

INFORME PLAN DE TRABAJO Y DESPLIEGUE IPV6 MEN

MINISTERIO DE EDUCACIÓN NACIONAL

PROYECTO OPERACIÓN GLOBAL SERVICIOS TICS



Bogotá, Mayo de 2021

Tabla de Contenido

1. INTRODUCCIÓN.....	4
2. OBJETIVOS	4
3. ALCANCE	5
4. ESTADO ACTUAL.....	5
4.1. ESTADO ACTUAL DE LA INFRAESTRUCTURA A NIVEL DE IPV6	5
4.2. DIAGNÓSTICO PLATAFORMA ACTUAL.....	18
5. ESTRATEGIA DE CUMPLIMIENTO	21
5.1. ESTRATEGIA PARA IMPLEMENTACIÓN DE IPV6 SISTEMAS	21
5.2. ESTRATEGIA PARA IMPLEMENTACIÓN DE IPV6 APLICACIONES	21
5.3. PRUEBAS DE FUNCIONALIDAD POR IMPLEMENTACIÓN IPV6.....	23
6. NO VIABILIDAD DE ADOPCIÓN IPV6	25
6.1. ESCRITORIOS VIRTUALES	25
6.2. APLICACIONES QUE NO SOPORTAN IPV6	25
7. CONCLUSIONES Y RECOMENDACIONES.....	26
7.1. CONCLUSIONES	26
8. REFERENCIAS	27
9. ACCIONES FUTURAS	27
10. ANEXOS	27

Índice de Ilustraciones

Ilustración 1. Configuración interfaces del Firewall CAN	10
Ilustración 2. Políticas del Firewall del CAN a nivel de IPV6.....	11
Ilustración 3. Interfaces WAF	11
Ilustración 4. Políticas de WAF.....	11
Ilustración 5. Bloqueos a nivel de ataques de denegación de servicio.	12
Ilustración 6. Configuración interfaces del Firewall.....	13
Ilustración 7. Políticas del Firewall del CAN a nivel de IPV6.....	13
Ilustración 8. Interfaces WAF	14
Ilustración 9. Políticas de WAF.....	14
Ilustración 10. Bloqueos a nivel de ataques de denegación de servicio	14
Ilustración 11. DNS configurados	15
Ilustración 12. Equipos de usuario final agregados en el dominio	15
Ilustración 13. Directorios activos.....	16
Ilustración 14. Arrendamiento de direcciones IP para los equipos de usuario final.....	16

Índice de Tablas

Tabla 1. Direccionamiento IPV6 Ministerio de Educación Nacional.....	5
Tabla 2. Direccionamiento LAN.....	6
Tabla 3. Direccionamiento servidores	6
Tabla 4. Tabla de vlan de switch distribución para sotano	6
Tabla 5. Direccionamiento de servidores DC externo.....	8
Tabla 6. Muestra de CI configurados en herramienta de monitoreo.	17
Tabla 7. Ítems lista de chequeo validación funcionamiento de IPv6	24

Índice de Gráficas

Gráfica 1 Soporte IPV6 Fabricante BD.....	18
Gráfica 2 Motores BD implementados en IPV6	19
Gráfica 3 Estados generales de implementación IPV6.....	19
Gráfica 4 Estado implementación de aplicaciones que soportan IPV6	20
Gráfica 5 Plan de implementación IPV6	22
Gráfica 6 Diagrama de Flujo implementación IPV6	22

1. INTRODUCCIÓN

Considerando el objetivo del Ministerio de Educación de liderar la formulación, implementación y evaluación de políticas públicas educativas, para cerrar las brechas que existen en la garantía del derecho a la educación, y en la prestación de un servicio educativo con calidad, además de la masiva conexión de dispositivos a internet y el agotamiento inminente de las direcciones IPV4, es importante garantizar el acceso a los servicios tecnológicos del MEN a través del protocolo IPV6.

Dentro de los servicios tecnológicos que son brindados por parte del MEN encontramos las aplicaciones y portales web, de las cuales es responsabilidad por parte de la UT Gestión Integral MEN realizar el despliegue del protocolo IPV6 sobre la infraestructura y aplicaciones, para lo cual es importante identificar el estado actual de su implementación, siendo considerados los componentes middleware, bases de datos, archivos de configuración entre otros, con el objetivo de definir la mejor estrategia a seguir para obtener exitosamente su apropiación.

