ACTA DE REUNION

CONSECUTIVO ACTA	FECHA	HORA INICIO	HORA FINAL	LUGAR
008	07-may-2026	03:00 p.m.	04:00 pm	Reunión virtual Microsoft Teams

OBJETIVO DE LA REUNIÓN
Seguimiento a la ejecución de los contratos Nos. 45 y 47 de 2025 cuyo objeto es: INTERVENTORÍA TÉCNICA, ADMINISTRATIVA, FINANCIERA, JURÍDICA, CONTABLE Y AMBIENTAL DE LA COMPRA DE EQUIPOS ACTIVOS DE RED PARA SEDES DE LA RAMA JUDICIAL EN LA SECCIONAL POPAYÁN – CAUCA y LA COMPRA DE EQUIPOS ACTIVOS DE RED PARA SEDES DE LA RAMA JUDICIAL EN LA SECCIONAL POPAYÁN – CAUCA. ACLARACIÓN DE TEMAS RELACIONADOS CON LA CONFIGURACIÓN DE RED.

RESPONSABLES DE LA REUNIÓN	
NOMBRE	**CARGO/ ROL**
JOSÉ ALDEMAR PAZ HURTADO	SUPERVISOR CONTRATO

CONVOCADOS / ASISTENTES

NOMBRES Y APELLIDOS	DEPENDENCIA	ASISTIO LIDER		DELEGO	
		SI	NO	SI	NO
JOSÉ ALDEMAR PAZ HURTADO	SOPORTE TECNOLÓGICO DESAJ	X			
JUAN CARLOS ALARCÓN	CONTRATISTA M@ICROTEL	X			
LUIS FELIPE ALARCÓN	CONTRATISTA M@ICROTEL	X			
LEANDRO GONZALEZ	CONTRATISTA M@ICROTEL	X			
LUIS MORALES	CONTRATISTA M@ICROTEL	X			
DIEGO TOBAR	CONTRATISTA M@ICROTEL	X			
LUIS EDUARDO SANGUINO PARRA	CONTRATISTA M@ICROTEL	X			
MARÍA ALEJANDRA ARISTIZABAL	INTERVENTORÍA IYD	X			
GABRIEL BALCAZAR	INTERVENTORÍA IYD	X			
JAIME ALBERTO ARIAS	INTERVENTORÍA IYD	X			
JUAN CARLOS RUÍZ CHOCONTÁ	SOPORTE REDES DEAJ NIVEL CENTRAL	X			
DANIEL TORRES – TÉCNICO REDES	MESA DE SERVICIOS	X			

AGENDA

TEMA	JUSTIFICACIÓN	RESPONSABLE	TIEMPO ESTIMADO
1: Definición de		General	

requerimientos de red y permisos de seguridad			
2: Diseño de arquitectura lógica y segmentación de red		General	
3: Definición de topología, stacking y capacidad de los equipos		M@ICROTEL	
4: Implementación WiFi, cobertura y dimensionamiento		General	
5: Estrategia de implementación y gestión de cambios (RFC)		General	
6: Riesgos técnicos y operativos identificados		General	
7: Requisitos técnicos de la solución (plataforma y servidores)		General	
8: Seguridad, autenticación y control de acceso		General	

DESARROLLO DE LA REUNIÓN

1: Definición de requerimientos de red y permisos de seguridad

La reunión inicia con el objetivo de definir los requerimientos técnicos necesarios para habilitar la administración de los switches en la nube (Omnivista). Se establece que es imprescindible abrir puertos, dominios y protocolos específicos hacia Internet, los cuales deben ser gestionados por el área de seguridad y conectividad. Se indica que el contratista ya cuenta con un documento técnico que detalla estos requisitos (puertos HTTPS, rangos, FQDN, NTP, DNS, etc.), el cual debe ser remitido formalmente para su aprobación. Se aclara que estos accesos son necesarios para garantizar la correcta operación de la consola de administración en la nube.

2: Diseño de arquitectura lógica y segmentación de red

Se desarrolla una discusión técnica detallada sobre la segmentación de red, proponiendo una arquitectura basada en microsegmentación por sede y por tipo de dispositivo (switches y access points). Se plantea la creación de VLANs independientes

para gestión, usuarios y servicios (biométricos, cámaras, Wi-Fi). Se definen tamaños de red utilizando máscaras como /27, /28 y /24 dependiendo del volumen de dispositivos. Se concluye que para sedes principales se usarán segmentos más amplios para permitir crecimiento futuro. También se analiza la necesidad de crear VLANs específicas para los access points, especialmente en sedes como Canencio. Se acuerda que los segmentos Wi-Fi se diseñarán de forma independiente para evitar interferencias con la red LAN.

