COPIA CONTROLADA 17

DENOMINACIÓN DEL BIEN O SERVICIO

Switch CORE.

CÓDIGO IDENTIFICACIÓN BIEN O SERVICIO

CLASIFICACION UNSPSC	TIPO DE BIEN O SERVICIO
43222600	Equipo de servicio de red.

DENOMINACIÓN TÉCNICA DEL BIEN O SERVICIO

Switch DataCenter CORE 24 Puertos (5 años soporte técnico y garantía)

UNIDAD DE MEDIDA

Unidad

DESCRIPCIÓN GENERAL

Característica	Requerimiento Mínimo
Características Generales	
La marca propuesta deberá estar presente por al menos 4 años consecutivos como líder o visionarios en el cuadrante mágico de gartner para redes cableadas e inalámbricas.	
Switch con desempeño mínimo de: • Para 24 puertos SFP+ de 100Mb - 1Gb - 10Gb y mínimo 2 puertos de apilamiento QSFP28: 100 Gbps de conmutación: 1070 Gbps de conmutación	
Tasa de transmisión de paquetes de al menos: • Para 24 puertos SFP+ de 100Mb - 1Gb - 10Gb y mínimo 2 puertos de apilamiento QSFP28: 100 Gbps de conmutación: 800 Mbps	
Debe permitir realizar el stack de al menos 8 unidades. El stack deberá ser de al menos 160 Gbps entre unidades.	
El equipo debe contar con al menos la siguiente densidad de puertos: • >= 24 puertos 100M/1G/10GBASE-X (SFP+) • >= 2 puertos Stacking/Uplink QSFP28 • Slot disponible para crecimiento de interfaces 1/10/25Gbps • >= 1 puerto serial para consola • >= 1 puerto 10/100/1000 BASE-T para Administración Fuera de Banda • >= 2 puerto USB para gestión de consola	
El equipo deberá soportar el siguiente tipo de interfaces de fibra: • Gigabit Ethernet: SX, LX, ZX, BX-D, BX-U, 100FX/1000LX, 10/100/1000BASE-T en formato SFP. • 10 Gigabit Ethernet: SR, LR, ER, LRM CR en formato SFP+	
A futuro el equipo debe soportar el manejo de uplinks de 25G. Se debe indicar cómo es posible.	
En caso de ser necesario se debe poder habilitar a futuro la funcionalidad de MACSec tanto para los puertos de acceso como para los puertos de uplink para garantizar cifrado de las comunicaciones. El cifrado deberá ser de al menos 256 bits.	
El equipo debe poder ser gestionado desde un sistema "on premises" instalado en el DC de la entidad o desde un sistema de gestión en nube (opción dentro de esta propuesta).	
El equipo deberá gestionarse desde el mismo sistema que la solución inalámbrica.	
El equipo debe incluir al menos 2 cables de poder.	

Debe incluir los accesorios necesarios para instalar y configurar stack de 2 switch a mínimo 40G.
El equipo debe contar con un sistema de ventilación con al menos 2 ventiladores.
El equipo debe soportar fuentes redundantes. En este momento se debe incluir 2.
El equipo deberá estar diseñado para una unidad de rack (1 RU)
El equipo deberá operar en rangos de temperatura de al menos 0 a 30 grados centígrados.
Soportar al menos >= 110K MAC Address
Soportar al menos >= 4000 VLANs
Soporte de Jumbo Frames >= 9216 Bytes
Soportar al menos 16 ACLs de ingreso y 4 de egreso
Soportar al menos 74000 entradas ARP
Soportar al menos 80000 rutas IPv4
Soportar al menos 17000 rutas IPv6
Soporte de al menos 3200 Servicios extendidos en capa 2 y 253 en capa 3
Características de Software
El equipo deberá contar al menos las siguientes funcionalidades y especificaciones:
Debe soportar mecanismos de ZTP (Zero Touch Provisioning)
IEEE 802.1D STP
IEEE 802.1w RSTP
IEEE 802.1s MSTP
PVST+, Per VLAN STP
VXLAN >= 2048
Scripts en Python
Políticas de Seguridad basadas en Usuarios
Debe contar con la habilidad para autenticar múltiples usuarios en un mismo puerto sea vía 802.1x, Web auth o MAC auth al mismo tiempo
Debe contar con un mecanismo de DDoS para garantizar la seguridad. Describir como lo hace.
Solución de SDLAN Habilitada y operativa. Indicar cuál.
Soporte de IEEE 802.3ad, Configuración de compartición de carga estática y configuración dinámica basada en LACP
Puertos de software redundantes
Soporte de Multi-Switch Link Aggregation Groups (M-LAG) o similar
Soporte de IEEE 802.1AB – LLDP Link Layer Discovery Protocol
Soporte de LLDP-MED
Soporte de un protocolo capas de recaudar información acerca de los nodos vecinos para el intercambio de la topología de la red entre los switches.
Soporte de un protocolo que controle paquetes originados localmente para prevención de ciclos.
Soporte de IEEE 802.1ag Connectivity Fault Management
IEEE 802.1 Audio Video Bridging (AVB), para garantizar el correcto manejo de audio y video dentro de toda la infraestructura.
SNTP para IPv4 e IPv6
NTP para IPv4 e IPv6
IGMP v3 Snooping
Modo de autoconfiguración de puertos para VoIP
Telnet
TFTP
BootP para IPv4 e IPv6
DHCP v4 Server y Cliente
DHCP v6 Relay y Cliente
Agregación de VLANs
Detección de Direcciones Duplicadas en IPv4 e IPv6
PBR para IPv4 (Enrutamiento basado en políticas)
PBR para IPv6 (Enrutamiento basado en políticas)

IPFIX
Rip v1/v2
RIPng
Rutas estáticas
OSPFv2 y v3 aplicable al acceso
VRRP
BGP
Vxlan
Listas de Control de Acceso
Deshabilitar aprendizaje de ARP
VRFs
Características de Sistema Operativo
Capacidad de correr distintos tipos de sistemas operativos (al menos 2) dentro del mismo hardware desarrollados por el fabricante, que permita utilizar el mismo hardware en distintos escenarios aprovechando las funcionalidades propias que puedan contar los SO para ambientes como pueden ser campus o DC.
GARANTÍA COMERCIAL O PRESUNTA
5 Años

DENOMINACIÓN DEL BIEN O SERVICIO	
Switch MultiGigabit.	
CÓDIGO IDENTIFICACIÓN BIEN O SERVICIO	
CLASIFICACION UNSPSC	TIPO DE BIEN O SERVICIO
43221700	Equipo de servicio de red.
DENOMINACIÓN TÉCNICA DEL BIEN O SERVICIO	
Switch multiGigabit 48 Puertos (5 años soporte técnico y garantía)	
UNIDAD DE MEDIDA	
Unidad	
DESCRIPCIÓN GENERAL	
Característica	Requerimiento Mínimo
Características Generales	
La marca propuesta deberá estar presente por al menos 4 años consecutivos como líder o visionarios en el cuadrante mágico de gartner para redes cableadas e inalámbricas.	
Switch con desempeño mínimo de: • Para 48 puertos de Cobre con 16 de estos multigigabit: 300 Gbps de conmutación	
Tasa de transmisión de paquetes de al menos: • Para 48 puertos de Cobre con 16 de estos multigigabit: 220 Mbps	
Debe permitir realizar el stack de al menos 8 unidades. El stack deberá ser de al menos 40 Gbps entre unidades.	
El equipo debe contar con al menos la siguiente densidad de puertos: • >= 48 puertos 10/100/1000 BASE-T PoE-Plus y 802.3at (30W) de los que al menos 16 deberán ser 100M/1/2.5G 802.3bt (90W) PoE ports • >= 4 puertos 10GBASE-X SFP+	

• >= 2 Puertos Stack/Uplink • >= 1 puerto serial para consola • >= 1 puerto 10/100/1000 BASE-T para Administración Fuera de Banda • >= 1 puerto USB para gestión de consola
El equipo deberá soportar el siguiente tipo de interfaces de fibra: • Gigabit Ethernet: SX, LX, 1000BASE-T en formato SFP • 10 Gigabit Ethernet: SR, LR, ER en formato SFP+
Debe incluir 5 Modulo Multimodo 10 Gigabit Ethernet SFP+, 850nm.
Debe incluir 5 conectores de fibra LC multimodo OM4
El equipo deberá tener un PoE Budget (disponibilidad de energía para PoE) de al menos: • Modelos multigigabit: 950W (una fuente de poder) / 1860W (dos fuentes de poder).
Debe soportar PoE perpetuo que permite que la alimentación vía PoE se mantenga incluso durante el reinicio del switch, evitando el reinicio de los equipos que son alimentados desde el switch.
Debe soportar fast PoE que permite la entrega de PoE a los dispositivos antes de que termine el switch el proceso de arranque.
El equipo debe contar con un sistema de ventilación con al menos 1 ventilador.
El equipo debe soportar fuentes redundantes. En este momento se debe incluir 1.
Debe incluir cables de poder.
Debe incluir los accesorios necesarios para instalar y cfgurar stack de más de 3 switch redundante.
El equipo deberá estar diseñado para una unidad de rack (1 RU)
El equipo deberá operar en rangos de temperatura de al menos 0 a 30 grados centígrados.
Soportar al menos >= 32K MAC Address
Soportar al menos >= 4092 VLANs
Soporte de Jumbo Frames >= 9216 Bytes
Soportar al menos 16 ACLs de ingreso y 4 de egreso
Soportar al menos 15.900 entradas ARP
Soportar al menos 11.900 rutas IPv4
Soportar al menos 5.900 rutas IPv6
Soporte de al menos 500 Servicios extendidos en capa 2 y 60 en capa 3
Características de Software
El equipo deberá contar al menos las siguientes funcionalidades y especificaciones:
Debe soportar mecanismos de ZTP (Zero Touch Provisioning)
IEEE 802.1D STP
IEEE 802.1w RSTP
IEEE 802.1s MSTP
PVST+, Per VLAN STP
Scripts en Python
Políticas de Seguridad basadas en Usuarios
Debe contar con la habilidad para autenticar múltiples usuarios en un mismo puerto sea vía 802.1x, Web auth o MAC auth al mismo tiempo
Debe contar con un mecanismo de DDoS para garantizar la seguridad. Describir como lo hace.
Soporte de Tecnologías de SDLAN. Indicar cuál.
Soporte de IEEE 802.3ad, Configuración de compartición de carga estática y configuración dinámica basada en LACP
Puertos de software redundantes
Soporte de Multi-Switch Link Aggregation Groups (M-LAG) o similar
Soporte de IEEE 802.1AB – LLDP Link Layer Discovery Protocol
Soporte de LLDP-MED
Soporte de un protocolo capas de recaudar información acerca de los nodos vecinos para el intercambio de la topología de la red entre los switches.
Soporte de un protocolo que controle paquetes originados localmente para prevención de ciclos.
Soporte de IEEE 802.1ag Connectivity Fault Management