En el actual documento se presenta el diagnóstico del estado actual de la plataforma de las aplicaciones del MEN, los servicios de con el cual se desea identificar, que aplicaciones no soportan actualmente su operación dual por los protocolos IPV4 e IPV6, que aplicaciones están pendientes por su implementación o no cuentan con su implementación totalmente.

Para ser llevado a cabo el diagnostico IPV6 a nivel de las aplicaciones fue realizada la evaluación de los siguientes ítems:

- Documento de su compatibilidad y/o implementación.
- Implementación IPV6 Capa Media.
- Resolución DNS por IPV6.
- Archivos de Configuración y Properties por Hostname.
- Implementación IPV6 en motores de Bases de Datos.

2. OBJETIVOS

Identificar el estado actual de implementación del protocolo IPV6 a nivel de las aplicaciones, bases de datos, infraestructura y seguridad; además de proponer las mejores estrategias y plan de trabajo acorde a las necesidades del Ministerio de Educación Nacional, con el fin de implementar el protocolo IPV6 para las aplicaciones candidatas según diagnóstico realizado son compatibles según lo componentes técnicos.

3. ALCANCE

Generar el diagnostico actual de la implementación IPV6 a nivel de los componentes middleware y bases de datos administrados por el frente de aplicaciones e infraestructura, siendo tomado el inventario de aplicaciones v76 y generar cronograma de implementación del protocolo IPV6.

4. ESTADO ACTUAL

4.1. ESTADO ACTUAL DE LA INFRAESTRUCTURA A NIVEL DE IPV6

En los siguientes capítulos se describe la red del Ministerio de Educación Nacional a nivel de IPV6, la cual se encuentra conformada por dos Datacenter Interno (denominado CAN) y externo. En el DC del CAN se cuenta con la red LAN para dar acceso a los funcionarios de manera alámbrica e inalámbrica. Este capítulo corresponde al capítulo 7.3 de la guía de MinTIC (Guía 1: Guía de Transición de IPv4 a IPv6 – MinTIC, febrero 2021).

4.1.1. NETWORKING

El Ministerio de Educación Nacional cuenta con dos pool de direcciones de IP v6, una por cada data center, los cuales, están asignados de la siguiente manera:

DESCRIPCIÓN	NETWORK
Pool Completo	2801:1e2::/44
Subnet A (CAN)	2801:1e2::/46
Subnet B (DC Externo)	2801:1e2:4::/46

Tabla 1. Direccionamiento IPV6 Ministerio de Educación Nacional.

4.1.1.1. CAN

Como se indicó al comienzo del capítulo, la red del CAN está compuesta por la red LAN y unos segmentos para la zona de servidores, distribuidos de la siguiente manera:

Segmentos red LAN

VLAN	Descripción	NETWORK IPV6
Vlan4	Red Wifi MEN	2801:1e2:2:4::0/64
Vlan6	Red wifi visitantes	2801:1e2:2:6::0/64
Vlan100	Sótano oriental	2801:1e2:2:100::0/64
Vlan105	Sótano occidental	2801:1e2:2:105::0/64
Vlan110	Primer piso oriental	2801:1e2:2:110::0/64
Vlan115	Primer piso occidental	2801:1e2:2:115::0/64

VLAN	Descripción	NETWORK IPV6
Vlan120	Segundo piso oriental	2801:1e2:2:120::0/64
Vlan125	Segundo piso occidental	2801:1e2:2:125::0/64
Vlan130	Tercer piso oriental	2801:1e2:2:130::0/64
Vlan135	Tercer piso occidental	2801:1e2:2:135::0/64
Vlan140	Cuarto piso oriental	2801:1e2:2:140::0/64
Vlan145	Cuarto piso occidental	2801:1e2:2:145::0/64
Vlan150	Quinto piso oriental	2801:1e2:2:150::0/64
Vlan155	Quinto piso occidental	2801:1e2:2:155::0/64
Vlan160	Sexto piso	2801:1e2:2:160::0/64

Tabla 2. Direcccionamiento LAN.

