administradores;
10.17	Debe tener interfaz basada en línea de comando para administración de la solución de gestión;
10.18	Debe tener un mecanismo de búsqueda por comandos en la gestión por SSH, facilitando la ubicación de comandos;
10.19	Bloquear cambios, en el caso de acceso simultaneo de dos o más administradores;
10.2	Definición de perfiles de acceso a la consola con permiso granular como: acceso a escrita, acceso de lectura, creación de usuarios, cambio de configuraciones;
10.21	Generar alertas automáticas por Email
10.22	Generar alertas automáticas por SNMP
10.23	Generar alertas automáticas por Syslog
10.24	Debe soportar backup/restore de todas las configuraciones de la solución de gestión, permitiendo al administrador agendar backups de configuración en un determinado día y horário;
10.25	Debe ser permitido al administrador transferir los backups a un servidor FTP.
10.26	Debe ser permitido al administrador transferir los backups a un servidor SCP
10.27	Debe ser permitido al administrador transferir los backups a un servidor SFTP
10.28	Los cambios realizados en un servidor de gestión deben ser automáticamente replicados al servidor redundante;
10.29	Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de cuentas de usuarios LOCALES
10.3	Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de base externa TACACS+
10.31	Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de base externa LDAP
10.32	Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de base externa RADIUS
10.33	Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de Certificado Digital X.506 (PKI)
10.34	Debe soportar sincronización de reloj interno por protocolo NTP.
10.35	Debe registrar las acciones efectuadas por cualquier usuario;
10.36	Deben proveerse manuales de instalación, configuración y operación de toda la solución, en los idiomas español, portugués o inglés, con presentación de buena calidad;
10.37	Debe suportar SNMP versión 2 y la versión 3 en los equipos de gestión;

10.38	Debe permitir habilitar o deshabilitar, para cada interfaz de red de la solución de gestión, permisos de acceso HTTP, HTTPS, SSH, SNMP y Web Services (API);
10.39	Debe permitir virtualizar la solución de gestión, de manera que cada administrador pueda gerenciar, visualizar y editar solo los dispositivos autorizados y registrados en su ambiente virtualizado;
10.40	La solución de gestión debe permitir crear administradores que tengan acceso a todas las instancias de virtualización;
10.41	La gestión debe permitir la creación y administración de políticas de firewall y control de aplicación;
10.42	La gestión debe permitir la creación y administración de políticas de IPS, Antivirus y Anti- Spyware;
10.43	La gestión debe permitir la creación y administración de políticas de Filtro de URL;
10.44	Permitir buscar cuáles reglas un objeto está siendo utilizado;
10.45	Permitir la creación de reglas que permanezcan activas en horario definido;
10.46	La solución debe permitir ser repositorio de firmas de antivirus, IPS, Web Filtering, email filtering, para optimizar la velocidad y descarga centralizada a los dispositivos gestionados
10.47	Debe tener capacidad de desplegar los resultados de auditoría de seguridad d en los dispositivos gestionados
10.48	Permitir backup de las configuraciones y rollback de configuración para la última configuración salva;
10.49	Debe tener mecanismos de validación de políticas avisando cuando haya reglas que ofusquen o conflictúen con otras (shadowing);
10.5	Debe permitir la visualización y comparación de configuraciones actuales, configuraciones previas y configuraciones antiguas;
10.51	Debe posibilitar que todos los firewalls sean controlados de manera centralizada utilizando solo un servidor de gestión;
10.52	La solución debe incluir una herramienta para gestionar centralmente las licencias de todos los aparatos controlados por estaciones de gestión, permitiendo al administrador actualizar licencias en los aparatos a través de esta herramienta;
10.53	La solución debe permitir la distribución y instalación remota, de manera centralizada, de nuevas versiones de software de los aparatos;
10.54	Debe ser capaz de generar reportes o presentar comparativos entre dos secciones distintas, resumiendo todos los cambios efectuados;