IEEE 802.1 Audio Video Bridging (AVB), para garantizar el correcto manejo de audio y video dentro de toda la infraestructura.
SNTP para Ipv4 e Ipv6
NTP para IPv4 e IPv6
IGMP v3 Snooping
Modo de autoconfiguración de puertos para VoIP
Telnet
TFTP
BootP para Ipv4 e Ipv6
DHCP v4 Server y Cliente
DHCP v6 Relay y Cliente
Agregación de VLANs
Detección de Direcciones Duplicadas en Ipv4 e Ipv6
PBR para Ipv4 (Enrutamiento basado en políticas)
PBR para Ipv6 (Enrutamiento basado en políticas)
IPFIX
Rip v1/v2
RIPng
Rutas estáticas
OSPFv2 y v3 aplicable al acceso
VRRP
BGP
Vxlan >=370
Listas de Control de Acceso
Deshabilitar aprendizaje de ARP
VRFs
Características de Sistema Operativo
Capacidad de correr distintos tipos de sistemas operativos (al menos 2) dentro del mismo hardware desarrollados por el fabricante, que permita utilizar el mismo hardware en distintos escenarios aprovechando las funcionalidades propias que puedan contar los SO para ambientes como pueden ser campus o DC.
La selección del sistema operativo podrá realizarse desde el sistema de gestión.
GARANTÍA COMERCIAL O PRESUNTA
5 Años

DENOMINACIÓN DEL BIEN O SERVICIO	
Switch Acceso PoE.	
CÓDIGO IDENTIFICACIÓN BIEN O SERVICIO	
CLASIFICACION UNSPSC	TIPO DE BIEN O SERVICIO
43221700	Equipo de servicio de red.
DENOMINACIÓN TÉCNICA DEL BIEN O SERVICIO	
Switch Acceso PoE 48 Puertos (5 años soporte técnico y garantía)	
UNIDAD DE MEDIDA	
Unidad	
DESCRIPCIÓN GENERAL	

Característica	Requerimiento Mínimo
Características Generales	
La marca propuesta deberá estar presente por al menos 4 años consecutivos como líder o visionarios en el cuadrante mágico de gartner para redes cableadas e inalámbricas.	
Switch con desempeño mínimo de: • Para 48 puertos de Cobre: 256 Gbps de conmutación	
Tasa de transmisión de paquetes de al menos: • Para 48 puertos de Cobre: 190 Mbps	
Debe permitir realizar el stack de al menos 8 unidades. El stack deberá ser de al menos 40 Gbps entre unidades.	
El equipo debe contar con al menos la siguiente densidad de puertos: • >= 48 puertos 10/100/1000 BASE-T PoE-Plus y 802.3at (30W) • >= 4 puertos 10GBASE-X SFP+ • >= 2 Puertos Stack/Uplink • >= 1 puerto serial para consola • >= 1 puerto 10/100/1000 BASE-T para Administración Fuera de Banda • >= 2 puerto USB para gestión de consola	
El equipo deberá soportar el siguiente tipo de interfaces de fibra: • Gigabit Ethernet: SX, LX, 1000BASE-T en formato SFP. • 10 Gigabit Ethernet: SR, LR, ER en formato SFP+.	
El equipo deberá tener un PoE Budget (disponibilidad de energía para PoE) de al menos: • Modelos de 48 puertos: 740 (una fuente de poder) / 1480W (dos fuentes de poder).	
Cables de apilamiento: 20G Passive DAC SFPDD 1m y los cables DAC: 20G Passive DAC SFPDD 3m necesarios para completar los Stack en cada centro de cableado	
Debe soportar PoE perpetuo que permite que la alimentación vía PoE se mantenga incluso durante el reinicio del switch, evitando el reinicio de los equipos que son alimentados desde el switch.	
Debe soportar fast PoE que permite la entrega de PoE a los dispositivos antes de que termine el switch el proceso de arranque.	
El equipo debe contar con un sistema de ventilación con al menos 1 ventilador.	
El equipo debe soportar fuentes redundantes. En este momento se debe incluir 1.	
Debe incluir cables de poder.	
Debe incluir los accesorios necesarios para instalar y cfgurar stack de mas de 3 switch redundante.	
El equipo deberá estar diseñado para una unidad de rack (1 RU)	
El equipo deberá operar en rangos de temperatura de al menos 0 a 30 grados centígrados.	
Soportar al menos >= 32K MAC Address	
Soportar al menos >= 4092 VLANs	
Soporte de Jumbo Frames >= 9216 Bytes	
Soportar al menos 16 ACLs de ingreso y 4 de egreso	
Soportar al menos 15.900 entradas ARP	
Soportar al menos 11.900 rutas IPv4	
Soportar al menos 5.900 rutas IPv6	
Soporte de al menos 500 Servicios extendidos en capa 2 y 60 en capa 3	
Características de Software	
El equipo deberá contar al menos las siguientes funcionalidades y especificaciones:	
Debe soportar mecanismos de ZTP (Zero Touch Provisioning)	
IEEE 802.1D STP	
IEEE 802.1w RSTP	
IEEE 802.1s MSTP	
PVST+, Per VLAN STP	
Scripts en Python	
Políticas de Seguridad basadas en Usuarios	

Debe contar con la habilidad para autenticar múltiples usuarios en un mismo puerto sea vía 802.1x, Web auth o MAC auth al mismo tiempo
Debe contar con un mecanismo de DDoS para garantizar la seguridad. Describir como lo hace.
Soporte de Tecnologías de SDLAN. Indicar cual.
Soporte de IEEE 802.3ad, Configuración de compartición de carga estática y configuración dinámica basada en LACP
Puertos de software redundantes
Soporte de Multi-Switch Link Aggregation Groups (M-LAG) o similar
Soporte de IEEE 802.1AB – LLDP Link Layer Discovery Protocol
Soporte de LLDP-MED
Soporte de un protocolo capas de recaudar información acerca de los nodos vecinos para el intercambio de la topología de la red entre los switches.
Soporte de un protocolo que controle paquetes originados localmente para prevención de ciclos.
Soporte de IEEE 802.1ag Connectivity Fault Management
IEEE 802.1 Audio Video Bridging (AVB), para garantizar el correcto manejo de audio y video dentro de toda la infraestructura.
SNTP para Ipv4 e Ipv6
NTP para IPv4 e IPv6
IGMP v3 Snooping
Modo de autoconfiguración de puertos para VoIP
Telnet
TFTP
BootP para Ipv4 e Ipv6
DHCP v4 Server y Cliente
DHCP v6 Relay y Cliente
Agregación de VLANs
Detección de Direcciones Duplicadas en Ipv4 e Ipv6
PBR para Ipv4 (Enrutamiento basado en políticas)
PBR para Ipv6 (Enrutamiento basado en políticas)
IPFIX
Rip v1/v2
RIPng
Rutas estáticas
OSPFv2 y v3 aplicable al acceso
VRRP
BGP
Vxlan >=370
Listas de Control de Acceso
Deshabilitar aprendizaje de ARP
VRFs
Características de Sistema Operativo
Capacidad de correr distintos tipos de sistemas operativos (al menos 2) dentro del mismo hardware desarrollados por el fabricante, que permita utilizar el mismo hardware en distintos escenarios aprovechando las funcionalidades propias que puedan contar los SO para ambientes como pueden ser campus o DC.
La selección del sistema operativo podrá realizarse desde el sistema de gestión.
GARANTÍA COMERCIAL O PRESUNTA
5 Años

DENOMINACIÓN DEL BIEN O SERVICIO
Access Point Tipo 1.

CÓDIGO IDENTIFICACIÓN BIEN O SERVICIO	
CLASIFICACION UNSPSC	TIPO DE BIEN O SERVICIO
43221700	Equipo de Servicio de red.

DENOMINACIÓN TÉCNICA DEL BIEN O SERVICIO

Access Point Tipo 1 (5 años soporte técnico de Fabrica y garantía).

UNIDAD DE MEDIDA

Unidad

DESCRIPCIÓN GENERAL

CARACTERÍSTICA	REQUERIMIENTO TÉCNICO MÍNIMO
Generalidades	• La marca propuesta deberá estar presente por al menos 4 años consecutivos como líder o visionarios en el cuadrante mágico de gartner para redes cableadas e inalámbricas. • La solución debe soportar 802.11ax • La solución debe soportar WPA3 Wi-Fi • La solución debe soportar procesos de visibilidad mediante procesos de ML/AI (Machine learning and artificial intelligence) • Debe soportar ser administrado desde la nube (opción a incluir) • Debe permitir administrarse en caso de ser necesario desde una implementación on-premises. • Debe permitir generación de contraseñas dinámicas a usuarios invitados y enviarlas por email o mensaje de texto o un medio similar • Toda la solución ofertada debe ser monomarca (con la controladora/sistema de gestión) incluyendo los accesorios de conectividad • Cada Access Point debe soportar al menos 510 clientes asociados por equipo. • Cada Access Point debe permitir al menos 8 SSID por radio. • Debe contar con un radio dedicado exclusivamente al monitoreo del espectro inalámbrico sin utilizar los mismos radios que se utilizan para transmisión de datos garantizando máximo desempeño, sin interrumpir las transmisiones • De tipo Indoor.
Especificación de Radios	• La solución debe soportar como mínimo los radios de frecuencia de: • SSID per Radio/Total: 16/48 • Users per Radio/total: 512/1536 802.11n • 2.4–2.5 GHz and 5.150–5.850 GHz Operating Frequency • 802.11n Modulation • HT 20 High-Throughput (HT) Support (for both 2.4 GHz and 5 GHz) • HT 40 High-Throughput (HT) Support for 5 GHz • A-MPDU and A-MSDU Frame Aggregation

