ANEXO - ESPECIFICACIONES Y CONDICIONES TÉCNICAS
Hoja No. 1
GENERALIDADES

	Descripción		
1	**REQUERIMIENTOS SUMINISTRO E INSTALACION DE DISPOSITIVOS LAN/WLAN - REQUISITOS HABITANTES**	**CUMPLE**	**DOCUMENTACIÓN**
1.1	Para garantizar la protección de inversión, alineación con las tendencias tecnológicas de la industria, soporte y vigencia tecnológica y estar preparados para los requerimientos futuros, los equipos de comunicación ofertados deben corresponder a una marca o fabricante que figure como líder en el cuadrante de Cuadrante Mágico Gartner para soluciones de acceso LAN Wired and Wireless durante al menos los últimos cinco años. Debe presentar el informe correspondiente a cada año.		
1.2	Dentro de las actividades a ejecutar por parte del contratista en sitio se contempla: El suministro, instalación, actualizaciones de versión, configuración y demás actividades requeridas que permitan la integración de los nuevos dispositivos y componentes a la solución LAN/WLAN de IMPRENTA NACIONAL DE COLOMBIA. Entregar la arquitectura final detallada de la solución Wifi operando y documentada.		
1.3	EL CONTRATISTA deberá validar previamente la topología y configuración de la red Wifi actual entregada por IMPRENTA NACIONAL DE COLOMBIA con el fin de presentar una propuesta de arquitectura detallada que garantice la correcta integración de los nuevos dispositivos y componentes de la solución LAN/WLAN a instalar. Este procedimiento deberá hacerse de mutuo acuerdo con el supervisor del contrato.		
1.4	Suministrar todos los elementos y accesorios necesarios para la instalación y puesta en funcionamiento de los dispositivos en las sedes de IMPRENTA NACIONAL DE COLOMBIA de acuerdo a la distribución del Anexo - Distribución de equipos. IMPRENTA NACIONAL DE COLOMBIA entregará cableados los puntos de red necesarios para la conexión a la red LAN/WLAN de los nuevos dispositivos.		
1.5	Coordinar con la IMPRENTA NACIONAL DE COLOMBIA las labores de entrega, instalación, actualización y demás requeridas para el aprovisionamiento de dispositivos objeto del contrato.		
1.6	Realizar entrega formal de los equipos y demás componentes de la solución LAN/WLAN instalados, actualizados y en correcto funcionamiento para verificación y visto bueno por parte de la supervisión del contrato o a quien este designe.		
1.7	El CONTRATISTA deberá suministrar los equipos y demás componentes de la arquitectura LAN/WLAN con la respectiva garantía y soporte del fabricante.		
1.8	La IMPRENTA NACIONAL DE COLOMBIA deberá contar con un contrato de soporte y atención de fallas en esquema 5X8 durante la vigencia del contrato directamente con el fabricante para equipos, software y platafomas de gestión y monitoreo, con el objetivo de atender cualquier anomalía que se pueda presentar, cumpliendo con los tiempos establecidos en el Anexo Técnico No. 2 - Acuerdos de Niveles de Servicio. En caso de requerirse la IMPRENTA NACIONAL DE COLOMBIA deberá poder abrir casos de soporte con el TAC del fabricante.		
1.9	El CONTRATISTA deberá entregar los dispositivos con las versiones de software actualizadas y de acuerdo a la arquitectura aprobada por IMPRENTA NACIONAL DE COLOMBIA.		
1.10	EL CONTRATISTA deberá suministrar y entregar en funcionamiento los componentes requeridos de acuerdo a la arquitectura de la solución LAN/WLAN aprobada. IMPRENTA NACIONAL DE COLOMBIA entregará las capacidades de cómputo en caso de ser requerido.		
1.11	EL CONTRATISTA debe proveer a IMPRENTA NACIONAL DE COLOMBIA los dispositivos y componentes requeridos de acuerdo a la hoja 2 del Anexo Técnico 1 - ESPECIFICACIONES TÉCNICAS DE LOS COMPONENTES LAN/WLAN de la los cuales deben ser nuevos y en óptimas condiciones de funcionamiento.		
1.12	Es responsabilidad del contratista que todos los componentes del servicio de la solución LAN/WLAN sean entregados funcionando correctamente y vinculados a la(s) plataforma(s) de gestión y monitoreo de la solución entregada.		
1.13	EL CONTRATISTA deberá garantizar que los equipos tengan configurado el protocolo IPv6 en la modalidad dual stack, cumpliendo la legislación vigente al respecto.		
1.14	Es responsabilidad del CONTRATISTA la adquisición, actualización y entrega del licenciamiento requerido para los elementos a suministrar de acuerdo al Anexo de Oferta Económica.		
1.15	Para la entrega e instalación de los dispositivos, EL CONTRATISTA deberá contar con el personal y servicios profesionales idóneos que considere pertinente, que le permitan garantizar el cumplimiento del objeto del contrato, en las condiciones técnica y de calidad definidas por la entidad sin generar costos adicionales para IMPRENTA NACIONAL DE COLOMBIA.		
1.16	El CONTRATISTA debe acreditar mediante certificación emitida por el fabricante de los equipos ofrecidos, donde informe la existencia de la representación de la marca y respaldo de repuestos y suministros en Colombia.		
1.17	El CONTRATISTA debe acreditar garantía técnica a la solución ofertada durante el tiempo de duración del contrato, mediante una certificación vigente emitida directamente por el fabricante de la solución.		
1.18	El contratista deberá entregar el modelo de administración que incluye el monitoreo, soporte y mantenimiento de la solución, los primeros treinta (30) días calendario posteriores al inicio de la etapa de operación del contrato, el cual deberá ser aprobado por IMPRENTA NACIONAL DE COLOMBIA.		
1.19	El contratista deberá entregar las herramientas necesarias para la ejecución de soporte de incidentes presentados sobre la solución.		
1.20	En caso de presentarse una falla de hardware, el CONTRATISTA deberá disponer de un equipo de reemplazo o los elementos necesarios para mantener el servicio mientras es gestionada la respectiva garantía cumpliendo con los ANS establecidos por IMPRENTA NACIONAL DE COLOMBIA. Las actividades de desmonte, transporte, instalación y demás requeridas serán asumidas por el contratista.		
1.21	El CONTRATISTA deberá realizar las actividades necesarias para la integración de componentes de la solución con otros sistemas de monitoreo, gestión, control y auditoría que tenga implementado la entidad. Todos los costos asociados con el desarrollo de esta labor, estarán a cargo del CONTRATISTA. (Ej: Envio de eventos al NOC, SOC, etc)		
1.22	El CONTRATISTA deberá mantener actualizada la integración de la solución control de acceso a la red NAC con el firewall de IMPRENTA NACIONAL DE COLOMBIA.		
