PLAN DE ADOPCIÓN E IMPLEMENTACIÓN DE IPv6
EMPOCABAL ESP–EICE
VERSIÓN 1.0
MAYO DE 2026

1. INTRODUCCIÓN

La Empresa de Obras Sanitarias de Santa Rosa de Cabal EMPOCABAL ESP–EICE, en el marco de su proceso de modernización tecnológica y fortalecimiento de la infraestructura informática institucional, formula el presente Plan de Adopción e Implementación de IPv6, con el propósito de garantizar la evolución tecnológica de la red institucional, mejorar la disponibilidad de servicios, fortalecer la seguridad informática y asegurar la compatibilidad con los estándares actuales y futuros de conectividad.

El agotamiento progresivo de direcciones IPv4 y los lineamientos establecidos por el Ministerio TIC impulsan a las entidades públicas y empresas prestadoras de servicios públicos a adoptar progresivamente el protocolo IPv6, garantizando interoperabilidad, escalabilidad y continuidad tecnológica.

Este documento establece el diagnóstico, estrategia, fases, requerimientos técnicos, lineamientos de seguridad, cronograma y recomendaciones necesarias para la transición gradual y controlada hacia IPv6 dentro de EMPOCABAL ESP–EICE.

2. OBJETIVO GENERAL

Definir la estrategia técnica, administrativa y operativa para la adopción progresiva del protocolo IPv6 en la infraestructura tecnológica de EMPOCABAL ESP–EICE, garantizando continuidad operativa, compatibilidad tecnológica, seguridad de la información y cumplimiento de lineamientos nacionales.

3. OBJETIVOS ESPECÍFICOS

1. Realizar diagnóstico de la infraestructura tecnológica actual.
2. Identificar activos compatibles e incompatibles con IPv6.
3. Diseñar esquema de direccionamiento IPv6 institucional.
4. Implementar un modelo de transición gradual.
5. Garantizar coexistencia IPv4/IPv6 durante el proceso.
6. Minimizar riesgos operativos y de conectividad.
7. Fortalecer la seguridad perimetral y segmentación de red.
8. Capacitar al personal técnico institucional.
9. Garantizar continuidad de servicios críticos.
10. Cumplir lineamientos de Gobierno Digital y MinTIC.

4. ALCANCE

El presente plan aplica para:

- Centro de datos institucional.
- Redes LAN y WLAN.
- Infraestructura de switching.
- Infraestructura de routing.
- Firewalls y seguridad perimetral.
- Sistemas de virtualización.
- Servidores físicos y virtuales.
- Servicios de correo electrónico.
- Hosting institucional.
- Servicios web.
- VPN institucional.
- Sistemas de monitoreo.
- Equipos de usuario final.
- Sistemas de respaldo y contingencia.
- Plataformas críticas institucionales.

5. MARCO NORMATIVO Y REFERENCIAL

Normatividad Nacional

- Ley 1341 de 2009.
- Decreto 1078 de 2015.
- Política de Gobierno Digital.
- Lineamientos MinTIC para adopción de IPv6.
- Modelo de Seguridad y Privacidad de la Información.

Referencias Técnicas

- RFC 8200 – Internet Protocol Version 6 (IPv6).
- RFC 4291 – IPv6 Addressing Architecture.
- RFC 4861 – Neighbor Discovery.
- RFC 4862 – Stateless Address Autoconfiguration.
- ISO 27001.
- Buenas prácticas Cisco, Mikrotik, Fortinet y VMware.

6. JUSTIFICACIÓN

La infraestructura tecnológica institucional de EMPOCABAL ESP–EICE ha venido evolucionando mediante procesos de transformación digital, fortalecimiento de servicios tecnológicos, virtualización, seguridad informática y modernización de plataformas.

Sin embargo, gran parte de la infraestructura actual opera principalmente sobre IPv4, protocolo que presenta limitaciones frente al crecimiento tecnológico, conectividad futura y disponibilidad de direcciones.

La adopción de IPv6 permitirá:

- Escalabilidad de direccionamiento.
- Mejor segmentación.
- Simplificación de NAT.
- Mejoras en rendimiento.
- Optimización de conectividad.
- Fortalecimiento de seguridad.
- Compatibilidad futura.
- Mejor interoperabilidad.
- Soporte para crecimiento institucional.
- Cumplimiento de lineamientos nacionales.