	802.11ac • 5.150–5.850 GHz Operating Frequency • 802.11ac Modulation (256-QAM) • Rates (Mbps): MCS0 – MCS31 (6.5MBps - 600Mbps) • 5G: 2x2 Multiple-In, Multiple-Out (MIMO) Radio • 2.4G: 2x2 Multiple-In, Multiple-Out (MIMO) Radio • Rates (Mbps): MCS0–MCS9 (6.5Mbps), 1734Mbps, NSS = 1-2. • 2x2:2 Stream Multiple-In, Multiple-Out (MIMO) Radio • VHT20/VHT40/VHT80 support • TxBF (Transmit Beamforming) 802.11ax • 2.4-2.5GHz, 5.15-5.850 GHz and 5.925-7.125 GHz Operating Frequencies • 802.11ax Modulation (1024-QAM) • Dual-band OFDMA • 6G Rate: HE0-HE11 (8 Mbps – 2400 Mbps) • 5G Rate : HE0-HE11 (8 Mbps – 1200 Mbps) • 2.4G Rate: HE0-HE11 (8Mbps – 574 Mbps) • 2x2:2 Stream Multiple-In, Multiple-Out (MIMO) Radio @ 6 GHz Deberá contar con un radio Bluetooth BLE • Bluetooth® 5.2 Low Energy, IEEE 802.15.4
Interfaces	La solución debe contar con mínimo: • Eth0, Eth1: (2) Wired Ethernet ports (RJ-45) • 100/1000/2500Mbps auto-sensing link speed Ethernet port, POE 802.3at • 10/100/1000 Mbps auto-sensing link speed Ethernet port • 802.3az Energy Efficient Ethernet (EEE) • USB 2.0, Type A, 5V/500mA
Especificaciones de corriente	Debe ser compatible con el estándar IEEE 802.3at para Power over Ethernet Funcionalidad total con 802.3at
Antenas	La solución debe contar como mínimo con las siguientes antenas: • (2) Integrated single band, 5.925-7.125 GHz omnidirectional antennas • (2) Integrated dual band, 2.4-2.5 GHz, and 5.1-5.8 GHz omnidirectional • (2) Integrated dual band, 2.4-2.5 GHz, and 5.1-5.8 GHz omnidirectional for sensor • (1) Integrated dual band, 2.4-2.5 GHz omnidirectional for IoT
Ganancia	• En 2.4 GHz >= 3.9 dBi • En 5 GHz >= 5.1 dBi • En 6 GHz >= 5.3 dBi • BLE >= 5.3 dBi
Cumplimiento de normativa	Los equipos ofertados deben cumplir por lo menos con una norma de cuidado del medio ambiente y/o manejo eficiente de energía, para lo cual el proponente debe adjuntar la ficha técnica del fabricante donde se pueda corroborar el cumplimiento de este requerimiento.
	• Cumplimiento de WiFi Alliance • WPA3 security

	• WMM • WMM-Power Save • Wi-Fi CERTIFIED 6™ • Wi-Fi Agile Multiband
Temperatura de Operación	Al menos en los rangos de 0 a 40*C

GARANTÍA COMERCIAL O PRESUNTA
5 Años

DENOMINACIÓN DEL BIEN O SERVICIO
Access Point Tipo 2.

CÓDIGO IDENTIFICACIÓN BIEN O SERVICIO	
CLASIFICACION UNSPSC	TIPO DE BIEN O SERVICIO
43221700	Equipo de Servicio de red.

DENOMINACIÓN TÉCNICA DEL BIEN O SERVICIO
Access Point Tipo 2 (5 años soporte técnico de Fábrica y garantía).

UNIDAD DE MEDIDA
Unidad

DESCRIPCIÓN GENERAL

CARACTERÍSTICA	REQUERIMIENTO TÉCNICO MÍNIMO
Generalidades	• La marca propuesta deberá estar presente por al menos 4 años consecutivos como líder o visionarios en el cuadrante mágico de gartner para redes cableadas e inalámbricas. • La solución debe soportar 802.11ax • La solución debe soportar WPA3 Wi-Fi • La solución debe soportar procesos de visibilidad mediante procesos de ML/AI (Machine learning and artificial intelligence). • Debe soportar ser administrado desde la nube (opción a incluir) • Debe permitir administrarse en caso de ser necesario desde una implementación on-premises. • Debe permitir generación de contraseñas dinámicas a usuarios invitados y enviarlas por email o mensaje de texto o un medio similar • Toda la solución ofertada debe ser monomarca (con la controladora/sistema de gestión) incluyendo los accesorios de conectividad. • Cada Access Point debe soportar al menos 510 clientes asociados por equipo. • Cada Access Point debe permitir al menos 8 SSID por radio. • Debe contar con un radio dedicado exclusivamente al monitoreo del espectro inalámbrico sin utilizar los mismos radios que se utilizan para transmisión de datos garantizando máximo desempeño, sin interrumpir las transmisiones. • De tipo Indoor.

Especificación de Radios	• La solución debe soportar como mínimo los radios de frecuencia de: SSID per Radio/Total: 16/32 • Users per Radio/total: 512/1024 802.11n • 2.4–2.5 GHz and 5.150–5.850 GHz Operating Frequency • 802.11n Modulation • HT 20 High-Throughput (HT) Support (for both 2.4 GHz and 5 GHz) • HT 40 High-Throughput (HT) Support for 5 GHz • A-MPDU and A-MSDU Frame Aggregation • Rates (Mbps): MCS0 – MCS15 (6.5MBps - 300Mbps) 802.11ac • 5.150–5.850 GHz Operating Frequency • 802.11ac Modulation (256-QAM) • 5G: 2x2 Multiple-In, Multiple-Out (MIMO) Radio • 2.4G: 2x2 Multiple-In, Multiple-Out (MIMO) Radio • Rates (Mbps): MCS0–MCS9 (6.5Mbps), 1734Mbps, NSS = 1-2. • 2x2:2 Stream Multiple-In, Multiple-Out (MIMO) Radio • VHT20/VHT40/VHT80 support • TxBF (Transmit Beamforming) 802.11ax • 2.4-2.5GHz, 5.15-5.850 GHz and 5.925-7.125 GHz Operating Frequencies • 802.11ax Modulation (1024-QAM) • Dual-band OFDMA • 6G Rate: HE0-HE11 (8 Mbps – 2400 Mbps) • 5G Rate : HE0-HE11 (8 Mbps – 1200 Mbps) • 2.4G Rate: HE0-HE11 (8 Mbps – 573.3 Mbps) • 2x2:2 Stream Multiple-In, Multiple-Out (MIMO) Radio @ 6 GHz • 2x2:2 Stream Multiple-In, Multiple-Out (MIMO) Radio @ 5 GHz • 2x2:2 Stream Multiple-In, Multiple-Out (MIMO) Radio @ 2.4 GHz • HE20/HE40/HE80/HE160 support for 6 GHz • HE20/HE40/HE80 support for 5 GHz • HE20/HE40 support for 2.4 GHz • DL SU-MIMO and MU-MIMO • TxBF (Transmit Beamforming) • Out (MIMO) Radio @ 6 GHz Deberá contar con un radio Bluetooth BLE • Bluetooth® 5.2 Low Energy, IEEE 802.15.4
Interfaces	La solución debe contar con mínimo: • Eth0 is 2.5/1GE with Power over Ethernet (PoE) • Eth1 is 1GE/100
Especificaciones de corriente	Debe ser compatible con el estándar IEEE 802.3at para Power over Ethernet • 802.3af Power over Ethernet (PoE) capable w/o USB • 802.3at Power over Ethernet (PoE) capable w/USB.
Antenas	La solución debe contar como mínimo con las siguientes antenas:

	• Indoor Dual Radio Wi-Fi 6E AP, 2.4 GHz, and 5 GHz or 5GHz and 6GHz, Multirate Port, Internal antennas. IoT Radio
Ganancia	• En 2.4 GHz >= 4.2 dBi • En 5 GHz >= 5.07 dBi • En 6 GHz >= 5.14 dBi • BLE >= .3.65 dBi.
Cumplimiento de normativa	Los equipos ofertados deben cumplir por lo menos con una norma de cuidado del medio ambiente y/o manejo eficiente de energía, para lo cual el proponente debe adjuntar la ficha técnica del fabricante donde se pueda corroborar el cumplimiento de este requerimiento.
	• Cumplimiento de WiFi Alliance • WPA3 security • WMM • Wi-Fi CERTIFIED 6™ • Wi-Fi Agile Multiband
Temperatura de Operación	Al menos en los rangos de 0 a 40*C
GARANTÍA COMERCIAL O PRESUNTA	
5 Años	

DENOMINACIÓN DEL BIEN O SERVICIO	
Access Point Tipo 3.	
CÓDIGO IDENTIFICACIÓN BIEN O SERVICIO	
CLASIFICACION UNSPSC	TIPO DE BIEN O SERVICIO
43221700	Equipo de Servicio de red.
DENOMINACIÓN TÉCNICA DEL BIEN O SERVICIO	
Access Point Tipo 3 (5 años soporte técnico de Fábrica y garantía).	
UNIDAD DE MEDIDA	
Unidad	
DESCRIPCIÓN GENERAL	
CARACTERÍSTICA	**REQUERIMIENTO TÉCNICO MÍNIMO**
Generalidades	• La marca propuesta deberá estar presente por al menos 4 años consecutivos como líder o visionarios en el cuadrante mágico de gartner para redes cableadas e inalámbricas. • La solución debe soportar 802.11ax • La solución debe soportar WPA3 Wi-Fi • La solución debe soportar procesos de visibilidad mediante procesos de ML/AI (Machine learning and artificial intelligence) • Debe soportar ser administrado desde la nube (opción a incluir) • Debe permitir administrarse en caso de ser necesario desde una implementación on-premises. • Debe permitir generación de contraseñas dinámicas a usuarios invitados y enviarlas por email o mensaje de texto o un medio similar