1.23	El oferente deberá adjuntar con su propuesta la certificación que lo acredite al menos en uno de los últimos tres niveles de membresía de la marca ofertada y que cuenta con las condiciones aplicables a los servicios de instalación, soporte y mantenimiento de sus productos en el territorio Colombiano. Esto con el fin de garantizar que tanto la compañía como sus ingenieros cuentan con la experiencia y las competencias idóneas para la prestación del servicio requerido. Dicha certificación no debe ser superior a seis (6) meses. Adicionalmente, se debe presentar el documento de las membresías del fabricante o el enlace donde se pueda observar la información correspondiente.		
2	**REQUERIMIENTOS DE SOPORTE DEL SERVICIO**		
2.1	El contratista entregara actualizada la arquitectura y topología de red, y deberá hacer entrega actualizada del plano gráfico que describa la infraestructura de la solución y la documentación relacionada a la misma donde se detalle la configuración de cada uno de los equipos.		
2.2	En el caso de hacer mejoramiento al diseño y configuraciones actuales de la red LAN y WLAN, la IMPRENTA NACIONAL DE COLOMBIA acordara con el CONTRATISTA para la ejecución de este tipo de actividades. El CONTRATISTA deberá tener la autorización del supervisor del contrato y se acogerá al proceso de gestión del cambio establecido por IMPRENTA NACIONAL DE COLOMBIA.		
2.3	La solución de LAN/WLAN deberá contar con sistemas de monitoreo en línea que incluyan herramientas de automatización de tareas, analítica de datos e inteligencia artificial.		
2.4	EL CONTRATISTA deberá interactuar con la Oficina de Sistemas e Informatica de la IMPRENTA NACIONAL DE COLOMBIA, para dar solucion a los incidentes y requerimientos sobre el servicio de conectividad LAN/WLAN de IMPRENTA NACIONAL DE COLOMBIA.		
2.5	IMPRENTA NACIONAL DE COLOMBIA se reserva el derecho de verificar el pleno funcionamiento de toda la solución, para ello el CONTRATISTA deberá suministrar reportes mensuales del funcionamiento de toda la solución ante el supervisor de la entidad, los cuales deberán poder generarse en tiempo real, teniendo acceso a la generación de ellos.		
2.6	EL CONTRATISTA debe proporcionar y mantener actualizada durante la vigencia del contrato, una matriz de escalamiento que permita la rápida solución de temas relacionados con fallas de la infra estructura instalada.		
2.7	EL CONTRATISTA deberá cumplir con los tiempos de atención, diagnóstico y solución de incidentes indicados en el Anexo Técnico No. 2 - Acuerdos de Niveles de Servicios, para atender y dar solución a las fallas presentadas sobre la red que afecte el servicio de IMPRENTA NACIONAL DE COLOMBIA.		
2.8	Realizar el mantenimiento Preventivo: Un mantenimiento semestral durante la vigencia del contrato. El cronograma de mantenimiento deberá ser enviado por el CONTRATISTA dentro del primer trimestre del inicio de la operación. Debe ser aprobado por IMPRENTA NACIONAL DE COLOMBIA vía correo electrónico. El objetivo de estos mantenimientos será prevenir fallas causadas por daños físicos de los equipos y debe incluir: - Actualización de versión de firmware de los dispositivos de red. - Limpieza física de los equipos - Organización de patchcord de ser requerido		
2.9	Los mantenimientos preventivos y correctivos deberán cumplir los niveles de servicio solicitados y establecidos en el Anexo Técnico No. 2 - Acuerdos de Niveles de Servicio.		
3	**INFORMES Y REPORTES**		

3.1	Presentación mensual de informe de la gestión realizada y estadísticas de servicios recibidos y atendidos, esta debe entregarse los cinco (5) primeros días hábiles Estos informes deben tener como mínimo: • Casos escalados durante el mes, estados y tiempos, diagnostico y solución, cumplimiento a los ANS. • Estado de indicadores de los servicios provistos por el CONTRATISTA. (uso y adherencia de los servicios) • Tráfico cursado por las interfaces troncales de los equipos, uso de memoria y procesamiento de cada uno de los equipos. • Disponibilidad por equipo y total del servicio. • Capacidad por equipo y total del servicio. • Detalle de actividades ejecutadas durante el período. • Detalle de avance de los planes dispuestos y acciones de mejora • Recomendaciones y observaciones. • Informe técnico de estado de salud de la red. • Informe de facturación del servicio. • Detalle de las conexiones de usuarios a la red WLAN por SSID • Documentar de forma completa y clara, las actividades realizadas.		
3.2	Si se presenta algún tipo de indisponibilidad en el servicio se debe presentar un informe de falla de acuerdo a las indicaciones señaladas en el Anexo técnico No. 2 - Acuerdo de niveles de servicio.		
3.3	Presentación de informes después de cada maniobra, mantenimiento preventivo y/o correctivo sobre el servicio contratado por IMPRENTA NACIONAL DE COLOMBIA. Este informe debe tener como mínimo: • Las actividades realizadas. • Los problemas encontrados, la criticidad y la solución dada a cada uno. • Las recomendaciones y el plan de trabajo realizado		
4	**PERSONAL**		
4.1	El contratista debe cumplir con lo establecido en el Anexo Técnico No. 3 - Roles del Recurso Humano requerido.		
5	**ACUERDOS DE NIVELES DE SERVICIO**		
5.1	El contratista debe cumplir con lo establecido en el Anexo Técnico No. 2 - Acuerdos de Nivel de Servicio.		
6	**CUMPLIMIENTO LEGAL Y OTROS**		
6.1	El CONTRATISTA debe alinearse a las siguientes Normas, Estándares y Circulares Externas y buenas practicas vigentes: Norma ISO 27001:2022 Seguridad de la informacion, ciberseguridad y proteccion de la privacidad.		

ANEXO - ESPECIFICACIONES Y CONDICIONES TÉCNICAS
Hoja No. 2
ESPECIFICACIONES TÉCNICAS DE LOS COMPONENTES LAN-WLAN

ESPECIFICACIONES TECNICAS MINIMAS - REQUISITOS HABILITANTES

		CUMPLE	DOCUMENTACIÓN
1	**SISTEMA DE GESTIÓN**		
1.1	**CARACTERÍSTICAS GENERALES** - Su despliegue debe ser en nube y su licencia debe ser ofrecida como servicio/suscripción. - Debe ser capaz de gestionar y correlacionar eventos de la red inalámbrica y cableada (de la misma fábrica) - La solución de gestión debe ofrecer acceso a la administración de los dispositivos de red por consola web y no limitar el número de sesiones a la misma - Debe contar con una interface fácil de utilizar - La solución debe proveer información histórica con disponibilidad de al menos 1 mes de información - Deberá detectar posibles problemas que afecten el rendimiento de la red y ofrecer pistas sobre la causa raíz del problema para ayudar al administrador en la resolución (Operaciones asistida por IA) - Debe permitir a los usuarios buscar clientes, dispositivos e infraestructura conectada a la red, y la busqueda de documentación para ayudar a los usuarios a operar eficienteme sus redes. El motor de búsqueda debe utilizar lenguaje natural para analizar consultas y devolver resultados relevantes. - Deberá poder definir perfiles de acceso para distintos tipos de usuarios de tal manera que se puedan asignar distintos privilegios de acceso a cada una de las secciones o módulos de la consola. - En caso de perder conectividad hacia la plataforma de gestión los equipos de la red cableada e inalámbrica deben permitir su operación con la última configuración que recibierón de la nube.		