10.55	Debe permitir crear flujos de aprobación en la solución de gestión, donde un administrador pueda crear todas las reglas, pero estas mismas solamente sean aplicadas después de la aprobación de otro administrador;
10.56	Tener "wizard" en la solución de gestión para agregar los dispositivos por interfaz gráfica utilizando IP, login y clave de estos;
10.57	Permitir que las políticas y los objetos ya presentes en los dispositivos sean importados a la solución de gestión cuando se agregan.
10.58	Permitir la visualización, a partir de la estación de gestión centralizada, informaciones detalladas de los dispositivos gerenciados, tales como hostname, serial, IP de gestión, licencias, horario de lo sistema y firmware;
10.59	Tener "wizard" en la solución de gestión para instalación de políticas y configuraciones de los dispositivos;
10.6	Permitir crear en la solución de gestión templates de configuración de los dispositivos con informaciones de DNS, SNMP, configuraciones de LOG y administración;
10.61	Permitir crear scripts customizados, que sean ejecutados de forma centralizada en un o más dispositivos gestionados con comandos de CLI de los mismos;
10.62	Tener histórico de los scripts ejecutados en los dispositivos gestionados pela solución de gestión;
10.63	Permitir configurar y visualizar el manejo de SD-WAN de los dispositivos gestionados de forma centralizada;
10.64	Permitir crear varios paquetes de políticas que serán aplicados/asociados a los dispositivos o grupos de dispositivos;
10.65	Debe permitir crear reglas de NAT64 y NAT46 de forma centralizada;
10.66	Permitir la creación de reglas anti DoS de forma centralizada;
10.67	Debe permitir la creación de objetos que serán utilizados en las políticas de forma centralizada;
10.68	Debe permitir crear a partir de la solución de gestión, VPNs entre los dispositivos gestionados de forma centralizada, incluyendo topología (hub, spoke, dial-up) autenticaciones, claves y métodos de criptografía;
10.69	Debe permitir el uso de DDNS en VPNs de manera centralizada
10.70	Debe permitir la gestión de Access Points propietarios de manera centralizada
10.71	Debe permitir la gestión de Switches propietarios de manera centralizada
10.72	Debe permitir la gestión de perfiles de seguridad de software endpoint propietario de manera centralizada
10.73	Con la adquisición se deben incluir todos los conectores, cables y licenciamiento necesario de toda la solución

10.74	La solución debe incluir todo el licenciamiento necesario para sacar beneficio de todos los feature indicados

Ítem 11. Solución de Network Access Control

Numeral	Especificaciones técnicas
11.1	Cantidad: 1
11.2	Solución de Control de Acceso basada en máquinas virtuales (VMs), desplegables sobre arquitecturas
11.3	VMware, Hyper-V, AWS o Azure
11.4	La solución debe soportar, al menos 1000 dispositivos conectados simultáneamente desde un único appliance, y deberá poder escalar hasta 15,000 dispositivos con la adición de licenciamiento a la arquitectura.
11.5	La Arquitectura de la solución debe ser escalable, permitiendo instalaciones de múltiples dispositivos físicos o virtuales coordinados para dar servicio de acceso a instalaciones de cientos de miles de dispositivos.
11.6	En caso de requerirse múltiples Appliances o VMs para la implementación de la solución, esta deberá permitir la administración centralizada del conjunto desde un Appliance o VM de administración
11.7	La solución debe ser licenciable por dispositivo concurrente. Estas licencias deben ser perpetuas y deben permitir distintos niveles de operación (visibilidad, control, cumplimiento)
11.8	La solución debe permitir un despliegue centralizado, en una arquitectura fuera de banda, y brindar control de acceso en Capa 2 y Capa 3 sobre una infraestructura cableada e inalámbrica.
11.9	Debe permitir crear una estructura jerárquica que permita ordenar los dispositivos de infraestructura de la red de manera lógica y/o geográfica.
11.10	Debe permitir crear, modificar y borrar dispositivos y sus características.
11.11	Debe permitir el registro manual de dispositivos no SNMP.
11.12	Debe contar con un proceso continuo de detección y categorización de dispositivos de infraestructura de red, que permita detectar y controlar los switches, routers y otros dispositivos de la red.
11.13	Debe permitir mover fácilmente los dispositivos dentro de la estructura jerárquica generada
11.14	Debe permitir realizar consulta a nivel Capa 2 y Capa 3 (polling) de los dispositivos que se encuentren conectados a los equipos de red controlados, para poder utilizar esta información en la fase de control de acceso.
11.15	La solución debe poder ser registrada como un dispositivo independiente dentro de la topología física en la consola de gestión unificada del firewall del mismo fabricante de la solución de control de acceso a la red ofertada