	• Toda la solución ofertada debe ser monomarca (con la controladora/sistema de gestión) incluyendo los accesorios de conectividad • Cada Access Point debe soportar al menos 510 clientes asociados por equipo. • Cada Access Point debe permitir al menos 8 SSID por radio. • Debe contar con un radio dedicado exclusivamente al monitoreo del espectro inalámbrico sin utilizar los mismos radios que se utilizan para transmisión de datos garantizando máximo desempeño, sin interrumpir las transmisiones • De tipo Indoor.
Especificación de Radios	• La solución debe soportar como mínimo los radios de frecuencia de: • SSID per Radio/Total: 16/48 • Users per Radio/total: 512/1536 802.11n • 2.4 GHz–2.5 GHz and 5.150 GHz–5.850 GHz Operating Frequency • 802.11n Modulation • HT 20 High-Throughput (HT) Support (for both 2.4 GHz and 5 GHz) • HT 40 High-Throughput (HT) Support for 5 GHz • A-MPDU and A-MSDU Frame Aggregation • Rates (Mbps): MCS0 – MCS31 (6.5MBps - 600Mbps) 802.11ac • 5.150 GHz–5.850 GHz Operating Frequency • 802.11ac Modulation (256-QAM) • 5G: 4x4 Multiple-In, Multiple-Out (MIMO) Radio • 2.4G: 4x4 Multiple-In, Multiple-Out (MIMO) Radio • Rates (Mbps): MCS0–MCS9 (6.5Mbps), 3466Mbps, NSS = 1-4. • 4x4:4 Stream Multiple-In, Multiple-Out (MIMO) Radio • VHT20/VHT40/VHT80/VHT160 • TxBF (Transmit Beamforming) 802.11ax • 2.4 GHz-2.5 GHz, 5.15 GHz-5.850 GHz and 5.925 GHz-7.125 GHz Operating • Frequencies • 802.11ax Modulation (1024-QAM) • Dual-band OFDMA • 6G Rate: HE0-HE11 (8 Mbps – 4800 Mbps) • 5G Rate : HE0-HE11 (8 Mbps – 4800 Mbps) • 2.4G Rate: HE0-HE11 (8Mbps – 1148 Mbps) • 4x4:4 Stream Multiple-In, Multiple-Out (MIMO) Radio @ 6 GHz • 4x4:4 Stream Multiple-In, Multiple-Out (MIMO) Radio @ 5 GHz • 4x4:4 Stream Multiple-In, Multiple-Out (MIMO) Radio @ 2.4 GHz • HE20/HE40/HE80/HE160 support for 6 GHz • HE20/HE40/HE80/HE160 support for 5 GHz • HE20/HE40 support for 2.4 GHz • DL SU-MIMO and MU-MIMO • TxBF (Transmit Beamforming)

	Deberá contar con un radio Bluetooth BLE • Bluetooth® 5.2 Low Energy, IEEE 802.15.4
Interfaces	La solución debe contar con mínimo: • Eth0, Eth1: (2) Wired Ethernet ports (RJ-45) • 100/1000/2500/5000Mbps auto-sensing link speed Ethernet port, PoE PD • 100/1000/2500Mbps auto-sensing link speed Ethernet port, optional PoE • 15.4W PSE mode requires 802.3bt on Eth0) • 802.3az Energy Efficient Ethernet(EEE) • USB 2.0, Type A, 5V/500mA
Especificaciones de corriente	Debe ser compatible con el estándar IEEE 802.3at para Power over Ethernet • Power Draw: 802.3at PoE: Typical 21W; Max: 25.5W (802.3at profile) w/o PoE • out and USB • Power Draw: 802.3bt: PoE out enable with USB • Eth0 PoE 5Gbps Ethernet port RJ45
Antenas	La solución debe contar como mínimo con las siguientes antenas: • (4) Dual Banded 2.4 GHz and 5 GHz • (4) Single band 6 GHz • (2) 5 GHz Sensor • (2) 6 GHz Sensor
Ganancia	• En 2.4 GHz >= 4.2 dBi • En 5 GHz >= 6 dBi • En 6 GHz >= 5.2 dBi • BLE >= 4.2 dBi
Cumplimiento de normativa	Los equipos ofertados deben cumplir por lo menos con una norma de cuidado del medio ambiente y/o manejo eficiente de energía, para lo cual el proponente debe adjuntar la ficha técnica del fabricante donde se pueda corroborar el cumplimiento de este requerimiento.
	• Cumplimiento de WiFi Alliance • WPA3 security • WMM • WMM-Power Save • Wi-Fi CERTIFIED 6™ • Wi-Fi Agile Multiband
Temperatura de Operación	Al menos en los rangos de: • Operating: 0°C to 50°C (32°F to 122°F) • Storage: 0°C to 70°C (32°F to 158°F) • Humidity: 0% to 95% (non-condensing)
GARANTÍA COMERCIAL O PRESUNTA	
5 Años	

DENOMINACIÓN DEL BIEN O SERVICIO
Solución de Gestión Wireless LAN.
CÓDIGO IDENTIFICACIÓN BIEN O SERVICIO

CLASIFICACION UNSPSC	TIPO DE BIEN O SERVICIO
43232804	Software de administración

DENOMINACIÓN TÉCNICA DEL BIEN O SERVICIO
Solución de Gestión Wireless LAN Cloud (5 años soporte técnico y garantía)
UNIDAD DE MEDIDA
Unidad
DESCRIPCIÓN GENERAL

SOLUCIÓN DE WLAN		
1: Solución de Gestión de Wifi Cloud		
ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
1.1	Generalidades	La marca propuesta deberá estar presente por al menos 4 años consecutivos como líder o visionarios en el cuadrante mágico de gartner para redes cableadas e inalámbricas.
		Toda la solución ofertada debe ser monomarca (con los Access point) incluyendo los accesorios de conectividad
		La solución debe soportar aprovisionamiento automático: con implementación de zero-touch, aplicando automáticamente políticas de configuración
		La solución debe permitir visibilidad de las aplicaciones para validar el uso de estas.
		La solución debe permitir la administración simplificada: flujos de trabajo guiados para crear e implementar políticas de red, con configuración avanzada opcional.
		La solución debe permitirse servicio en Nube con más de dos proveedores.
		La solución debe operar en arquitectura de Nube que garantice disponibilidades superiores al 99.995%
		La solución debe estar en capacidad de validar el estado de la red, vista en tiempo real e histórica del estado del cliente y del dispositivo con herramientas de corrección integradas.
		La solución debe ser en modalidad cloud, más los planos de control y datos deben permanecer en premisas dentro de los equipos de red.
		La solución debe tener la posibilidad que los Access Point puedan ser administrados en nube publica y on-premises, sin cambios de hardware en estos.
		En caso de que la entidad decida migrar su sistema de cloud a premisas durante el tiempo de la solución, la misma licencia deberá poder ser utilizada en cualquiera de los dos esquemas.
		La solución debe soportar como mínimo los siguientes idiomas: inglés, español.
		La solución debe permitir también el monitoreo y gestión de switches y routers garantizando la operación de toda la red.
		La solución debe contar con herramientas de localización con características como:
		Detectar la ubicación de un dispositivo

		Rastreo de la ubicación de un dispositivo
		Conteo de dispositivos por ubicación
1.2	Seguridad y privacidad	La solución debe soportar como mínimo funcionalidades de:
		Control de acceso basado en roles.
		Los datos del cliente y de la red deben ser privados y seguros.
		Ningún dato del cliente debe atravesar la red Cloud del fabricante
		Los administradores deben poder tener single sing on a través de Security Assertion Markup Language
		Autenticación multifactor para administradores.
1.3	Configuración centralizada	La solución debe soportar:
		Funcionalidad de acceso de invitado
		Actuar como servidor RADIUS o proxy RADIUS, y como Servidor DHCP.
		Vista centralizada de todos los objetos de configuración.
		Capacidad para editar en masa las propiedades de los dispositivos
		Posibilidad de programar la actualización del firmware.
		Acceso a la interfaz de línea de comandos (CLI) a dispositivos extremos
		Autenticación con directorio activo / LDAP
		Soporte IPv6
		Configuración del servidor Syslog y SNMP
		Autoaprovisionamiento
		Auditoría de configuración, copia de seguridad, restauración, importación y exportación.
		Capacidad de generar administraciones separadas e independientes por sedes con el fin de admitir múltiples organizaciones virtuales
		La solución debe permitir acceder por SSH a los equipos para configuraciones por CLI.
		La solución debe permitir aplicar políticas de red distintas a diferentes grupos de Access Points incluso si se encuentran ubicados en el mismo edificio.
1.4	Características de implementación	La solución debe soportar:
		Registro de clientes usando autoservicio
		Configuración guiada paso a paso en pantalla
		Capacidad de construcción de mapas de calor
		Los dispositivos se deben conectar automáticamente o generando aprovisionamiento
		Autoaprovisionamiento de dispositivos con política de red y udpates de firmware
1.5	Gestión centralizada de políticas	La solución debe estar en capacidad de:
		Clasificación de dispositivos por ubicación y zona horaria
		Definición de la aplicación del cliente
		Clasificación del cliente por ubicación, tipo de sistema operativo, dirección MAC
		Múltiples perfiles de usuario para cada SSID

		Desplegar y gestionar reglas de políticas de firewall de aplicación, red y capa MAC.
		Desplegar y gestionar Política de WIPS para detección y mitigación de puntos de acceso no autorizados
1.6	Seguridad Operacional	La solución debe ser capaz de:
		Proteger las cuentas con sus contraseñas, accediendo de forma segura con SSL
		Manejar el tráfico de gestión cifrado y restringido por medio de un protocolo estándar y líder en la industria probado sobre HTTPS
		Manejar la operación fuera de banda asegura que no haya datos del cliente atravesando los servicios en la nube del fabricante
		El inicio de sesión único (SSO) debe ser empleado también para el administrador de cuentas
		Generar monitoreo y gestión centralizados.
		Permitir control de acceso basado en roles (RBAC) integrado para delegar roles y permisos a diferentes administradores
1.7	Dashboard	La solución debe soportar:
		Widgets gráficos y tarjetas de estado con capacidades de desglose.
		Control por rango de tiempo en el dashboard para ver el historial.
		Vistas de políticas de red, AP, dispositivos cliente, usuarios y aplicaciones
		Función de búsqueda global por política de red, dirección MAC, número de serie, usuario, nombre de host o nombre de la aplicación.
		Tiempo ilimitado en retención de datos históricos de monitoreo e informes.
		Informe de resumen de red interactivo.
		Filtros contextuales guardables por ubicación, SSID, política, usuario, perfil y tipo de SO cliente.
1.8	Acceso de Invitados	La solución debe estar en capacidad de:
		Incorporar y gestionar dispositivos personales de visitantes y empleados.
		Proporcionar múltiples flujos de trabajo de incorporación a través del portal web cautivo.
		Autenticación de PSK, 802.1X (RADIUS)
		Se requiere de una funcionalidad para poder asignar claves independientes para un mismo SSID, sabiendo a que usuario se le dio que clave directamente desde la plataforma.
		Admitir la creación o integración (de portales cautivos de terceros y/o personalizados, incluida la carga HTML para una mayor flexibilidad de su implementación.
		Se debe poder segmentar el tráfico de los invitados de manera lógica para garantizar su aislamiento.
		Se debe contar con la capacidad de que invitados hagan el login mediante redes sociales desde la misma plataforma.
		Poder colocar splash pages personalizables por ubicación.
		Contar con mecanismos como auto registro y recibir código vía SMS para acceso a la red de invitados.