1.2	**MONITOREO** - La solución debe contar con una interface fácil de utilizar. - La solución debe mostrar información actualizada sobre el uso de la red y métricas de rendimiento de la misma. - Debe poder mostrar el mapa topológico, mostrando la interconexión de los dispositivos de red - Debe proveer vistas de red de cada dispositivo (por ejemplo, puntos de acceso, switches, etc) bajo su gestión. - En el caso de la red inalámbrica para cada dispositivo o radio se deberá contar cómo mínimo con información sobre la cantidad de dispositivos conectados, ancho de banda (bajada y subida), modelo y versión de software, utilización de canales, ruido, pérdidas, errores y retransmisiones, dirección IP, serie, y dirección MAC. - En el caso de la red cableada para cada dispositivo deberá contar cómo mínimo con información sobre modelo, serie, dirección MAC, dirección IP, versión de software, estado de puertos (estado, utilización de subida y bajada, vlans configuradas, información de paquetes unicast, multicas, broadcast, errores y descartes), PoE consumido y disponible, utilización de CPU y memoria, estado de ventiladores y fuentes. - Debe proveer información sobre los clientes inalámbricos y cableados conectados a los dispositivos de red gestionados como: - En el caso de los clientes inalámbricos se deberá mostrar como mínimo el nombre de usuario o hostname, dirección IP, MAC, vlan, estado (en línea, fuera de línea o fallido especificando el por qué) radio y canal de conexión inalámbrica, velocidad, throughput de subida y bajada. - En el caso de los clientes cableados se deberá mostrar como mínimo el nombre de usuario o hostname, dirección IP, MAC, vlan, puerto y switch al cual está conectado, throughput de subida y bajada.		
1.3	**DIAGNÓSTICO Y ALERTAS** - Debe permitir la habilitación y configuración de alertas - Las alertas deben poder ser categorizadas por severidad - Las alertas deben poder ser enviadas por correo electrónico - Las capacidades de solución de problemas incluyen eventos en vivo, captura de paquetes, registros y herramientas de línea de comando enriquecidas. También están disponibles comprobaciones de diagnóstico, como pruebas de ping y rutas de seguimiento, así como pruebas de rendimiento a nivel de dispositivo. - Debe ofrecer extensibilidad con otras plataformas y soluciones de TI a través de API y webhooks, para permitir por ejemplo, automatizaciones de red, interacción con herramientas de tiquetes, etc.		
1.4	**ADMINISTRACIÓN Y CONFIGURACIONES DE FIRMWARE** - La plataforma deberá poder hacer cambios de configuración en la infraestructura de red ya sea de manera global, por grupos de equipos o de manera específica a un dispositivo en particular. - Debe ser capaz de generar una plantilla de configuración o grupo de configuración. Este debe poder ser aplicada a uno o varios dispositivos de red. - Debe proporcionar el aprovisionamiento sin contacto permitiendo un flujo de trabajo simple e intuitivo para configurar los Puntos de Acceso, sin necesidad de participación de TI en el sitio. Los parámetros de configuración se pueden definir según los requisitos específicos de la red o del sitio. - Debe proveer información de auditoria para todos los cambios realizados en la red que incluya el nombre del usuario que hizo el cambio así como la fecha/horas y detalle del cambio. - Debe proveer la opción de actualizar el firmware de uno o más dispositivos a la vez de manera inmediata o programada. - Se debe poder definir versiones de firmware mínimas aceptables por tipo de equipamiento o grupo de dispositivos. - Debe indicar si es que hay una versión de firmware superior a la utilizada en los dispositivos. Asimismo, debe recomendar una versión de firmware por tipo de dispositivo.		
1.5	**SEGURIDAD** La solución debe estar implementada en datacenters que cumplan con las mejores prácticas de seguridad y operación que aseguren el cumplimiento de regulaciones y certificaciones como: SOC, PCI DSS, ISO 27001, GDPR.		
1.6	**REPORTES** - La solución deberá generar reportes. - Los reportes deberán poder generarse y enviarse vía correo electrónico de manera diaria, semanal o mensual. - Los reportes generados deberán poder ser exportados en formato pdf o csv		
1.7	**VIGENCIA** Al menos UN (1) año.		
2	**GENERALIDADES DE REQUERIMIENTOS TÉCNICOS DISPOSITIVOS LAN-WLAN**		
2.1	**CARÁCTERÍSTICAS ESPECIFICAS SWITCH ACCESO 48 PUERTOS No PoE**		
2.2	**Especificaciones técnicas** Switch Acceso, L2/L3		
2.3	**Puerto para Datos** - 48x - puertos 10/100/1000 Base-T - 4x - puertos 1G/10G SFP Todas las interfaces deben estar habilitadas, activas y listas para su uso. El proveedor deberá incluir todo el licenciamiento que el equipo requiera para cumplir esta condición.		
2.4	**Puertos para Administración** - 1 puerto serial de consola RJ45 - 1 puerto consola USB-C - 1 puerto Ethernet RJ45 para administración fuera de banda. - 1 USB para administración de archivos.		
2.5	**SFP+ 10GE incluidas** Incluir al menos (Por cada switch): - 2 transceivers SFP+ SR		
2.6	**Caracteristicas de Memoria** -Memoria: 8 GB DDR4, Flash: 16 GB eMMC; packet buffer : 8 MB -Switching 176 Gbps -Throughput 130 Mpps		
2.7	**Apilamiento** - Capacidad de conectarse en stack con otro switch de la misma familia de switches - Los equipos que son parte del cluster o stack deberán comportarse como un dispositivo virtual. - El cluster o stack debe ser capaz de crecer al menos hasta ocho (8) equipos (con otros de 24/48 puertos de la misma familia) - Soporte de ancho de banda de apilamiento 40 Gbps - Máxima distancia del apilamiento 10 kms - Proveer todo el hardware y software necesario para conectar los equipos mediante al menos dos (2) enlaces de 1m/3m a 10GE.		
2.8	**Sistemas Operativo** El sistema operativo debe incluir el licenciamiento de todos los puertos y características de servicio que el equipo pueda soportar.		