11.16	La solución debe operar indistintamente para entornos cableados o inalámbricos, locales o remotos.
11.17	Debe permitir la detección de hosts desconocidos (rogue)
11.18	Debe permitir la identificación de hosts mediante Portal Cautivo
11.19	Debe permitir la categorización automática de hosts y dispostivos IoT.
11.2	Debe permitir la recategorización periódica de los hosts desconocidos
11.21	Debe recordar el perfil asignado a cada host, y verificar que sigue siendo válido en cada nueva conexión del host. Si el perfil variara, deberá impedir su conexión y notificar inmediatamente sobre el evento.
11.22	Debe permitir la fijación de períodos de tiempo en los que el host está autorizado a conectarse, y evaluarlos periódicamente.
11.23	Debe permitir la importación de un archivo .CSV conteniendo información sobre los hosts a registrar.
11.24	Debe permitir la integración con plataformas MDM.
11.25	La solución no debe requerir el uso de 802.1x para permitir el descubrimiento de hosts o usuarios, o brindar control de acceso a nivel de Puerto en la infraestructura cableada.
11.26	Debe permitir determinar el perfil de los hosts descubiertos mediante métodos que no requieran la instalación de agentes incluyendo, al menos, los siguientes: - DHCP Fingerprinting - HTTP/HTTPS - Ubicación - Rangos IP - SNMP - SSH - Telnet - TCP - UDP - OUI - WMI - WinRM - Activo con NMAP - Pasivo con P0F - Agente - ONVIF - Network traffic - Script usando Perl
11.27	Debe permitir determinar el perfil de los dispositivos IoT mediante una URL hacia una base de datos de Servicios de IoT del mismo fabricante de la solución de control de acceso a la red ofertada
11.28	Debe permitir determinar el perfil de los dispositivos descubiertos mediante sesiones de firewall del mismo fabricante de la solución de control de acceso a la red ofertada

11.29	Debe permitir la integración con las siguientes plataformas de MDM: - Air Watch - Google GSuite - MaaS360 - Mobile Iron - XenMobile - Fortinet EMS - Nozomi - JAMF
11.3	La solución debe poder reconocer los siguientes sistemas operativos sin necesidad de agentes: - Android - Apple iOS for iPhone/iPad7/iPod - Blackberry OS/Blackberry 10 OS - Chrome OS - Free BSD - Kindle/Kindle Fire - Linux - Mac OS X - Open BSD - Solaris - Symbian - Web OS - Windows - Windows Phone/CE/RT
11.31	Debe permitir el uso de Agentes Persistentes para el perfilamiento de hosts
11.32	Debe permitir la identificación de usuarios mediante Active Directory
11.33	Debe permitir la identificación de usuarios mediante Portal Cautivo
11.34	La solución debe incluir opciones de análisis flexibles para plataformas Windows, MacOS y Linux. La tecnología de agentes efímeros no debe requerir la instalación de software de terceros, tales como Java.
11.35	Debe permitir la designación de un Sponsor que autorice el acceso de un invitado.
11.36	Debe permitir la designación de un Sponsor que autorice la categorización de un host.
11.37	Debe permitir el ingreso de credenciales mediante 802.1x o Portal Cautivo.
11.38	Debe soportar la validación de credenciales: - Con Google Account - Con un servidor RADIUS externo - Con un servidor LDAP
11.39	Debe soportar como postura de seguridad la restricción de conexiones inalámbricas a SSIDs específicos
11.40	Debe soportar como postura de seguridad la detección de Multihoming