1.9	Troubleshooting	La solución debe estar en capacidad de hacer automáticamente:
		Análisis de comportamiento del cliente, Monitoreo y optimización del rendimiento de la red en tiempo real e histórico
		Interfaz optimizada de la mesa de ayuda con resumen del problema y solución sugerida
		Rol de usuario dedicado del servicio de asistencia
		Solución de problemas históricos con detección automática de problemas.
		Marcar problema resuelto o escalar problema con notificación por correo electrónico.
		Interfaz de línea de comando (CLI) incorporada y SSH remoto hacia los equipos
		Visibilidad de log de autenticación de RADIUS
		Descarga de datos técnicos del AP
		Debe permitir la captura de paquetes para usar eso en aplicaciones como Wireshark o Cloudshark
		Análisis de Espectro.
1.10	Monitoreo	La solución debe soportar y ejecutar tareas como:
		Informe de historial de WIPS
		Capacidad de desglose de la lista de clientes a la vista del cliente.
		Lista de dispositivos conectados y visibilidad de aplicaciones.
		Lista de clientes en tiempo real, uso de datos y estado de conexión
		Filtros guardables y reutilizables compartidos en el tablero y el monitor.
		Posibilidad de generar Informes en formatos como: PFD o Word, Excel o CSV.
		Rogue AP y monitoreo de clientes no autorizados.
		La solución de WIPS deberá permitir una vista centralizada de todas las ubicaciones y sus amenazas.
		La solución de WIPS deberá contar con una base de al menos 35 amenazas.
		Datos en tiempo real para clientes y usuarios de conexión.
		Contar con mecanismos para el control y monitoreo de dispositivos de IoT dentro del sistema.
1.11	Confiabilidad	La solución en nube debe ofrecer al menos:
		Alta disponibilidad con recuperación ante desastres y redundancia.
		99.995% de tiempo de actividad SLA (excluyendo ventanas de mantenimiento)
		Copias de seguridad programadas
		Soporte de monitoreo 24x7
1.12	Herramientas de Ubicación	Se deberá contar con las siguientes funcionalidades dentro de la solución:
		Determinar en qué zonas se encuentran dispositivos WiFi.
		Determinar en qué zonas se encuentran dispositivos bluetooth.
		Contar con un dashboard dedicado para esta función.
GARANTÍA COMERCIAL O PRESUNTA		

5 Años

DENOMINACIÓN DEL BIEN O SERVICIO	
Solución de Gestión de Redes.	
CÓDIGO IDENTIFICACIÓN BIEN O SERVICIO	
CLASIFICACION UNSPSC	TIPO DE BIEN O SERVICIO
43232804	Software de administración
DENOMINACIÓN TÉCNICA DEL BIEN O SERVICIO	
Software de Gestión de Redes (5 años soporte técnico y garantía)	
UNIDAD DE MEDIDA	
Unidad	
DESCRIPCIÓN GENERAL	

Función	Descripción
CANTIDAD	Debe ser la indicada para soportar toda la propuesta. En caso de que la solución SDN dependa de la plataforma de gestión o controladora SDN, esta debe ser redundante en todos sus módulos.
Requisitos Generales	Sistema de Administración unificada LAN que permita además la visibilidad centralizada y el control de los recursos de hardware de red alámbrica a través de una interfaz gráfica basada en web.
	La solución deberá ser de la misma marca que los switches ofertados
	La herramienta podrá ser un appliance físico y podrá ser una o más máquinas virtuales, en caso de que la plataforma de comunicaciones del DataCenter o la red corporativa dependa de dicho software para proveer la solución SDN o mantener su operación, esta deberá ser redundante y el oferente deberá considerar todo lo necesario para que ello ocurra.
	La solución propuesta debe ser del mismo fabricante que la plataforma de Wireless / Networking / Gestion.
	La solución debe considerar el licenciamiento necesario para soportar todo el equipamiento solicitado en la presente licitación (Switch / Wireless / Analíticos)
Administración	Capacidad de definir usuarios y grupos de acceso a la herramienta
	Capacidad de definir el método de autenticación de usuarios. Debe permitir la autenticación mediante servidor RADIUS o LDAP externo.
	Capacidad de definir los privilegios de acceso o capacidades de los usuarios o grupos (qué pueden ver, qué pueden administrar)
	Capacidad de establecer las credenciales y perfiles de acceso a los dispositivos descubiertos
	Capacidad de presentar información en dispositivos móviles (tabletas y teléfonos inteligentes)
Inventario	Capacidad de descubrimiento automático de dispositivos por rangos de direcciones IP
	Capacidad de agregar dispositivos manualmente

	Capacidad de agrupar dispositivos en grupos creados automática o manualmente
	Capacidad de agrupar puertos en grupos creados manualmente.
	Capacidad de agregar MIBs de terceras partes.
	Capacidad de examinar las MIBs soportadas por un dispositivo activo, incluyendo las capacidades de realizar queries, escribir valores y agregar filas.
	Capacidad de crear tablas y gráficos basados en información extraída de las MIBs de un dispositivo.
	Capacidad de publicar la información extraída de las MIBs de un dispositivo en formato web para poder ser vista desde cualquier browser.
	Capacidad de agregar aplicaciones de terceras partes a los menús de la herramienta para la administración específica de dispositivos de otros fabricantes.
	Capacidad de agregar y borrar dispositivos de la base de datos de inventario.
	Capacidad de agregar y borrar grupos de la base de datos de inventario.
	Capacidad de mantener una biblioteca de Firmware y de asignar determinadas imágenes a distintos dispositivos
	Capacidad de actualizar manual o automáticamente el firmware de uno o varios dispositivos simultáneamente
	Capacidad de archivar información de configuración de dispositivos manual o automáticamente
	Capacidad de comparar una configuración almacenada con la configuración actual de un dispositivo, resaltando las diferencias entre ambas.
	Capacidad de crear y aplicar plantillas de configuración a uno o más dispositivos simultáneamente,
	Capacidad de restaurar la configuración almacenada de un dispositivo.
	Capacidad de configurar el método de transferencia de firmware y configuraciones. Debe soportar TFTP, FTP y SCP.
	Capacidad de aplicar (al menos) las siguientes funcionalidades a dispositivos de terceras marcas:
	1. Carga de configuración.
	2. Descarga de configuración.
	3. Descarga de firmware.
	4. Reset del dispositivo.
	Capacidad de seguimiento de un dispositivo en función de su número de serie.
	Capacidad de generar reportes de puertos y slots libres y ocupados en los dispositivos.
	Deberá tener la capacidad de visualizar la red física y la red SDN en la misma plataforma, integrando un único software para la gestión de la red SDN.
Dispositivos	Capacidad de desplegar una representación gráfica del dispositivo, incluyendo información sobre puertos y su estado.
	Capacidad de presentar información de estado de fuentes y ventiladores, y de uso de CPU.

	Capacidad de crear y ejecutar secuencias de comandos CLI en los dispositivos administrados.
	Capacidad de integrar scripts a los menús de un dispositivo.
	Capacidad de ver información sobre un dispositivo, incluyendo:
	1. Imagen gráfica del dispositivo.
	2. Puertos y su estado.
	3. Información del dispositivo y sus módulos.
	4. Estado de fuentes de alimentación y ventiladores.
	5. Utilización de puertos.
	6. Alarmas y eventos.
	7. Archivos de configuración.
	Capacidad de administrar dispositivos de múltiples marcas.
	Capacidad de localizar un dispositivo o usuario final y mostrar su punto de conexión a la red, empleando:
	1. Dirección MAC.
	2. Dirección IP.
	3. Nombre de Usuario
	Capacidad de mostrar gráficamente los dispositivos empleados para conectar un usuario a la red.
	Deberá soportar búsquedas de dispositivos por MAC Address, dirección IP, username, hostname.
Wireless	Capacidad de administrar controladores y AP del mismo fabricante.
	Capacidad de detectar por lo menos las siguientes amenazas:
	1. AP intrusos (rogue)
	2. Dispositivos en modo Ad-Hoc.
	3. Ataques de Denial of Service (DoS)
	4. Fuentes de interferencia
	5. Intentos de password Cracking
	Capacidad de habilitar la captura de información en tiempo real en un AP de la red.
	Capacidad de reportar fuentes de interferencia.
	Capacidad de desplegar información sobre cada controlador inalámbrico.
	1. Listado de APs conectados por canal
	2. Clientes
	Uso de ancho de banda.
	Capacidad de listar los APs del sistema y desplegar información individual sobre:
	1. Controlador al que está conectado
	2. Ancho de banda
	3. Clientes conectados
	Alarmas