2.9	**Tamaño de tablas (L2)** Capacidad mínima de tabla MAC: ≥ 32K entradas por dispositivo lógico		
2.10	**VLANs (L2)** 4094 VLAN Ids		
2.11	**Tramas** soporte de jumbo frames con tamaño de trama L2 ≥ 9198 bytes y MTU IP configurable ≥ 1500		
2.12	**Spanning tree (L2)** - Spanning tree estándar IEEE 802.1D - Rapid STP IEEE 802.1w - Multiple STP (MSTP) IEEE 802.1s - Rapid Per-VLAN Spanning Tree (RPVST+)		
2.13	**Características (L2)** - IEEE 802.1v para aislamiento automático en VLANs de protocolos no IPv4 - MVRP aprendizaje automático y asignación dinámica de VLANs - VXLAN - IGMP para el manejo y control de multicast en capa 2 - QinQ para mejorar la utilización de las VLANs - IEEE 802.3ad LACP, soporte de 32 grupos (cada grupo con soporte de hasta 8 enlaces), grupos dinámicos o estáticos y selección del algoritmo de hashing - Multichassis Link aggregation (capacidad de agregación de enlaces en todos los switches del stack) - LLDP-MED - Configuración automática de VLAN para teléfonos IP		
2.14	**Performance (L3)** - 2048 entradas IPv4 - 1024 entradas IPv6 - 8192 entradas ARP		
2.15	**Protocolos (L3)** - ECMP Equal-Cost Multipath - Rutas estáticas IPv4/IPv6 - RIPv2, RIPng - OSPF, OSPFv2, OSPFv3 - Dual Stack IPv4/IPv6 - mDNS (Multicast Domain Name System)		
2.16	**Características (L3)** - ARP: estático, gratituous ARP, proxy ARP - DNS: cliente - DHCP: relay, server, cliente - Route maps para redistribución de rutas y modificación de métricas de enrutamiento		

2.17	**Multicast Listener Discovery** MLD para IPv6, v1 y v2		
2.18	**Protocol Independent Multicast (PIM)** - IGMP Snooping - PIM SM (Sparse Mode) - PIM SSM (Source-specific Multicast) - PIM DM (Dense Mode) - PIM para IPv4 e IPv6		
2.19	**Internet Group Management (IGMP)** IGMP v1, v2 y v3		
2.20	**Encolamiento** Al menos: - Strict Priority - Deficit WRR (DWRR)		
2.21	**Servicio** Al menos: - 802.1p - CoS utlizando dirección IP, Type of service, protocolo capa 3, puerto UDP/TCP, diffserv - IP SLA para monitoreo de VoIP		
2.22	**Autenticación para administración** Soporte de: - Radius - TACACS+ - local		
2.23	**Autenticación de usuarios** Soporte de: - Autenticación por dirección MAC - Radius - 802.1x - Autenticación basada en WEB desde portal cautivo externo. - Autenticación concurrente de los esquemas de autenticación IEEE 802.1X, web y MAC por puerto. - CoA (Change of Authorization)		
2.24	**Políticas basadas en roles** Integración con Sistema de Control de Acceso AAA para asignar políticas basada en el rol del usuario que se conecta, como ACL y VLAN.		
2.25	**Carácteristicas** Al menos: - Listas de acceso de control (ACL) soportadas en IPv4 e IPv6, para controlar el acceso no autorizado a la red y para controlar el tráfico. Las reglas niegan o permiten el tráfico y se pueden basar en los headers de capa 2 o capa 3. También proporcionan filtrado basado en los campos IP, subredes e IPs origen/destino, puertos TCP/UDP origen/destino sobre VLANs o puertos. - Protección de CPU ante tráfico malicioso que intente interrumpir el servicio del equipo - Limitación de tráfico ICMP de negación de servicio - Protección de BPDU STP en puertos que no se requiera este protocolo - Protección de STP root de ataques maliciosos o por errores de configuración - Protección dinámica de ARP para el bloqueo de ARP desde host no autorizados, evitando escuchas o robo de datos de la red. - Port security permite el acceso de direcciones MAC específicas, que pueden ser aprendidas o especificadas por el administrador - MAC address lockout evita que direcciones MAC configuradas específicas se conecten a la red. - DHCP snooping, ayuda evitar problemas causados por servidores DHCP no autorizados - Despliegue de banner de seguridad - RadSec para utilización del protocolo RADIUS de forma segura - Private VLAN (PVLAN) - Bloqueo dinámico de IP para bloquear el tráfico de hosts no autorizados y evitar la suplantación de direcciones IP de origen - Rol de autenticación crítico que garantiza que los dispositivos de infraestructura importantes, como los teléfonos IP, tengan acceso a la red incluso en ausencia de un servidor RADIUS. - Criptografía FIPS 140-2 - TPM (Trusted Platform Module) para asegurar la integridad de la plataforma		
2.26	**Alta disponibilidad** Al menos: - Capacidad de agregación de enlaces en todos los switches del stack (LACP) - Soporte de UDLD (Uni-directional Link Detection) para monitorear la conectividad del enlace y apagar puertos en ambos extremos si se detecta tráfico unidireccional, evitando loops en redes basadas en STP - Proporcionar imágenes flash duales de archivos independientes del sistema operativo primario y secundario.		
2.27	**Administración** - Capacidad de administración CLI, GUI, Nube. - CLI estándar de industria con una estructura jerárquica para reducir el tiempo y los gastos de capacitación. Ofrece mayor productividad en entornos de múltiples proveedores - Interfaz API REST integrada, programable y fácil de usar - Aprovisionamiento de día cero - sFlow (RFC 3176) - Restricción en comandos para configuraciones críticas, proporcionar múltiples niveles de privilegios con protección por contraseña, registro de acceso local y remoto por syslog. - TACACS+ proporciona autorización de acceso administrativo - SNMP (v2c/v3) , MIBs estándar y extensiones privadas - RMON - TFTP, SFTP, SSH - NTP - Almacenamiento de multiples archivos de configuración en memoria flash - Port mirroring para tráfico saliente y entrante; soportar hasta 4 grupos de mirror - Soportar un motor que automáticamente monitorea y analiza eventos que pueden impactar en la salud de la red. Este debe estar ubicado en el mismo switch para hacer análisis y monitoreo de eventos de manera distribuida.		
2.28	**Montaje** Debe traer todos los accesorios para montaje y operación en rack estándar de 19"		
2.29	**Alimentación eléctrica** Soporte al menos: - AC 100V-240V - 50 Hz/60 Hz.		
2.30	**Fuente de poder** Una fuente de poder Fija		
2.31	**Ventilación** Una ventilador fijo.		
2.32	**Medio ambiente** Cumplir al menos: - RoHS - WEEE - Soporte de IEEE 802.3az		
2.33	**Temperatura de operación** 0°C a 45°C hasta 5000 pies; reducir 1 °C por cada 1000 pies desde 5000 pies a 10 000 pies.		
2.34	**Humedad de operación** 5% a 95% non-condensing		
2.35	**Garantía limitada de por vida** - Duración de garantía EOS + 5 años - Vida útil limitada: la cobertura de la garantía se amplía solo durante el tiempo que el usuario final original de buena fe posea o haga uso del producto		
3	**CARÁCTERÍSTICAS ESPECIFICAS SWITCH ACCESO 24 PUERTOS No PoE**		
3.1	**Especificaciones técnicas** Switch Acceso, L2/L3		
3.2	**Puerto para Datos** - 24x - puertos 10/100/1000 Base-T - 4x - puertos 1G/10G SFP Todas las interfaces deben estar habilitadas, activas y listas para su uso. El proveedor deberá incluir todo el licenciamiento que el equipo requiera para cumplir esta condición.		