11.41	Debe permitir la autenticación de usuarios mediante las siguientes redes sociales Facebook, Google, linkedIn, outlook, twitter y yahoo
11.42	Debe actuar como servidor de radius local embebido dentro de la misma solución de control de acceso a la red
11.43	Debe permitir modo de autenticación de Radius Local con los siguientes modos de EAP 802.1X: - TTLS/PAP - TTLS/MSCHAPv2 - PEAP/MSCHAPv2 - TLS
11.44	Debe soportar la validación automática de credenciales mediante agentes persistentes o volátiles
11.45	La solución debe tener la capacidad de aprovechar la combinación de informaciones sobre la identidad del usuario y el tipo de dispositivo para aprovisionar dinámicamente permisos de acceso basados en roles y distintos niveles de acceso.
11.46	Debe permitir la generación de políticas de control, agrupadas jerárquicamente, y determinar la política a aplicar a cada dispositivo en función de una serie de reglas de asignación.
11.47	Debe soportar, al menos, los siguientes tipos de información para determinar la política a aplicar: - Ubicación - Grupo de Pertenencia - Atributo - Fecha y Hora
11.48	La solución debe incluir funcionalidades de Guest Management, permitiendo la creación de perfiles de Invitados y Contratistas.
11.49	Debe permitir la creación de plantillas que agrupen a los invitados o contratistas en grupos que tengan distintos permisos de acceso, o períodos de tiempo de acceso permitido.
11.5	Debe contar con herramientas que permitan la generación y mantenimiento de este tipo de usuarios y sus claves de acceso.
11.51	Debe permitir la creación de Portales de Auto-Registro.
11.52	Debe soportar el envío de claves de acceso y mensajes personalizables mediante SMS y correo electrónico
11.53	Debe permitir la existencia de Sponsors que aprueben el ingreso de Invitados o Contratistas a la red, o que eleven los permisos de acceso de ciertos individuos.
11.54	La solución debe incluir funcionalidades de IoT Onboarding con autorización de Sponsors

11.55	La solución debe incluir funcionalidades de detección y contención de dispositivos desconocidos (rogues)
11.56	La solución debe incluir funcionalidades de Endpoint Compliance. Antes de permitir el acceso de los dispositivos a la red, debe asegurarse de que estos cumplen con una serie de requisitos de seguridad, integridad y configuración, que hagan seguro su acceso a la red.
11.57	Debe permitir el uso de agentes persistentes, evanescentes (desaparecen luego de realizado en análisis) o pasivos.
11.58	Debe permitir el control de acceso a la red basado en políticas de acceso que determinen el tipo de segmentación de red para los dispositivos y usuarios registrados. Estas políticas deben asignar un tag de firewall que será recibido automáticamente por el firewall del mismo fabricante de la solución ofertada.
11.59	Si un dispositivo no pasa los tests de Compliance, debe ser posible: - No forzar la remediación - Forzar la remediación inmediatamente, enviando al dispositivo a una red de cuarentena - Permitir la remediación retardada, dando un período de tiempo desde la detección inicial de problemas, para la solución de estos. Pasado el período de tolerancia, de persistir los problemas, el dispositivo debe ser puesto en cuarentena inmediatamente.
11.6	Debe permitir el control de acceso a la red de los usuarios remotos autenticados a través de VPN IPSec y/o SSL utilizando como terminador VPN el mismo fabricante de la solución de control de acceso a la red ofertada
11.61	Debe permitir determinar la postura de Seguridad de los usuarios conectados remotamente a través de VPN IPSec y/o SSL utilizando agente disolvente descargado a través de un portal para las redes de contratistas y agente persistente para la red corporativa
11.62	Debe permitir la construcción de reglas de seguridad que se activen ante eventos de seguridad definidos por el administrador, para generar alarmas de seguridad.
11.63	Ante una alarma de seguridad debe permitir el bloqueo o aislamiento automático de los hosts comprometidos
11.64	Debe permitir homogeneizar los niveles de severidad de los mensajes de syslog de múltiples dispositivos externos
11.65	Debe permitir la creación, modificación y borrado de acciones que puedan ser asociadas a una alarma.