	Capacidad de listar los clientes del sistema y desplegar información individual sobre:
	1. Horarios de inicio y fin de sesión.
	2. Historial de roaming entre APs.
	3. Cambios de dirección IP.
	4. Cambios de estado de autenticación.
	Clientes conectados.
	Capacidad de listar las amenazas detectadas mediante WiDS/WiPS
	Realizara capturas de tráfico en tiempo real en Puntos de Acceso, para facilitar diagnósticos y solución de problemas.
Mapas	Capacidad de crear mapas físicos manual o automáticamente con descubrimiento automático de enlaces entre dispositivos en función de información obtenida de:
	1. Protocolos de descubrimiento (CDP/LLDP/STP).
	2. STP.
	3. OSPF.
	4. 802.3ad (Link Aggregation).
	Capacidad de crear mapas planos o jerárquicos.
	Capacidad de guardar y volver a abrir mapas creados.
	Capacidad de editar mapas agregando fondos, líneas, textos y otros objetos gráficos.
	Capacidad de brindar información detallada de los vínculos presentes en los mapas
	Capacidad de brindar información detallada de los puertos presentes en un dispositivo del mapa.
	Capacidad de agregar información contextual a los mapas (color y grosor de enlaces, símbolos, etc.), basado en información de Spanning Tree, OSPF, Link Aggregation (802.3ad).
	Capacidad de localizar el puerto de ingreso a la red de usuarios o dispositivos (por dirección IP o nombre de usuario).
	Capacidad de localizar un cliente inalámbrico, un AP, un dispositivo o un cliente alámbrico en la red.
Alarmas y Eventos	Capacidad de monitorear alarmas y eventos de los dispositivos administrados en forma centralizada
	Capacidad de agregar, configurar y modificar alarmas basadas en diferentes eventos tales como:
	1. Caída de un equipo.
	2. Severidad de evento (informational, warning, critical, emergency, etc).
	3. Notificación Trap.
	Capacidad de borrar una alarma que ya ha sido atendida
	Capacidad de generar alarmas basadas en anomalías de flujo de información
	Capacidad de agregar traps que puedan disparar alarmas
	Capacidad de recolectar información de Syslog y SNMP traps de los dispositivos administrados

	Capacidad de manejar alarmas y eventos de RMON
	Capacidad de capturar información con RMON
	Capacidad de presentar información capturada con RMON
	Capacidad de presentar información detallada de estadísticas RMON los puertos Ethernet
	Al generar una alarma el sistema debe tener la capacidad de realizar las siguientes acciones:
	1. Envío de e-mail.
	2. Envío de Syslog.
	3. Envío de Trap SNMP.
	4. Ejecutar scripts de configuración o programas.
Políticas	Capacidad de centralizar la creación y distribución de políticas de acceso a la red.
Reportes	Capacidad de diseñar reportes a medida o modificar reportes existentes.
	Generará reportes que proporcionen la siguiente información sobre los dispositivos:
	1. Alarmas.
	2. Disponibilidad.
	3. Inventario.
	4. Rastrear cambios realizados en los dispositivos.
	5. CPU.
	6. Memoria.
	Generará reportes que proporcionen la siguiente información sobre las interfaces:
	1. Flujos.
	2. Ancho de banda.
	3. Uso de PoE.
	4. Utilización.
	Podrá realizar las siguientes funciones de monitoreo:
	1. Mostrar vistas topológicas de un dispositivo de Red.
	2. Analizar detalles de flujos, aplicaciones, fuentes y destinos por puerto.
	3. Analizar en tiempo real estatus, utilización, errores y paquetes por puerto.
	4. Analizar un histórico de utilización y disponibilidad por puerto.
	5. Mostrar todos los endpoints conectados a un puerto.
	Generará reportes que proporcionen la siguiente información sobre la red inalámbrica:
	1. APs.
	2. Clientes.
	3. Controladoras.
	4. Top de APs y clientes por utilización de ancho de banda
Visor de flujos	Deberá contar con un Visor de Flujos para sFlow o NetFlow el cual mostrará la siguiente información:

	1. Dirección IP Cliente, quien origina el flujo
	2. Dirección IP Servidor, que recibe o maneja el flujo
	3. Puerto TCP/UDP del Servidor
	Protocolo
	4. Conteo de flujos.
	5. Duración.
	6. Cantidad de bytes transmitidos.
	7. Cantidad de bytes recibidos.
	8. DSCP(Diffserv Codepoint).
	9. TTL (Time to Live).
	10. Tiempo de respuesta de las aplicaciones.
	11. Tracking de aplicaciones.
	12. Correlación de aplicaciones con usuarios.
Integraciones	Deberá contar con integraciones a plataformas de seguridad, tipo palo alto/Fortinet/checkpoint entre otros y a sistemas de virtualización como VMWare para hacer seguimiento de las máquinas virtuales. Además de la integración con plataforma del tipo MDM como Intune para hacer perfilamiento de usuarios.
Seguridad	Deberá tener la capacidad de adicionar funcionalidades de control de acceso solo adicionando licenciamiento de NAC, el cual, podrá integrar la información recolectada de analíticos/wifi/red para correlacionar la información de los usuarios.
Flujos y Aplicaciones	La solución deberá ser capaz de recolectar información de flujos de NetFlow.
	Capacidad de presentar información sobre flujos recolectados por la aplicación incluyendo:
	1. Cantidad de flujos
	2. Direcciones IP de cliente y servidor
	3. Protocolos y puertos
	4. Duración
	5. Tasa de transmisión
	6. Paquetes/bytes transmitidos
	7. Paquetes/bytes recibidos
	Capacidad de interactuar con Analizadores de Aplicación que permitan conocer las aplicaciones de los flujos
	Contará con un visor de flujos que permita obtener la siguiente información:
	1. Dirección IP del Cliente
	2. Dirección IP del Servidor
	3. Puerto del Servidor
	4. Aplicación
	5. Tiempo de respuesta de la Red
	6. Tiempo de Respuesta de la Aplicación
	7. Ubicación

	8. Username del cliente
	9. Protocolo empleado para la conexión
	10. Ubicación del cliente (Switch/puerto, Access Point/SSID)
	11. Ancho de banda promedio del flujo
	12. Paquetes Transmitidos/Recibidos
	13. Bytes Transmitidos/Recibidos
	Debe permitir al administrador agrupar segmentos de red para asociarlos con un edificio, oficina o áreas geográficas, para así identificar el análisis de tráfico relacionado con alguna ubicación específica.
	Debe determinar la siguiente información: la aplicación, URL, información del certificado, versión del browser, medir tiempo de respuesta y capaz de obtener información contextual del acceso como: usuario, rol o perfil, tipo de dispositivo y ubicación.
	La solución debe presentar la información analizada con múltiples Dashboards con funcionalidad Drill-down para mostrar información más detallada.
	El Dashboard debe contar con al menos cuatro distintos tipos de grafica para mostrar la información (p.e. grafica de pay, etc.)
	Debe mostrar los servidores y clientes activos durante las últimas 24 horas, así como el top de clientes y servidores por ancho de banda.
	Mostrará el Top de aplicaciones en diversos tipos de gráfica, así también permitirá revisar por aplicación los clientes y datos relacionados.
	Mostrará los flujos de comunicación de las aplicaciones, con las siguientes opciones:
	1. Flujos con los tiempos de respuesta TCP más altos (peores)
	2. Aplicaciones con tiempos de respuesta más altos (peores)
	3. Top de aplicaciones, clientes o servers con base al ancho de banda empleado, paquetes o cantidad de conexiones
	La solución debe incluir la capacidad de identificar al menos 10,000 huellas de aplicaciones. Además, la solución debe contar con una base de identificación de aplicaciones (fingerprints) abierta y personalizable, para que el administrador pueda crear y personalizar la identificación de aplicaciones.
	Para simplificar la resolución de problemas de aplicaciones, la solución debe mostrar el tiempo de respuesta de la Red y de las aplicaciones, para que el administrador distinga entre problemas de desempeño de la Red o de la aplicación.
	Debe mostrar el número de veces que han sido detectados flujos que concuerden con el fingerprint de una aplicación con (hits).
	La solución debe ser capaz de procesar un mínimo de 50mil flujos por minuto.
Data Center Manager	Capacidad de administrar en forma unificada un Data Center Fabric brindando visibilidad, control y automatización a entornos de red, servidores, almacenamiento y aplicaciones virtualizadas
SDN/APIs	Capacidad de soporte de una base abierta, programable y administrada centralmente que permita implementar SDN e interactuar con diferentes aplicaciones de terceras partes para :
	1. Datacenters

	2.	Seguridad
	3.	Movilidad
	4.	Operaciones de IT
	5.	Convergencia

GARANTÍA COMERCIAL O PRESUNTA
5 Años

DENOMINACIÓN DEL BIEN O SERVICIO
Software de Control de Acceso (NAC).

CÓDIGO IDENTIFICACIÓN BIEN O SERVICIO

CLASIFICACION UNSPSC	TIPO DE BIEN O SERVICIO
43233203	Software de manejo de seguridad de red o de redes privadas virtuales VPN.