3.3	**Puertos para Administración** - 1 puerto serial de consola RJ45 - 1 puerto consola USB-C - 1 puerto Ethernet RJ45 para administración fuera de banda. - 1 USB para administración de archivos.		
3.4	**SFP+ 10GE incluidas** Incluir al menos (Por cada switch): - 2 transceivers SFP+ SR		
3.5	**Caracteristicas de Memoria** -Memoria: 8 GB DDR4, Flash: 16 GB eMMC; packet buffer : 8 MB -Switching 128 Gbps -Throughput 95 Mpps		
3.6	**Apilamiento** - Capacidad de conectarse en stack con otro switch de la misma familia de switches - Los equipos que son parte del cluster o stack deberán comportarse como un dispositivo virtual. - El cluster o stack debe ser capaz de crecer al menos hasta ocho (8) equipos (con otros de 24/48 puertos de la misma familia) - Soporte de ancho de banda de apilamiento 40 Gbps - Máxima distancia del apilamiento 10 kms - Proveer todo el hardware y software necesario para conectar los equipos mediante al menos dos (2) enlaces de 1m/3m a 10GE.		
3.7	**Sistemas Operativo** El sistema operativo debe incluir el licenciamiento de todos los puertos y características de servicio que el equipo pueda soportar.		
3.8	**Tamaño de tablas (L2)** Capacidad mínima de tabla MAC: ≥ 32K entradas por dispositivo lógico		
3.9	**VLANs (L2)** 4094 VLAN Ids		

3.10	**Tramas** soporte de jumbo frames con tamaño de trama L2 ≥ 9198 bytes y MTU IP configurable ≥ 1500		
3.11	**Spanning tree (L2)** - Spanning tree estándar IEEE 802.1D - Rapid STP IEEE 802.1w - Multiple STP (MSTP) IEEE 802.1s - Rapid Per-VLAN Spanning Tree (RPVST+)		
3.12	**Características (L2)** - IEEE 802.1v para aislamiento automático en VLANs de protocolos no IPv4 - MVRP aprendizaje automático y asignación dinámica de VLANs - VXLAN - IGMP para el manejo y control de multicast en capa 2 - QinQ para mejorar la utilización de las VLANs - IEEE 802.3ad LACP, soporte de 32 grupos (cada grupo con soporte de hasta 8 enlaces), grupos dinámicos o estáticos y selección del algoritmo de hashing - Multichassis Link aggregation (capacidad de agregación de enlaces en todos los switches del stack) - LLDP-MED - Configuración automática de VLAN para teléfonos IP		
3.13	**Performance (L3)** - 2048 entradas IPv4 - 1024 entradas IPv6 - 8192 entradas ARP		
3.14	**Protocolos (L3)** - ECMP Equal-Cost Multipath - Rutas estáticas IPv4/IPv6 - RIPv2, RIPng - OSPF, OSPFv2, OSPFv3 - Dual Stack IPv4/IPv6 - mDNS (Multicast Domain Name System)		
3.15	**Características (L3)** - ARP: estático, gratituous ARP, proxy ARP - DNS: cliente - DHCP: relay, server, cliente - Route maps para redistribución de rutas y modificación de métricas de enrutamiento		
3.16	**Multicast Listener Discovery** MLD para IPv6, v1 y v2		
3.17	**Protocol Independent Multicast (PIM)** - IGMP Snooping - PIM SM (Sparse Mode) - PIM SSM (Source-specific Multicast) - PIM DM (Dense Mode) - PIM para IPv4 e IPv6		
3.18	**Internet Group Management (IGMP)** IGMP v1, v2 y v3		
3.19	**Encolamiento** Al menos: - Strict Priority - Deficit WRR (DWRR)		
3.20	**Servicio** Al menos: - 802.1p - CoS utlizando dirección IP, Type of service, protocolo capa 3, puerto UDP/TCP, diffserv - IP SLA para monitoreo de VoIP		
3.21	**Autenticación para administración** Soporte de: - Radius - TACACS+ - local		
3.22	**Autenticación de usuarios** Soporte de: - Autenticación por dirección MAC - Radius - 802.1x - Autenticación basada en WEB desde portal cautivo externo. - Autenticación concurrente de los esquemas de autenticación IEEE 802.1X, web y MAC por puerto. - CoA (Change of Authorization)		
3.23	**Políticas basadas en roles** Integración con Sistema de Control de Acceso AAA para asignar políticas basada en el rol del usuario que se conecta, como ACL y VLAN.		
3.24	**Carácteristicas** Al menos: - Listas de acceso de control (ACL) soportadas en IPv4 e IPv6, para controlar el acceso no autorizado a la red y para controlar el tráfico. Las reglas niegan o permiten el tráfico y se pueden basar en los headers de capa 2 o capa 3. También proporcionan filtrado basado en los campos IP, subredes e IPs origen/destino, puertos TCP/UDP origen/destino sobre VLANs o puertos. - Protección de CPU ante tráfico malicioso que intente interrumpir el servicio del equipo - Limitación de tráfico ICMP de negación de servicio - Protección de BPDU STP en puertos que no se requiera este protocolo - Protección de STP root de ataques maliciosos o por errores de configuración - Protección dinámica de ARP para el bloqueo de ARP desde host no autorizados, evitando escuchas o robo de datos de la red. - Port security permite el acceso de direcciones MAC específicas, que pueden ser aprendidas o especificadas por el administrador - MAC address lockout evita que direcciones MAC configuradas específicas se conecten a la red. - DHCP snooping, ayuda evitar problemas causados por servidores DHCP no autorizados - Despliegue de banner de seguridad - RadSec para utilización del protocolo RADIUS de forma segura - Private VLAN (PVLAN) - Bloqueo dinámico de IP para bloquear el tráfico de hosts no autorizados y evitar la suplantación de direcciones IP de origen - Rol de autenticación crítico que garantiza que los dispositivos de infraestructura importantes, como los teléfonos IP, tengan acceso a la red incluso en ausencia de un servidor RADIUS. - Criptografía FIPS 140-2 - TPM (Trusted Platform Module) para asegurar la integridad de la plataforma		
3.25	**Alta disponibilidad** Al menos: - Capacidad de agregación de enlaces en todos los switches del stack (LACP) - Soporte de UDLD (Uni-directional Link Detection) para monitorear la conectividad del enlace y apagar puertos en ambos extremos si se detecta tráfico unidireccional, evitando loops en redes basadas en STP - Proporcionar imágenes flash duales de archivos independientes del sistema operativo primario y secundario.		