7. DIAGNÓSTICO INICIAL DE INFRAESTRUCTURA

7.1 Infraestructura Identificada

Centro de Datos

- Infraestructura virtualizada.
- Sistemas de respaldo.
- UPS.
- Servicios de almacenamiento.
- Segmentación lógica.

Servicios Críticos

- Correo electrónico institucional.
- Hosting institucional.
- Sistemas ERP.
- Plataformas financieras.
- Sistemas comerciales.
- Servicios web.
- VPN.
- Directorio activo.

Red Institucional

- Switching administrable.
- Segmentación VLAN.
- Enlaces internos.
- Redes inalámbricas.
- Firewall perimetral.

- Servicios DHCP y DNS.

Seguridad

- Firewall perimetral.
- Segmentación lógica.
- Control de acceso.
- Copias de seguridad.
- Monitoreo.

8. PRINCIPIOS DE IMPLEMENTACIÓN

La adopción de IPv6 deberá:

1. Ser gradual.
2. No afectar la operación institucional.
3. Mantener coexistencia IPv4/IPv6.
4. Priorizar servicios críticos.
5. Implementarse por fases.
6. Garantizar pruebas previas.
7. Mantener planes de reversa.
8. Garantizar seguridad informática.

9. MODELO DE TRANSICIÓN PROPUESTO

MODELO DUAL STACK

Se recomienda implementar inicialmente un esquema Dual Stack, permitiendo la coexistencia simultánea de IPv4 e IPv6.

Ventajas

- Menor impacto operativo.
- Compatibilidad progresiva.
- Menor riesgo.
- Facilidad de migración.
- Validación gradual.

10. FASES DEL PLAN

FASE 1 – INVENTARIO Y DIAGNÓSTICO

Actividades

1. Inventario de activos tecnológicos.
2. Identificación de compatibilidad IPv6.
3. Validación de firmware.
4. Identificación de sistemas críticos.
5. Revisión de proveedores ISP.

6. Identificación de riesgos.

Entregables

- Inventario tecnológico.
- Matriz de compatibilidad.
- Informe de riesgos.

FASE 2 – DISEÑO DE ARQUITECTURA IPv6

Actividades

1. Solicitud de prefijo IPv6 al ISP.
2. Diseño de direccionamiento.
3. Definición de VLAN IPv6.
4. Diseño de rutas.
5. Definición DNS.
6. Diseño de políticas firewall.

Entregables

- Plan de direccionamiento.
- Arquitectura lógica.
- Diseño de segmentación.

FASE 3 – ADECUACIÓN DE INFRAESTRUCTURA

Actividades

1. Actualización firmware.
2. Configuración switches.
3. Configuración routers.
4. Configuración firewall.
5. Configuración servidores.
6. Configuración virtualización.

Entregables

- Equipos habilitados.
- Configuraciones documentadas.

FASE 4 – IMPLEMENTACIÓN PILOTO

Alcance sugerido

- Área de sistemas.
- Segmento administrativo controlado.
- Laboratorio tecnológico.

Actividades

1. Activación Dual Stack.

2. Pruebas DNS.
3. Pruebas conectividad.
4. Validación servicios.
5. Monitoreo.

Entregables

- Informe piloto.
- Registro incidencias.
- Ajustes técnicos.

FASE 5 – IMPLEMENTACIÓN GRADUAL

Prioridades

1. Centro de datos.
2. Servicios críticos.
3. Áreas administrativas.
4. Redes inalámbricas.
5. Servicios externos.

Actividades

1. Habilitación progresiva.
2. Monitoreo continuo.
3. Validación rendimiento.
4. Ajustes seguridad.

FASE 6 – OPTIMIZACIÓN Y DOCUMENTACIÓN

Actividades

1. Actualización diagramas.
2. Actualización inventarios.
3. Ajustes políticas.
4. Auditoría técnica.
5. Capacitación final.

Entregables

- Documentación final.
- Manual operativo.
- Informe técnico.

11. COMPONENTES TÉCNICOS A VALIDAR

Networking

- Routers.
- Switches.