DENOMINACIÓN TÉCNICA DEL BIEN O SERVICIO
Software de Control de Acceso (NAC) (5 años soporte técnico y garantía)

UNIDAD DE MEDIDA
Unidad

DESCRIPCIÓN GENERAL

Función	Descripción
Características generales	· La solución propuesta debe ser del mismo fabricante que la plataforma de Wireless / Networking / Gestion / SDWAN / Control de acceso
	· La solución debe ser implementada en modalidad virtual VMWare ESXi 6.5 o superior
	· La solución debe quedar habilitada en alta disponibilidad, considerando al menos 3 equipos implementados en redes diferentes en ambos datacenter de caja la araucana
	· Debe operar con acceso de usuarios a la red cableada, inalámbrica y VPN.
	· La solución debe tener integración absoluta con la herramienta de gestión y SDN del mismo fabricante.
	· Soportar al menos 5000 endpoints concurrentes en un solo Appliance.
	· Soportar un esquema de alta disponibilidad.
	· Gestión Centralizada de la Solución de Control de Acceso para simplificar la implementación y administración de la misma.
	· La solución debe combinar autenticación, escaneo de vulnerabilidades y localización, para autorizar el acceso a la red con un perfil adecuado para cada dispositivo. Por medio de integraciones con terceros
	· La solución debe contar con funcionalidades de BYOD (Bring Your Own Device), que incluya registro de dispositivos sesiones basadas en login de usuarios.
	· La funcionalidad de BYOD debe cumplir con lo siguiente:
	o Auto-descubrimiento

	o Perfilamiento multinivel de dispositivos
	o Flexibilidad
	o Gestión de Políticas
	o Acceso de Invitados
	o Integración con MDM (Mobile Device Management)
	o Integración con VDI (Virtual Desktop Infraestructure)
	· Debe realizar un registro automático de invitados, que permita un acceso seguro de invitados en la red.
	· Debe contar con un esquema para limitar la visualización de endpoints, para que en ambiente Multi-tenant o Enterprise pueda limitarse la información y estadísticas de grupos de endpoints entre usuarios Administradores.
	· La Solución tendrá la capacidad de integrarse a una Arquitectura de Seguridad Preventiva y Reactiva, por lo tanto, deberá ser capaz de interactuar con:
	o Consola MDM (Mobile Device Management)
	o Sistema de Detección de Intrusos (IPS)
	o Firewall de Siguiente Generación (NGFW)
	· La Solución debe ser capaz de integrarse con terceros, tales como:
	· Polycom
	· Avaya
	· Palo Alto
	· Fortinet
	· IF-MAP
	· OS LIA
	· MS Intune
	En caso de requerir licenciamiento adicional para las integraciones, este deberá estar incluido.
	El sistema de Control de Acceso a la Red deberá cumplir con las siguientes características de Control y Seguridad:
	· Tener la capacidad de ser un RADIUS Proxy
	· Soportar RFC 3580
	· Soportar las siguientes autenticaciones:
	- 802.1X (Extensible Authentication Protocol)
Funciones de Control y Seguridad	- MAC
	- Web-based
	- Kerberos
	· Soportar IPv6
	· Debe ser interoperable con Microsoft NAP y Trusted Computing Group TNC.
	· Debe contar con un esquema de balanceo de carga para una solución compuesta por más de un appliance de NAC.
	· La solución debe ser capaz de manejar los siguientes protocolos de autenticación RADIUS:

o PAP
o CHAP
o MS-CHAP
o EAP-TTLS
o EAP-MD5
o PEAP
o EAP-MSCHAPv2
o EAP-TLS
· La solución debe ser capaz de usar un registro RADIUS accounting, para determinar en tiempo real estado de las conexiones.
· La solución debe ser capaz de ofrecer un control granular de acceso con los siguientes criterios:
o Tipo de autenticación
o Grupos de endpoints por MAC Adress, dirección IP o Hostname
o Tipo de dispositivo por sistema operativo
o Ubicación en la Red del endpoint
o Hora y Día
o Grupo de usuario, en LDAP, RADIUS, etc.
· La solución deber contar con las funcionalidades de: permitir, negar, priorizar, etiquetar, redirigir, aplicar rate-limit y auditar tráfico de red, con base en identidad del usuario, tipo de dispositivo, hora y ubicación de acceso, asignar VLan, servicios, control de accesos
· La solución debe tener integración nativa con la plataforma SDN del mismo fabricante, dando la capacidad de asignar túneles/VLan, Servicios o Vxlan directamente al role del usuario.
· Debe incluir una función de Registro de endpoints a través de una página Web, la cual debe contemplar lo siguiente:
o Determinar la validez de los usuarios en una base de datos.
o Ofrecer un Patrocinador, usuario confiable de la Organización, quien podrá autorizar y asignar el nivel de acceso de los endpoints
o Especificar el número máximo de MAC Address registradas por usuario
o A través de un portal seguro (HTTPS) se podrán: visualizar, agregar, eliminar y modificar los registros. El portal estará disponible para Patrocinadores y Administradores de la Solución.
· La Solución debe contar con un portal para registro de Invitados, en el cual el usuario introduzca la dirección de correo electrónico del Patrocinador, quien será notificado por correo electrónico y asignara el acceso. El registro de Invitados contara con las opciones de acceso:
o Sin Patrocino
o Patrocinio opcional
o Patrocinio obligatorio
· La solución debe contar con la funcionalidad de verificar los datos de contacto del usuario que se registra a través del Portal de Invitados, dicha validación se realizara mediante un código que se enviara al usuario a través de e-mail y/o SMS.

· La solución debe tener la capacidad de cerrar el acceso de una MAC Address dada a un solo puerto de un switch, para que el dispositivo solo tenga acceso a la red mediante el switch y puerto especificado.
· La solución debe ser capaz de mostrar la siguiente información de los enpoints conectados a la Red:
o MAC Address
o IP Address
o Dirección IP y puerto del switch acceso
o Estatus en la revisión del endpoint
o Username
o Hostname
o Tipo de dispositivo
o Tipo de autenticación
o Autorización
o Perfil
o Fecha de primera vez que se detecto
o Fecha de última vez que se detecto
o Fecha ultima en que se escaneo
o Ubicación
o Aplicaciones más consumidas
o Tiempo de respuesta de las aplicaciones
· La Solución deberá permitirle al Administrador crear grupos de endpoints en base a :
o MAC Address
o Dirección IP o Subredes
o Hostname
o Grupos en LDAP
· La Solución permitirá al Administrador crear Grupos de Ubicación, los cuales restrinjan el acceso de los endpoints por:
o Dirección IP de Switch y puerto
o Dirección IP de Controladora, Access Point y SSID
· La Solución debe ser capaz de restringir endpoints con base en el día y la hora que el usuario solicita el acceso a la Red.
· La Solución deberá permitirle al Administrador crear grupos de usuarios en base a:
o Username
o Grupo LDAP
o Grupo RADIUS
· La Solución debe ser capaz de detectar de forma automática los endpoints por familia de sistema operativo:
o MAC
o Windows

	o Apple iOS
	o Android
	o Blackberry
	o Linux
	· La Solución debe ser capaz de retener información y estadísticas de los endpoints y su actividad al menos por 90 días, el Administrador podrá modificar el periodo de retención de dicha información.
	La solución debe permitir agregar, editar y probar reglas de notificación, las cuales se activen por eventos de NAC, permitiendo acciones como:
	o Envío de e-mail
	o Syslog
	o SNMP trap
	o Ejecutar script
	· Las reglas de notificación de NAC podrán ser activadas por los eventos siguientes:
	o Cuando un enpoint sea agregado o removido
	o Cuando el estatus de un endpoint cambie
	o Cuando el tipo de autenticación o un tipo de dispositivo cambie
	o Cuando se produzca un cambio en un Grupo de Usuarios
	o Cuando se produzca un cambio en un Grupo de Endpoints
	o Cuando en el Registro un usuario o dispositivo sea agregado, actualizado o removido
	· Debe contar con una herramienta capaz de proporcionar:
	o Reportes
	o Dashboard
	o Identificación de los endpoints conectados a la Red
	o Información sobre los endpoints y eventos asociados
	o Salud o nivel de cumplimiento de cada endpoint
	· Debe contar con una herramienta de análisis que muestre detalles del endpoint registrado por NAC y sus flujos (Netflowo Sflow), tanto para red alámbrica como inalámbrica. Debe permitir al administrador:
	o Visualizar la topología de los dispositivos de red y endpoint en cuestión.
	o Analizar detalles de flujos, aplicaciones, emisor y receptor por puerto
	o Analizar en tiempo real el estatus, utilización, errores y paquetes por puerto
	o Análisis histórico de la utilización y disponibilidad de un puerto
Hardware	Instalado On-Premise. Rack (1U) - Procesador: 1 x Intel Xeon-B 3508U CPU for 8 Core (2,1 GHZ/ Máximo: 1 Procesador - Memoria RAM: 32GB (1 x 32GB) PC5-5600 RDIMM / Máximo: 16 Memorias - Red: 2 x 1GbE Embedded- Disco Duro: 2 x 960GB SSD SATA 6G Read Intensive LFF (3.5in) / Máximo: 4 Discos Controladora de Discos: SATA 1 - RAID - RAID: 0/1/5/10 Fuente De Alimentación: 1 x 800W Hot Plug Low Halogen Power Supply Kit / Máximo 2 Fuentes -

	Garantía: 5 Year Next Business Day Warranty - Administración: Integrated Lights-Out 6 (iLO 6) management processor (No Licence) / (Advanced) / No OneView or Insight Control - Otros: No incluye teclado ni mouse.
	Condiciones Garantía. Cobertura: 24x7.El soporte técnico está disponible para registrar y trabajar en incidentes en cualquier momento. Respuesta Remota (Severidad Critica):15 minutos, 24x7. Para incidentes críticos (Servidor inoperativo), Fábrica se comunica y conecta. Acceso a Expertos. Acceso directo a especialistas de producto. Se conecta rápidamente con un técnico que conoce a fondo el producto. Respuesta In Situ (Hardware). 4 horas, 24x7. Garantiza que un técnico autorizado estará en su sitio con las piezas de repuesto en un plazo de 4 horas para comenzar la reparación del hardware.

GARANTÍA COMERCIAL O PRESUNTA
5 Años

DENOMINACIÓN DEL BIEN O SERVICIO
Servicios Técnicos Profesionales.

CÓDIGO IDENTIFICACIÓN BIEN O SERVICIO	
CLASIFICACION UNSPSC	TIPO DE BIEN O SERVICIO
81111800	Servicios de sistemas y administración de componentes de sistemas

DENOMINACIÓN TÉCNICA DEL BIEN O SERVICIO
Servicios Técnicos Profesionales.

UNIDAD DE MEDIDA
Unidad

DESCRIPCIÓN GENERAL

Se deben realizar o cumplir los siguientes requerimientos y actividades:

- Dentro de los servicios se debe tener en cuenta la Instalación, configuración y puesta en producción de las soluciones ofertadas, así como la entrega a satisfacción de estos a la entidad, realizando todas las tareas necesarias para cumplir con ello, sin que esto genere gastos o cobros adicionales para la entidad.
- El oferente deberá entregar todas las soluciones / equipos en los sitios/sedes indicadas por la entidad.
- Todas las plataformas deberán ser de propósito específico, no se aceptan soluciones genéricas.
- Configuración y alistamiento del software y firmware del hardware a la última versión estable aprobada por el fabricante.
- Implementación de las soluciones de acuerdo con las mejores prácticas del fabricante, teniendo en cuenta una arquitectura de red segura.
- Puesta en Producción de las plataformas ofertadas.
- Configuración y estabilización de las plataformas ofertadas.
- Entrega de informes y diagramas de la solución implementada
- Las actividades de instalación, configuración y puesta en producción de las plataformas ofertadas deberán ser realizadas por personal certificado por el fabricante a nivel instalación y configuración o su equivalente según el fabricante, asegurando un mínimo de certificación en instalación y configuración de soluciones de Switching y Wireless. Para esto se deben aportar las hojas de vida.
- Dentro de los servicios se debe incluir un curso dictado por directamente por fábrica para 2 empleados de la entidad.