3.26	**Administración** - Capacidad de administración CLI, GUI, Nube. - CLI estándar de industria con una estructura jerárquica para reducir el tiempo y los gastos de capacitación. Ofrece mayor productividad en entornos de múltiples proveedores - Interfaz API REST integrada, programable y fácil de usar - Aprovisionamiento de día cero - sFlow (RFC 3176) - Restricción en comandos para configuraciones críticas, proporcionar múltiples niveles de privilegios con protección por contraseña, registro de acceso local y remoto por syslog. - TACACS+ proporciona autorización de acceso administrativo - SNMP (v2c/v3) , MIBs estándar y extensiones privadas - RMON - TFTP, SFTP, SSH - NTP - Almacenamiento de multiples archivos de configuración en memoria flash - Port mirroring para tráfico saliente y entrante; soportar hasta 4 grupos de mirror - Soportar un motor que automáticamente monitorea y analiza eventos que pueden impactar en la salud de la red. Este debe estar ubicado en el mismo switch para hacer análisis y monitoreo de eventos de manera distribuida.		
3.27	**Montaje** Debe traer todos los accesorios para montaje y operación en rack estándar de 19"		
3.28	**Alimentación eléctrica** Soporte al menos: - AC 100V-240V - 50 Hz/60 Hz.		
3.29	**Fuente de poder** Una fuente de poder Fija		
3.30	**Ventilación** Una ventilador fijo.		
3.31	**Medio ambiente** Cumplir al menos: - RoHS - WEEE - Soporte de IEEE 802.3az		
3.32	**Temperatura de operación** 0°C a 45°C hasta 5000 pies; reducir 1 °C por cada 1000 pies desde 5000 pies a 10 000 pies.		
3.33	**Humedad de operación** 5% a 95% non-condensing		
3.34	**Garantía limitada de por vida** - Duración de garantía EOS + 5 años - Vida útil limitada: la cobertura de la garantía se amplía solo durante el tiempo que el usuario final original de buena fe posea o haga uso del producto		

4	**ACCESS POINT (Interiores) Generalidades**		
4.1	La solución debe contar con Access Point de rendimiento para Wi-Fi 7 802.11be Bandas de operación: 2.4Ghz / 5GHz y 6GHz 2x2 en todos sus radios		
4.2	Se debe mantener activa la garantía y soporte de fábrica durante vigencia del contrato.		
4.3	**DESEMPEÑO** 2.4GHz - Hasta 344 Mbps 5 GHz - Hasta 1.44 Gbps 6 GHz - Hasta 2.88 Gbps Hasta 4.7 Gbps de forma agregada		
4.4	**CLIENTES CONCURRENTES** Soporta: - Hasta 512 clientes asociados por radios, y hasta 16 BSSIDs por radio		
4.5	**GANANCIA DE LAS ANTENAS** 2.4GHz - Al menos 5.1 dBi 5 GHz - Al menos 5.4 dBi 6 GHz - Al menos 5.4 dBi - Antena omnidireccional downtilt		
4.6	**INTERFACES** Incluye: - 1 x 1/2.5 Base-T con capacidad de soportar PoE 802.3 at - 1 puertos USB 2.0 - Indicadores visuales LED - Boton de re inicio - Consola serial - Slot de seguridad		
4.7	**CONECTIVIDAD WIRELESS** Tasas de Transmisión al menos de hasta: - 802.11b: 11 Mbps - 802.11a/g: 54 Mbps - 802.11n: 300 Mbps - 802.11ac: 867 Mbps - 802.11ax: 574 Mbps (2.4 GHz), 1201 Mbps (5 GHz), 2402 Mbps (6GHz).		
4.8	**SOPORTE DE TECNOLOGÍAS** - Soportar FTM 802.11mc/az para mejorar la presición en la ubicación de los clientes - El AP debe incluir radios ZigBee y Bluetooth para el soporte de iniciativas de transformación digital - Soportar integración con soluciones de NAC para simplificar el acceso de los usuarios a la red - Incluir soluciones de detección y prevención de amenezas inalámbricas WIDS/WIPS para identificar y resolver posibles errores o ataques en la red - Implementar mecanismos de seguridad y segmentación como VLANS, Roles o perfiles **FUNCIONALIDADES DE FIREWALL** - Incluir capacidades de filtrado de contenido L4-L7 - Visibilidad y control a través de Deep Packet Inspection (DPI) con el objetivo de clasificar, bloquear, priorizar o limitar ancho de banda de las aplicaciones. - Identificación de categoría de páginas Web. - Identificación de reputación de página Web.		
4.9	**ALIMENTACIÓN ELÉCTRICA** - El AP puede ser alimentado por un switch al menos con servicio PoE+ standard IEEE 802.3at - Se debe incluir un Power Injector 802.3at 30W como minimo, por cada Access Point.		
4.10	**SEGURIDAD FISICA** Al menos slot para candado estándar tipo Kensington.		
4.11	**CUMPLIMIENTO REGULATORIO** • FCC/ISED • CE Marked • Low Voltage Directive 2014/35/EU • UL/IEC/EN 62368 1 • EN60601 1 2		
4.12	**CERTIFICACIONES** • UL2043 plenum rating • Wi Fi Alliance (WFA): –Wi Fi CERTIFIED a, b, g, n, ac, 6, 7 –WPA2 y WPA3 – Enterprise, Personal, Enhanced Open (OWE) –WMM, W Fi Agile Multiband • Bluetooth SIG • Ethernet Alliance (PoE, PD device, class 4)		
4.13	**GARANTIA Y SERVICIO DIRECTO DEL FABRICANTE** Al menos TRES (3) años. La garantía de fábrica deberá incluir al menos: - Soporte telefónico. - Reemplazo de hardware. - Actualizaciones de software.		
4.14	**SERVICIOS PARA EL HW** - Garantía de por vida limitada		
5	**INTEGRACIÓN DEL SISTEMA DE CONTROL DE ACCESO NAC**		
5.1	Actualmente la IMPRENTA NACIONAL DE COLOMBIA cuenta con un sistema de control de acceso NAC (ClearPass) con una capacidad de 500 sesiones concurrentes (Access). Se requiere la integración de la LAN con el ClearPass para brindar un control de acceso seguro mediante visibilidad y automatización, incluyendo autenticaciones de tipo 802.1X, MAC AUTH, TACACS+, entre otros.		
5.2	Deberá incluir en el licenciamiento base los siguientes servicios: – 802.1X – Autenticación por MAC Address – Autenticación por portal cautivo y manejo de invitados – Múltiple Factor de Autenticación (MFA) – TACACS+ – Enforcement a través de SNMP – Perfilamiento de dispositivos – Integraciones con terceros mediante REST APIs		
5.3	La solución NAC debe identificar, clasificar y controlar (permitir o bloquear) y aislar dispositivos de la red, basado en políticas de acceso y soportando sistemas operativos Windows 8 o superiores, MAC OS, Unix, Linux, Windows Server. Debe soportar dispositivos móviles con sistema operativo Android, IOS, endpoints IoT, Multifuncionales, Impresoras, Teléfonos de VoIP entre otros.		
5.4	La solución debe contar con funcionalidades de servidor de escaneo propias y tendrá la posibilidad de integrarse con servidores externos de assessment.		
5.5	La política de seguridad deberá permitir tomar en consideración elementos contextuales como: horario, ubicación, tipo de dispositivo, versión de SO y nombre del dispositivo, entre otros.		