3: Definición de topología, stacking y capacidad de los equipos

Se analiza la topología propuesta para la implementación, destacando que la red estará compuesta principalmente por switches de acceso sin un core dedicado en algunas sedes. Se define el uso de stacking (chasis virtual) para agrupar switches, optimizando administración y disponibilidad. Sin embargo, se recomienda limitar el tamaño de los stacks (idealmente 3-5 equipos, máximo 7), debido a riesgos de desempeño y tiempos prolongados de reinicio. Cada stack compartirá una única IP de gestión, lo que optimiza la administración. También se revisa la topología en estrella basada en fibra óptica entre racks. Se valida la capacidad de los puertos uplink y la disponibilidad de enlaces. Se identifica que actualmente muchos enlaces están en cobre, lo que limita rendimiento futuro.

4: Implementación WiFi, cobertura y dimensionamiento

Se aborda el despliegue de la red inalámbrica, indicando la instalación de 12 access points distribuidos en varias sedes. Se detalla la distribución: 5 en Canencio, 2 en adolescentes, 2 en Silvia y otros en Santander. Se establece que en sedes principales (Palacios) no se instalarán nuevos APs dentro del contrato. Se discute la importancia de mapas de calor para garantizar cobertura adecuada, aunque solo se cuenta con estudios parciales. Se sugieren futuras ampliaciones como recomendación. También se analizan características técnicas de los APs (WiFi 6, 4x4 MIMO, hasta 3.5 Gbps).

5: Estrategia de implementación y gestión de cambios (RFC)

Se define que la instalación debe realizarse bajo un esquema controlado mediante RFC (gestión de cambios). Se establece que no se deben realizar desconexiones durante horario laboral para evitar afectaciones al servicio. Las migraciones reales de tráfico se realizarán en ventanas fuera de horario, preferiblemente fines de semana. Se permite avanzar con instalación física y configuración base antes de aprobación final. Se recomienda continuar actividades incluso si algunos permisos están pendientes. Se destaca que las interrupciones deben minimizarse y ser previamente autorizadas.

También se plantea actualizar el RFC con horarios reales (después de las 5 o 6 pm). Se resalta la importancia del comité de cambios en la aprobación final.

6: Riesgos técnicos y operativos identificados

Se identifican varios riesgos críticos que pueden afectar la implementación. El principal es la falta de energía en el Palacio Nacional, debido a fallas del proveedor eléctrico, lo cual detiene cualquier actividad técnica. También se menciona la caída de la planta eléctrica como agravante. Se reconoce incertidumbre en la fecha de restablecimiento del servicio. Se identifican riesgos de cobertura WiFi insuficiente. Además, se señala la posible afectación por cambios mal programados. Este punto demuestra una gestión activa de riesgos. Se establecen medidas de mitigación como planificación, pruebas y control de cambios.

7: Requisitos técnicos de la solución (plataforma y servidores)

Se detallan los requerimientos técnicos de la solución, incluyendo el uso de Omnivista Cirrus y un servidor local tipo collector (Ubuntu). Se especifica que la entidad debe proporcionar el hardware del servidor. Se definen requisitos mínimos (CPU, RAM, almacenamiento). Se detallan configuraciones de DHCP (opción 43), DNS, NTP y firewall. Se enfatiza el uso de HTTPS (puerto 443) para comunicación. También se describen puertos internos para gestión (SSH, logs, etc.). Se establece que la conectividad será por FQDN y no IP. Se destaca la simplicidad relativa de la solución. Se indica que la administración puede ser local y en nube.

8: Seguridad, autenticación y control de acceso

Se plantea la implementación de autenticación mediante RADIUS para controlar el acceso a la red, especialmente WiFi. El objetivo es restringir el acceso a usuarios institucionales y evitar conexiones externas no autorizadas. Se menciona la integración con directorio activo. También se analiza la posibilidad de implementar autenticación en LAN. Se reconoce que esta funcionalidad se implementará en fases posteriores. Se enfatiza la importancia de seguridad en redes inalámbricas. Se plantea evitar redes abiertas o sin control. También se recomienda segmentar adecuadamente por roles.

COMPROMISOS

N°	TEMA	RESPONSABLE	ENTREGA

1	Enviar documento (PDF) con puertos, dominios y requisitos	Contratista / Entidad	Inmediato
2	Gestionar apertura de puertos con seguridad y conectividad	Entidad	Inmediato
3	Actualizar RFC con nuevos horarios	Contratista / Entidad	Antes de ejecución
4	Validar mapas de calor y cobertura WiFi	Contratista	Durante implementación
5	Coordinar con comité de cambios aprobación final	Entidad / ITIL	Pendiente

En Constancia firma,

_____

JOSÉ ALDEMAR PAZ HURTADO
Supervisor



Anexos: SI() NO (X)
Elaboró: JPazH
Revisó: Miembros del Comité.