- El oferente debe contemplar en su oferta todos los costos o gastos asociados a la logística (desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, refrigerios, entre otros) requerida para que el personal asignado al proyecto pueda cumplir sus funciones.
- Instalación de los Access Point, es decir, se deben dejar instalados en la edificación en sitio estipulado por el Municipio de Envigado (Montaje de Access Point en Altura). Cada Access Point debe incluir su base soporte para instalación a la medida.

Servicio de Soporte Técnico deberá contemplar:

- El oferente debe contar con un SOC (Security Operation Center) con el fin de brindar el servicio de soporte el cual debe incluir atención de incidentes sobre la plataforma ofertada.
- El contratista deberá realizar y documentar entre otras, las siguientes actividades previa coordinación con el supervisor del contrato en desarrollo:
    - Revisar y resolver las actividades de soporte sobre las plataformas ofertadas.
    - Revisar la consistencia de las configuraciones realizadas a la solución implementada. Hacer uso de las herramientas de detección, diagnóstico y resolución de novedades que ayuden a conservar la estabilidad y óptimo rendimiento de la plataforma.
    - Mantener actualizado el Firmware de todos los componentes ofertados de acuerdo con las últimas versiones estables liberadas por el fabricante.
    - Configurar y revisar los reportes / logs de las plataformas.
-

Condiciones del Servicio.

Terminología.

Caso: Incidente, problema, requerimiento o evento manifestado por el Municipio de Envigado que requiere atención técnica programada, independiente de su severidad. La atención programada puede reuniones para definir mejoras, alcances, buenas prácticas o rediseños.
Requerimiento: Solicitud del Municipio de Envigado para realizar configuraciones, ajustes, mejoras, implementación de buenas prácticas que mejoren el desempeño o saquen mejor provecho a las funcionalidades de la plataforma o infraestructura tecnológica objeto del servicio.

Tiempo de Atención: Tiempo en que se tarda el contratista en establecer contacto con el Municipio de Envigado y empezar a establecer la causa del problema o incidente. En los casos de severidad 3 y 4 el tiempo en que se tarda en establecer la programación de las actividades.

Tiempo de Solución: Tiempo que se tarda el contratista en solucionar el caso o establecer el diagnóstico aceptado por el Municipio de Envigado a través de la Dirección de TIC en los casos en los cuales la solución del caso tarda más de 4 horas.

Requisitos Generales.

El proponente debe establecer y ofrecer una herramienta se seguimiento de los casos.

El cumplimiento de dicho servicio se evaluará con los informes mensuales, utilizando los siguientes criterios:
*Total incidentes escalados correctamente.
*Total incidentes que cumplen.
*Total incidentes que no cumplen.
*Porcentaje de cumplimiento.
Para obtener el porcentaje de cumplimiento se aplicara la siguiente formula:
(Incidentes que cumplen/total incidentes)*100%

Consultas pueden ser a través de llamadas telefónicas, correo electrónico y contar con una plataforma de tickets donde se pueda llevar registros de los casos.
Los requerimientos Alto y Urgente deben ser atendidos en sitio y por el ingeniero certificado en la plataforma que corresponda. Los requerimientos Medio se podrían solicitar a petición del Municipio de Envigado que sea en sitio, a consideración de esta.
El contratista deberá disponer de los recursos humanos y técnicos para la administración, gestión, solución en el sitio de los requerimientos.

Horario.

Lunes a Viernes	Sábado	Observaciones
7:00 a.m. a 7:00 p.m	8:00 a.m a 1:00 p.m.	Solo en caso de alguna eventualidad o despliegue programado que comprometa la operación del Municipio de Envigado, la disponibilidad deberá ser de 24 horas los 7 días de la semana.

La programación de actividades se realizará mínimo 4 horas previas en el horario arriba mencionado para los días de lunes a sábado y 48 horas previas para actividades en horario por fuera del cuadro arriba relacionado.

Si el caso reportado no se puede resolver a través de los servicios ofrecidos debido a que obedece fallas físicas o lógicas de fabricación, el contratista escalará el problema al fabricante o al distribuidor (vendedor de la infraestructura informática), mediante la apertura de un caso que dará solución al error. En este caso, se exime al proponente de cualquier nivel de servicio, ya que depende directamente del fabricante.

Niveles de Servicio.					
Nivel Severidad	Descripción	Tiempo de Atención	Tiempo de Solución	Medio de Apertura de caso	Tipos de Casos que aplican
Urgente	"Sistema Caído" o condición de producto inoperativo que afecta su sistema de producción y/o sus operaciones.	1 Horas	N/A	Celular por tipo de servicio.	Los que apliquen de acuerdo al sistema (hardware o software) que falle en cada caso.
Alto	Afecta y/o restringe severamente su funcionalidad, pero su sistema continúa productivo. Sistema parcialmente en funcionamiento	2 Horas	N/A	Celular por tipo de servicio. Correo electrónico	Los que apliquen de acuerdo al sistema (hardware o software) que falle en cada caso.
Medio	Problema menor que no tiene mayor efecto en las operaciones de negocio.	8 Horas	1 día hábil	Correo electrónico	Actualización de S.O. Actualización de Firmware Análisis de incidentes o problema recurrentes. Actividades que surjan de casos con severidad baja y que sean clasificados como severidad media. Mantenimiento preventivo
Bajo	Problema menor o consulta acerca de Documentación, Funcionalidad, buenas prácticas, análisis de la plataforma con el fin de hacer planes de mejora del producto, servicio o	Próximo día hábil	3 días hábiles	Correo electrónico, teléfono.	Reuniones estratégicas de Seguimiento. Pruebas de Concepto Visitas de Puesta a Punto o revisión de actividades.

	plataforma objeto del servicio.				

Equipo Mínimo de Trabajo.

El oferente debe contar con un equipo mínimo de trabajo para la ejecución del proyecto, el cual debe estar conformado como mínimo por:
Gerente del proyecto.
Un Ingeniero de Sistemas y/o Electrónico y/o Telecomunicaciones con especialización en Gerencia de Proyectos y certificaciones en PMP, quien deberá coordinar, supervisar, administrar y comunicar todas las tareas del proyecto de manera permanente. Mínimo 5 años de experiencia a partir de la expedición de la tarjeta profesional; dicho ingeniero deberá estar vinculado directamente con el oferente, para su verificación deberá presentar, según lo dispuesto por la Ley 842 de 2002 y la Ley 51 de 1986, diploma o acta de grado, copia de su tarjeta o matrícula profesional y certificado de vigencia expedido por la entidad competente. Adicional el oferente deberá presentar certificación laboral y planilla parafiscales.
Especialista en servicio de Red Inalámbrica.
Un (1) ingeniero o tecnólogo electrónico o de sistemas o afines, graduados, con matrícula profesional mínimo 2 años. Para su verificación deberá presentar, según lo dispuesto por la Ley 842 de 2002 y la Ley 51 de 1986, diploma o acta de grado, copia de su tarjeta o matrícula profesional y certificado de vigencia expedido por la entidad competente. El personal propuesto deberá realizar la función de instalación, configuración y puesta en marcha de la solución ofertada, y para garantizar su expertise en los productos ofertados los ingenieros deberán estar certificados por el fabricante en soluciones de Wireless y al menos deberá contar con los niveles de certificación Instalación y Configuración emitidos por marca, para lo cual deberán adjuntar el certificado vigentes del fabricante, con el fin de garantizar que el personal tiene los conocimientos sobre las últimas versiones, equipos y funcionalidades liberadas por el fabricante. El personal debe estar vinculado directamente con la empresa. Dicho profesional deberá estar vinculado directamente con el oferente, para su verificación deberá presentar, según lo dispuesto por la Ley 842 de 2002 y la Ley 51 de 1986, diploma o acta de grado, copia de su tarjeta o matrícula profesional y certificado de vigencia expedido por la entidad competente. Adicional el oferente deberá presentar certificación laboral y planilla parafiscales.
Especialista en servicio de Switching.
Un (1) ingeniero o tecnólogo electrónico o de sistemas o afines, graduados, con matrícula profesional mínimo 2 años. Para su verificación deberá presentar, según lo dispuesto por la Ley 842 de 2002 y la Ley 51 de 1986, diploma o acta de grado, copia de su tarjeta o matrícula profesional y certificado de vigencia expedido por la entidad competente. El personal propuesto deberá realizar la función de instalación, configuración y puesta en marcha de la solución ofertada, y para garantizar su expertise en los productos ofertados los ingenieros deberán estar certificados por el fabricante en soluciones de Switching y al menos deberá contar con los niveles de

certificación Instalación y Configuración emitidos por marca, para lo cual deberán adjuntar el certificado vigente del fabricante, con el fin de garantizar que el personal tiene los conocimientos sobre las últimas versiones, equipos y funcionalidades liberadas por el fabricante. El personal debe estar vinculado directamente con la empresa. Dicho profesional deberá estar vinculado directamente con el oferente, para su verificación deberá presentar, según lo dispuesto por la Ley 842 de 2002 y la Ley 51 de 1986, diploma o acta de grado, copia de su tarjeta o matrícula profesional y certificado de vigencia expedido por la entidad competente. Adicional el oferente deberá presentar certificación laboral y planilla parafiscales
GARANTÍA COMERCIAL O PRESUNTA
12 Meses.
NOMBRE DEL FUNCIONARIO QUE ELABORA
FELIPE JOSE BURGOS ORTEGA
FIRMA DEL SECRETARIO DE DESPACHO
LUIS FELIPE ROSSO RICAUTE