5.6	Debe soportar IPv6 (Dual Stack)		
5.7	Toda la comunicación interna de la solución debe ser segura o cifrada.		
5.8	Los dispositivos deben ser revisados para encontrar software no autorizado o servicios TCP no autorizados en la red.		
5.9	Los dispositivos que no cumplan con los requerimientos mínimos de acceso (definidos por la IMPRENTA NACIONAL DE COLOMBIA) serán direccionados a una VLAN de cuarentena.		
5.10	Debe permitir conectar a la red solamente los dispositivos autenticados/administrados .		
5.11	Deberá controlar el acceso de usuarios y dispositivos a través de la red cableada (switches).		
5.12	Deberá soportar la aplicación de políticas contextuales mediante servicios AAA: RADIUS, RADIUS CoA, TACACS+ y SNMP		
5.13	Deberá proveer la opción de autoregistro con confirmación de cuenta vía SMS o e-mail, para asegurar que los datos ingresados por los usuarios seran válidos.		
5.14	Deberá permitir que antes de que un usuario externo se pueda conectar, el acceso deba ser aprobado por un usuario corporativo (auto-registro con sponsor).		
5.15	Deberá permitir que la validez de las cuentas de invitados sea configurable en base a tiempo, anchos de banda utilizados, horario de conexión, entre otros.		
5.16	Deberá permitir la personalización del portal cautivo con logos, publicidad, videos, encuestas, etc.		
5.17	El portal deberá proporcionar un diseño que permita adaptarse a dispositivos fijos y móviles permitiendo una correcta visualización y una mejor experiencia de usuario.		
5.18	Deberá permitir la asignación de políticas de acceso basadas en roles, para poder asegurar anchos de banda, acceso a recursos específicos y duración de las conexiones, de acuerdo al tipo de invitado.		
5.19	Deberá permitir realizar Caching de direcciones MAC por cierta cantidad de tiempo, para evitar que los usuarios recurrentes tengan que introducir constantemente sus credenciales.		
5.20	Deberá permitir asignar accesos basados en roles a los operadores que crean o modifican las cuentas de usuarios.		
5.21	Las reglas de notificación de NAC podrán ser activadas por los eventos siguientes: · · Cuando un enpoint sea agregado o removido · Cuando el estatus de un endpoint cambie · Cuando el tipo de autenticación o un tipo de dispositivo cambie · Cuando se produzca un cambio en un grupo de usuarios · Cuando se produzca un cambio en un grupo de endpoints · Cuando en el registro un usuario o dispositivo sea agregado, actualizado o removido		
5.22	Se requiere que la solución aplique el control de acceso y segmentación dinámica basada en roles, para evitar el uso de múltiples VLANs para aplicar políticas de seguridad.		
5.23	Se requiere que la solución pueda perfilar y categorizar los dispositivos que se conectan a la red sin licenciamiento adicional.		
6	**OTROS**		
6.1	EL CONTRATISTA debe suministrar e instalar los equipos, los cuales deben cumplir las siguientes características: - Equipos NUEVOS, y no deben ser re-manufacturados, de marcas blancas, de última tecnología y en óptimas condiciones de funcionamiento. - Todos los dispositivos suministrados y en operacion no deben presentar estado "End of Sale" según información publicada por el fabricante en sus plataformas. para ello, EL CONTRATISTA debe anexar la constancia expedida por el fabricante. - Las CARACTERÍSTICAS de los dispositivos del presente anexo técnico son las mínimas solicitadas, monomarca y de uso corporativo.		

ANEXO - ESPECIFICACIONES Y CONDICIONES TÉCNICAS
Hoja No. 3
RENOVACIÓN DE SOPORTE SWITCH CORE - NAC

ESPECIFICACIONES TECNICAS MINIMAS

ITEM	Descripcion - modelo - producto	Numero parte/producto	Numero de serial	Cantidad	Nivel de servicio (minimo)
SWITCH CORE	Aruba 5412R zl2 Switch	J9822A	SG59G4B0FL	1	HPE Foundation Care 4H Exchange SVC
	Aruba 5400R 700W PoE+ zl2 PSU	J9828A	IN58G4D2CM	1	HPE Foundation Care 4H Exchange SVC
	Aruba 5400R 700W PoE+ zl2 PSU	J9828A	IN58G4D2H8	1	HPE Foundation Care 4H Exchange SVC
	Aruba 5400R zl2 Management Module	J9827A	SG57G4C1T2	1	HPE Foundation Care 4H Exchange SVC
NAC	HPE Aruba Networking ClearPass NAC Cx000V VM-Based Appliance License E-LTU	JZ399AAE	PRSW2402856728	1	Aruba 1Y FC SW
	HPE Aruba Networking ClearPass Access License 500 Concurrent Endpoints E-LTU	JZ401AAE	PRSW2402856729	1	Aruba 1Y FC SW

ANEXO - ESPECIFICACIONES Y CONDICIONES TÉCNICAS
Hoja No. 4
SERVICIOS PROFESIONALES

SERVICIOS PROFESIONALES REQUERIDOS - REQUISITOS HABILITANTES		
1	**INSTALACIÓN FÍSICA**	**CUMPLE**
1.1	Instalación física completa de los nuevos componentes de red, incluyendo: - 20 switches de borde nuevos. - 12 Access Points.	
1.2	Esta actividad deberá incluir montaje, conexión física, cableado estructurado (en caso de que aplique) y verificación de conectividad eléctrica y de red.	
2	**CONFIGURACIÓN Y PUESTA EN MARCHA**	
2.1	- 20 switches nuevos. - 1 switch CORE existente, el cual será revalidado, actualizado, optimizado y reconfigurado para integrarse con la nueva arquitectura. - 12 Access Points, incluyendo su integración a la consola de gestión.	
2.2	Configuración, integración y puesta en funcionamiento optimo, efectivo y eficiente con los dispositivos y elementos existentes en INC, como minimo mas no limitados a: Seguridad perimetral (Firewall PaloAlto V8.9), equipo(s) de enrutamiento de canal(es) dedicado(s) y de acceso a internet.	
2.3	Este servicio se deberá realizar tanto en horario hábil como no hábil, asegurando continuidad operativa y disponibilidad del equipo técnico.	
3	**ARQUITECTURA Y RECONFIGURACIÓN DEL NAC (CLEARPASS)**	
3.1	Como parte crítica de la operación segura de la red, se deberá realizar la revisión, actialización, rediseño y reconfiguración de la solución NAC ClearPass existente, con el objetivo de garantizar su integración fluida con la nueva infraestructura LAN/WLAN. Las actividades incluyen. Este conjunto de actividades permitirá a la organización consolidar su estrategia de Zero Trust y acceso por identidad, alineando la operación del NAC con la nueva red modernizada.	