11.66	Las acciones por ejecutar deben incluir, al menos: - Ejecución de un script de comandos - Enviar una alarma a un log externo - Enviar un mensaje de correo electrónico al usuario o a los administradores - Enviar un SMS - Cambiar el rol del host involucrado - Deshabilitar el host - deshabilitar el puerto de conexión - Revalidar el estado de compliance del host - marcar el host como En Riesgo - Marcar el host como Seguro
11.67	La solución debe poder interoperar con dispositivos de conexión cableada e inalámbrica de los principales fabricantes, incluyendo, como mínimo: - Adtran NetVanta - Alcatel-Lucent - Allied Telesis - Arista Networks - Cisco/Meraki - Dell - D-Link - Extreme Networks/Enterasys/Motorola/Avaya/Foundry Networks - Fortinet/Meru - HPE/HP Procurve/3Com/H3C/Aruba - Hirschmann - Huawei - Juniper - Linksys - Mist - Riverbed/Xirrus - Ruckus/Brocade - Ubiquity Unifi

11.68	La solución debe permitir la integración de dispositivos de infraestructura de seguridad de terceras partes, incluyendo: - CheckPoint - Cyphort - Cisco/SourceFire - FireEye - Fortinet - Juniper/Netscreen - Palo Alto - Qualys - SonicWall - Sophos - Tenable - AirWatch - MobileIron - MaaS360 - Citrix XenMobile - Adtran/BlueSocket.
11.69	La solución debe permitir la integración de Servicios de Directorios y Sistemas Operativos, incluyendo: - RADIUS: Microsoft IAS, Cisco ACS, FreeRADIUS - LDAP: Microsoft Active Directory, OpenLDAP, Google SSOCheckPoint - Microsoft Windows - Apple Mac OS X e IOS - Linux - Android
11.70	La solución debe permitir la integración de Aplicaciones de Seguridad de Endpoints, incluyendo: - Avast/AVG - Avira - Blink - ESET - Kaspersky - Lavasoft - McAffee - Microsoft - Norton - Panda - PC Tools - Sophos - Symantec - Trend Micro - Zone Alarm
11.71	La solución debe contar con un método genérico de integración de dispositivos, mediante la recepción, análisis e interpretación de mensajes de Syslog.

11.72	La solución debe incluir una REST API que permita: - Obtener información detallada sobre un elemento en particular, tal como un usuario o un host. - Interrogar a la base de datos para obtener información sobre un conjunto de dispositivos - Actualizar los registros de usuarios o dispositivos - Bloquear o desbloquear el acceso de un usuario o dispositivo a la red.
11.73	La solución debe integrarse con la plataforma actual de seguridad perimetral que tiene la institución permitiendo alcanzar un control de acceso granular y respuesta automatizada ante cualquier evento de seguridad presentado utilizando TAGs de firewall y conectores.
11.74	La información enviada por la solución de control de acceso a la red a la plataforma de seguridad perimetral que tiene la institución debe contener IP, usuario, Grupo o TAGs personalizados que permiten ser asignados de manera automática a grupos de usuarios de firewall utilizados en políticas de IPV4 para aplicar segmentación de acceso a la red
11.75	Control de usuarios conectados por VPN, con el fin de validar su postura antes que éstos ingresen a los recursos de Red. Esta funcionalidad debe estar integrada como mínimo a plataformas Fortigate y Cisco.
11.76	La solución debe permitir distintos roles administrativos, incluyendo la capacidad de limitar y controlar la cantidad de acceso permitido a las funcionalidades disponibles, dependiendo del grupo administrativo de la organización al que pertenezca el usuario. Por ej., Help Desk, Operaciones de Red, Operaciones de Seguridad.
11.77	La solución debe proveer información de auditoría de todas las conexiones de la red, tanto cableadas como inalámbricas. Esto debe incluir una interfaz amigable, que permita buscar y generar consultas en la información almacenada.
11.78	La solución debe incluir información de auditoría de todas las acciones y cambios realizados al sistema por los usuarios administradores, incluyendo qué se cambió, cuándo se cambió y quién lo cambió.
11.79	Debe contar con un Tablero de Control que presente información relevante de manera resumida.
11.80	El Tablero de Control debe poder ser modificable para permitir el despliegue de la información que el Administrador considere más relevante.
11.81	Debe contar con reportes predefinidos que incluyan resultados sobre: - Registro de Invitados - Registro de dispositivos - Escaneo de Dispositivos
11.82	Debe permitir la generación de reportes a medida sobre: - Registro de usuarios y Dispositivos - Falla en los Registros - Logs de Conexión