- VLAN.
- ACL.
- QoS.
- Routing dinámico.

Seguridad

- Firewall IPv6.
- IDS/IPS.
- VPN.
- Filtrado.
- Segmentación.
- Políticas acceso.

Sistemas

- Windows Server.
- Linux.
- VMware.
- Hyper-V.
- Active Directory.
- DNS.
- DHCPv6.

Aplicaciones

- ERP.
- Correo.
- Hosting.
- Servicios web.
- Sistemas internos.

12. ESQUEMA DE DIRECCIONAMIENTO PROPUESTO

Ejemplo Base

Prefijo asignado ISP:
2001:db8:1000::/48

Segmentación sugerida

Segmento	Prefijo
Centro de Datos	2001:db8:1000:1::/64
Administración	2001:db8:1000:2::/64
Sistemas	2001:db8:1000:3::/64
CCTV	2001:db8:1000:4::/64
WiFi Corporativo	2001:db8:1000:5::/64

Segmento	Prefijo
Invitados	2001:db8:1000:6::/64
VoIP	2001:db8:1000:7::/64
Gestión	2001:db8:1000:8::/64

13. SEGURIDAD EN IPv6

Riesgos

- Rogue RA.
- Túneles no autorizados.
- Exposición directa.
- Escaneo IPv6.
- Fallas de filtrado.

Controles

- RA Guard.
- DHCPv6 Guard.
- ACL IPv6.
- IDS/IPS.
- Segmentación.
- Hardening.
- Monitoreo.
- Logging.

14. CONTINUIDAD Y RESPALDO

Se deberán garantizar:

- Copias de seguridad.
- Configuración backup.
- Plan reversa.
- Alta disponibilidad.
- Recuperación rápida.

El esquema de custodia externa institucional deberá incluir configuraciones IPv6 críticas.

15. CAPACITACIÓN

Personal Objetivo

- Área de sistemas.
- Soporte técnico.
- Seguridad informática.
- Infraestructura.

Temas

- Fundamentos IPv6.
- Seguridad IPv6.
- Routing.
- DNS.
- Firewall.
- Troubleshooting.
- Monitoreo.

16. CRONOGRAMA PROPUESTO

Fase	Actividad	Tiempo
1	Diagnóstico	1 mes
2	Diseño	1 mes
3	Adecuación	2 meses
4	Piloto	1 mes
5	Implementación gradual	3 meses
6	Optimización	1 mes

Duración estimada total: 9 meses.

17. MATRIZ DE RIESGOS

Riesgo	Impacto	Mitigación
Equipos incompatibles	Alto	Actualización o reemplazo
Fallas conectividad	Alto	Dual Stack
Falta conocimiento técnico	Medio	Capacitación
Problemas DNS	Alto	Pruebas controladas
Fallas seguridad	Alto	Hardening y monitoreo

18. INDICADORES DE SEGUIMIENTO

Indicador	Meta
Equipos compatibles IPv6	>90%
Servicios habilitados Dual Stack	>80%
Incidentes críticos	0
Personal capacitado	100%
Documentación actualizada	100%

19. RECOMENDACIONES FINALES

1. Mantener esquema Dual Stack durante transición.
2. Priorizar seguridad perimetral.
3. Actualizar firmware permanentemente.
4. Implementar monitoreo IPv6.
5. Mantener documentación actualizada.
6. Realizar pruebas periódicas.
7. Mantener coordinación con ISP.
8. Integrar IPv6 al plan de continuidad institucional.

20. CONCLUSIONES

La adopción progresiva de IPv6 permitirá a EMPOCABAL ESP–EICE fortalecer su infraestructura tecnológica, garantizar escalabilidad futura, mejorar la interoperabilidad de servicios y alinearse con las políticas nacionales de transformación digital y modernización tecnológica.

La implementación propuesta bajo esquema Dual Stack minimiza riesgos operativos y permite una transición controlada, segura y gradual, garantizando la continuidad de los servicios institucionales y la protección de los activos tecnológicos de la Empresa.

ELABORADO POR

JOHN JAIRO CASTAÑEDA REINOSA
COORDINADOR DE SISTEMAS
EMPOCABAL ESP–EICE