3.3	•Revisión de la arquitectura actual (topología, servidores, roles, subsistemas activos). •Actualización y optimización de políticas de autenticación y autorización para redes cableadas. •Configuración de roles basados en identidad, tipo de dispositivo, grupo de AD, ubicación o perfil. •Integración de los nuevos switches y Access Points a la arquitectura ClearPass a través de RADIUS y Mac auth. •Aplicación de políticas de segmentación mediante VLAN assignment o rol asignado, con visibilidad unificada desde ClearPass Policy Manager. •Validación de la interoperabilidad con Active Directory y servicios de certificados (EAP-TLS, PEAP, etc.), según política de autenticación definida por la entidad. •Portal cautivo para la red de invitados, con formulario de autoregistro, sponsor. •Políticas de control de acceso para LAN/ WLAN como TACACS+, 802.1X. •Se debe garantizar la integración del NAC con los Firewall de la Entidad (Palo Alto) para extender las políticas de seguridad de los usuarios.	
4	**MANTENIMIENTO EN GABINETES DE COMUNICACIONES**	
4.1	Servicio de mantenimiento físico y lógico de gabinetes, que incluye: •Limpieza, organización y peinado del cableado. •Soplado y retiro de polvo. •Identificación y levantamiento de información de puertos y patch panel. •Mantenimiento de disipadores (Mantenimeinto de RACKS). •Patchcords de fibra óptica (3 de 5 m + 4 de 10 m). •Etiquetado profesional con estándar PANDUIT.	
4.2	Revisión y certificación de todos y cada uno de los enlaces de fibra óptica que llegan o salen del datacenter principal. •Enlaces hacia 14 Racks de Comunicaciones. •Certificación de cada uno de los enlaces de fibra óptica entre el datacenter y los 14 racks de comunicaciones distribuidos en la infraestructura. •Verificación de conectividad, pérdidas por empalmes o conectores, y estado físico del cableado. •Uso de conectores y adaptadores adecuados (LC, SC, MPO, según corresponda). •Generación de un reporte individual por cada Rack, documentando los resultados obtenidos y el estado de los enlaces certificados.	
4.3	Condiciones Generales •El servicio deberá ser ejecutado por personal técnico calificado, utilizando equipos de certificación calibrados y actualizados. •Se deben incluir etiquetas de identificación en cada extremo de los enlaces certificados, según estándar definido con PANDUIT.	
4.4	Cobertura: •13 racks + 1 rack de datacenter. •Horario: No habil de bajo impacto y/o previo acuerdo y programación entre las partes. •2 horas de soporte correctivo el siguiente día hábil, si es requerido. •El servicio debe incluir acciones correctivas, acorde al alcance del objeto contracual.	
5	**PUESTA EN MARCHA**	
5.1	•Desmonte de los equipos de reemplazo y ejecución de la organización del cableado que se encuentra conectado a los equipos actuales y que se deben migrar a los nuevos a adquirir. •Coordinar y ejecutar un site survey al iniciar el proyecto para evaluar los aspectos de cobertura y diseño de la ubicación de los Access Point; El contratista debe incluir una revisión de las ubicaciones de los acces point y modelar mediante un mapa de calor, la cobertura resultante. •Contar con el personal certificado por fabricante, en los equipos objeto de esta convocatoria, para la instalación, puesta en marcha y mantenimiento. •Realizar la entrega total de los dispositivos y partes de acuerdo con lo establecido en esta convocatoria. •Coordinar y ejecutar la visita técnica, con el objetivo de evaluar las condiciones de los Centros de Cableado y del Datacenter a intervenir para realizar las labores descritas anteriormente, así como también la ubicaciones de los Access Point en su sede principal. •El proveedor seleccionado deberá contar con el personal capacitado, en la ciudad de Bogotá por el fabricante para la instalación, puesta en marcha y mantenimiento de la base a instalar. •La Garantía de Fábrica para la renovación de soporte del Switch CORE debe ser mínimo de 3 años en modalidad 7x24 con tiempo de respuesta de 4 horas para el reemplazo de partes.	
6	**PLAN DE IMPLEMENTACIÓN**	
6.1	El plan de implementación del proyecto, el cual se debe realizar en un plazo máximo de treinta (30) días calendario (Instalación, configuración y puesta en marcha), debe ser acordado con La Imprenta Nacional de Colombia, con la premisa de no poner en riesgo los servicios actuales. Para el desarrollo de las actividades debe tener en cuenta: •Se deben especificar los tiempos y tareas necesarias para el Rollback. •Se podrán efectuar cambios en el cronograma de implementación, previo acuerdo con entre las partes (Imprenta Nacional de Colombia – Contratista). En el evento de retrasos en el programa inicial, atribuidos al contratista, este deberá suministrar todos los recursos técnicos y humanos necesarios para el cumplimiento de las fechas inicialmente pactadas. •Toda la instalación de la solución se deberá realizar siguiendo las mejores prácticas establecidas por el fabricante y serán ejecutadas por el contratista, siendo el responsable directo de los métodos utilizados. •Entregar al inicio del proyecto, todos los documentos que soporten los procedimientos para la implementación del sistema y los métodos que utilizara para la instalación de hardware y software. • Se debe tener en cuenta que, para la ejecución del proyecto, un porcentaje importante de actividades se debe realizar en horas de la noche o en la madrugada y fines de semana, para lo cual se debe garantizar disponibilidad de los integrantes del equipo del proyecto y los recursos técnicos que se necesiten para el cumplimiento de sus actividades, en los tiempos comprometidos. • Las actividades que requieran o generen indisponibilidades de cualquier servicio que se encuentre en producción o contingencia, deben ser ejecutadas los fines de semana, previa autorización de la Impren Nacional de Colombia. • Todas las configuraciones de equipos se realizarán bajo la supervisión de la Imprenta Nacional de Colombia y se garantizará que los nuevos equipos y software interactúan correctamente con la infraestructu actual. • La puesta en funcionamiento de equipos y software se realizará cumpliendo un set de pruebas previamente definido entre el contratista y la Imprenta Nacional de Colombia, donde estas deben est documentadas en una bitácora de seguimiento de los equipos puestos en producción. •La fecha y hora en la que se colocaran en producción será coordinada con la Imprenta Nacional de Colombia • El contratista definirá la mejor manera de configurar según su criterio, experiencia y recomendaciones del fabricante, los equipos especificados en esta oferta. Para esto debe tener en cuenta todos los factor necesarios para la configuración de los elementos adquiridos, con el fin de optimizar su desempeño.	
7	**CAPACITACIONES**	
7.1	•Capacitación Técnica Especializada Capacitación teórico - practica dictada por ingenieros certificados del partner en el fabricante ofertado, con foco en las soluciones LAN, WLAN y control de acceso (NAC) ofertadas. Detalles: •Duración: 15 horas (3 sesiones de 5 horas cada una). •Capacidad: Minimo 3 personas •Modalidad: Presencial o remota. •Contenido: •Arquitectura y operación de switching y WLAN. •Integración y políticas en plataforma NAC. •Visibilidad, segmentación y automatización. •Gestión centralizada desde la nube. •Casos de uso y prácticas guiadas sobre la plataforma instalada. Este entrenamiento está diseñado para fortalecer las competencias del personal TI de la entidad y garantizar el aprovechamiento completo de la solución implementada.	