11.83	Debe permitir la generación y archivado de reportes periódicos
11.84	Debe permitir el envío automatizado de reportes mediante correo electrónico
11.85	El log de alarmas debe poder ser ordenado por severidad.
11.86	Debe permitir la aceptación y eliminación de alarmas del log de forma manual.
11.87	Debe permitir la aceptación y eliminación de alarmas del log de forma automática.
11.88	Debe permitir la definición de alarmas en función de la ocurrencia de determinados eventos.
11.89	El proponente debe garantizar que cuenta como mínimo 6 días de servicios profesionales de fábrica, para los servicios de implementación
11.90	El fabricante debe entregar el soporte directo sobre la plataforma en español

Ítem 12. Instalación y Configuración

Numeral	Especificaciones técnicas
12.1	Cantidad: 1
12.2	Con la adquisición se deben incluir todos los conectores, cables y licenciamiento necesario de toda la solución.
12.3	La solución debe incluir todo el licenciamiento necesario para sacar beneficio de todos las funcionalidades requeridas.
12.4	Su solución debe incluir soporte y mantenimiento para Hardware y Software por 3 años (24/7 por 365 días) que incluya el soporte (reemplazo de partes) y actualización de versiones sin costo adicional.
12.5	El proveedor entregará lo siguiente:
12.6	• Plan de trabajo y documentación del diseño propuesto.
12.7	• Solución debidamente instalada e integrada con toda la infraestructura de hardware y software, bajo las mejores prácticas recomendadas por el proveedor.
12.8	• Documentación de la instalación (configuraciones realizadas, etc.) y diagramas de Red.
12.9	• Manuales de usuarios y técnicos.
12.10	• Planes de mantenimiento a la solución.
12.11	Los técnicos a implementar la solución deben de poseer conocimiento y experiencia comprobada en la integración de soluciones como la propuesta en esta licitación.
12.12	Cualquier material, licencia o equipo adicional que sea necesario para la instalación y operación de la solución “no especificado” o “no descrito”, será considerado como parte de la propuesta.
12.13	No se requiere cableado estructurado, grúas o andamios. De ser necesario será algo adicional a lo requerido en este pliego será tomado como un control de cambio.
12.14	Todo equipo, accesorio, entrenamiento, software, hardware, trabajo y materiales que se deban considerar para la instalación de la plataforma tecnológica ofertada, debe de estar especificado en la propuesta.
12.15	El proveedor debe poseer su propia infraestructura de servicios locales con las debidas certificaciones técnicas y comerciales, y garantizar que el soporte y la implementación se preste con personal técnico certificado y con experiencia en este tipo de soluciones.

12.16	El integrador debe proporcionar un project plan detallado con las tareas a ejecutar. Debe tener un project manager asignado con la capacidad de dirigir el proyecto y culminarlo en los tiempos establecidos.
12.17	La solución debe de ser instalada y configurada por el personal técnico especializado en la solución.
12.18	El integrador realizará las instalaciones físicas de los equipos de red.
12.19	Los equipos propuestos no deben poseer un tiempo de salida de mercado de mínimo 5 años, significa que no deberá llegar el fin de soporte en los próximos 5 años.
12.20	El soporte del fabricante debe incluir reemplazo de partes y de equipos local en la República Dominicana.
12.21	El proveedor debe contar con la certificación de Partner Expert, y contar con las especializaciones de Firewall de red y Borde de Servicio de Acceso Seguro (SASE).
12.22	El oferente debe incluir el entrenamiento oficial para tres personas e incluir los vouchers de exámenes para todas las soluciones.