Segmentos Servidores

VLAN	Descripción	NETWORK IPV6
215	DMZ certificación 2	2801:1e2:1:214::1/64
210	DMZ producción	2801:1e2:1:210::1/64
211	DMZ certificación	2801:1e2:1:211::1/64
212	DMZ pruebas	2801:1e2:1:212::1/64
1025	Red de balanceo	2801:1e2:1:1025::1/64
1026	Red de WAF	2801:1e2:1:1026::1/64

Tabla 3. Direcccionamiento servidores

4.1.1.1.1. RED LAN

A continuación, se puede observar la implementación del direccionamiento IPV6 configurado en los switch de distribución:

VLAN	NETWORK IPV6	HSRP ACTIVE SW-A	HSRP STANBY SW-B	HSRP VIRTUAL
Vlan100	2801:1e2:2:100::0/64	2801:1e2:2:100::253/64	2801:1e2:2:100::254/64	2801:1e2:2:100::1/64
Vlan105	2801:1e2:2:105::0/64	2801:1e2:2:105::253/64	2801:1e2:2:105::254/64	2801:1e2:2:105::1/64

Tabla 4. Tabla de vlan de switch distribución para sótano

```
interface Vlan100
description VLAN_SOT_OR
ip address 10.1.100.253/24
ipv6 address 2801:1e2:2:100::253/64
ipv6 nd prefix 2801:1e2:2:100::/64 no-advertise
hsrp version 2
hsrp 100
authentication text P@ssw0rd
preempt
priority 150
ip 10.1.100.1
hsrp 100 ipv6
preempt
priority 150
ip 2801:1e2:2:100::1
ip dhcp relay address 192.168.30.220
ipv6 dhcp relay address 2801:1e2:1:210::220 |
```

Ilustración 1. Vlan de switch distribución para sótano

A continuación, se puede observar un equipo dentro de la red navegando por IPv6:

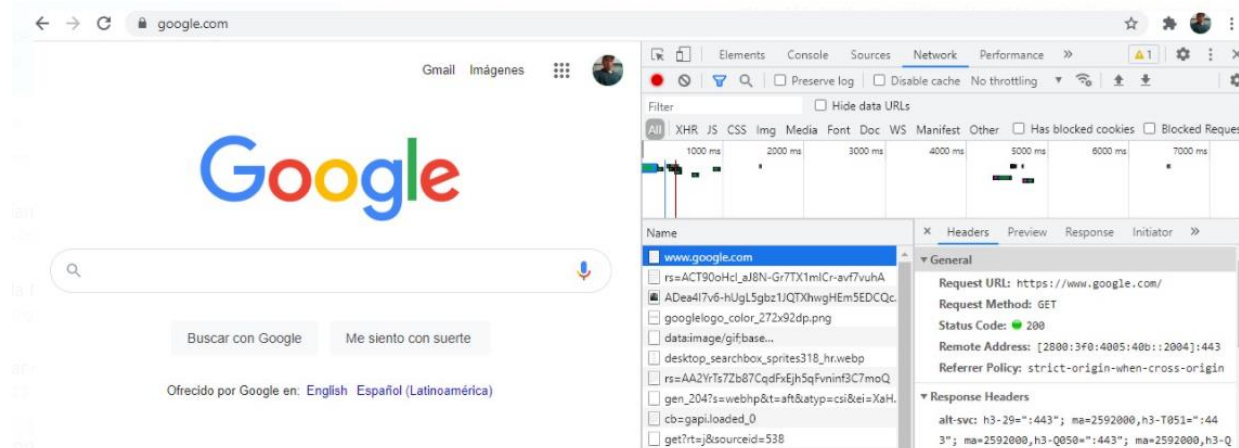


Ilustración 2. Navegando con IPv6



Ilustración 3. Validación de conectividad en Ipv6

4.1.1.1.2. RED DE SERVIDORES

A continuación, se muestra la evidencia de la implementación del direccionamiento IPV6 configurado en el equipo balanceador de tráfico:

Name	Type	Mode	IPv4	IPv6
210_self	vlan	static	192.168.30.253/24	2801:1e2:1:210::253/64
211_self	vlan	static	192.168.31.253/24	2801:1e2:1:211::253/64
212_self	vlan	static	192.168.32.253/24	2801:1e2:1:212::253/64
215_Self	vlan	static	192.168.215.253/23	2801:1e2:1:214::253/64
1025_self	vlan	static	10.200.100.253/23	2801:1e2:1:1025::3/64

Ilustración 4. Direccionamiento IPv6 sobre el ADC

4.1.1.2. DATACENTER EXTERNO

Para el caso de data center externo, la asignación de IPV6 se hizo con su par de IPV4, es decir por cada componente (canales de internet), quedando de la siguiente manera:

Segmentos Externo

VLAN	NETWORK IPV6
100	2801:1e2:4:100::0/64
101	2801:1e2:5:101::0/64
103	2801:1e2:5:103::0/64
104	2801:1e2:5:104::0/64
106	2801:1e2:5:106::0/64
200	2801:1e2:5:4200::0/64
201	2801:1e2:5:4201::0/64
208	2801:1e2:5:4208::0/64
281	2801:1e2:5:281::0/64
401	2801:1e2:5:4401::0/64
410	2801:1e2:5:4410::0/64
420	2801:1e2:5:4420::0/64
421	2801:1e2:5:4421::0/64
422	2801:1e2:5:422::0/64
430	2801:1e2:5:4430::0/64
431	2801:1e2:5:4431::0/64
750	2801:1e2:0:750::0/64
900	2801:1e2:1:214::0/64
901	2801:1e2:5:8000::0/50

Tabla 5. Direccionamiento de servidores DC externo.

4.1.1.2.1. CONFIGURACIÓN DE LOS DISPOSITIVOS

A continuación, se muestra la evidencia de la implementación del direccionamiento IPV6 configurado en el en el equipo balanceador de tráfico.

Name	Type	Mode	IPv4	IPv6
9_self	vlan	static	172.31.8.205/23	::/0
200_self	vlan	static	10.100.100.205/24	2801:1e2:5:4200::205/64
209_self	vlan	static	10.100.200.205/24	2801:1e2:5:4209::205/64
210_self	vlan	static	192.168.30.205/24	::/0
211_self	vlan	static	192.168.31.205/24	2801:1e2:1:211::205/64
401_self	vlan	static	10.100.120.205/24	2801:1e2:5:4401::205/64
405_self	vlan	static	10.100.110.205/24	::/0
410_self	vlan	static	10.125.10.205/24	2801:1e2:5:4410::205/64
420_self	vlan	static	10.40.2.205/24	2801:1e2:5:4420::205/64
421_self	vlan	static	10.40.4.205/24	2801:1e2:5:4421::205/64

Ilustración 5 Direcccionamiento IPv6 sobre el ADC

4.1.2. SEGURIDAD

La arquitectura de seguridad perimetral en data center es un espejo, esto con el fin de desarrollar una solución de DRP, sin embargo, la red del CAN por contar con una red LAN, dispone de tecnologías adicionales como son:

- **IDS**
- **Antispam**
- **Seguridad Perimetral**

4.1.2.1. CAN

4.1.2.1.1. IDS

La solución de IDS hace parte de la suite de identidades de Broadcom con el que se administra la identidad de los funcionarios del Ministerio de Educación. Sobre esta herramienta se administra el ciclo de vida de la identidad en su proceso de creación, modificación, inactivación y eliminación. Además, provee al usuario final un portal de autogestión de recuperación y cambio de contraseña. Actualmente no cuenta con configuración IPV6, está en proceso de implementación con el proveedor MSL.

4.1.2.1.2. ANTISPAM

Se cuenta con dos appliance Cisco para el análisis de correo. Estos dispositivos corresponden a un cluster de Email Security Appliance en donde se clasifican los correos entrantes para posterior entrega a los buzones del Ministerio. Allí, además de la clasificación que realiza el dispositivo para con los correos, se tienen también filtros de correos a bloquear personalizados, de acuerdo con las campañas SPAM que se van detectando en la red y los reportes que se van recibiendo por diferentes medios. También tiene una funcionalidad de relay de correo para aplicaciones que así lo requieren. Actualmente no cuenta con configuración IPV6.

4.1.2.1.3. SEGURIDAD PERIMETRAL

- **Firewall - FORTIGATE:** Dispositivo de Infraestructura de Seguridad con el que se controla el tráfico dirigido desde y hacia internet de la infraestructura del Ministerio de Educación, así como desde la LAN hacia las DMZs. En este se cuenta además con controles de IPS, Antivirus y Filtrado WEB. Sobre este dispositivo se encuentra configurado direccionamiento IPV4 e IPV6 y se replican los perfiles de seguridad sobre ambos protocolos.

	Name 🌐	Type 📁	IP/Netmask 📏	IPv6 Address 📏 📶
📁	Po_Ch	802.3ad Aggregate	0.0.0.0/0.0.0.0	::/0
•	ADC	VLAN	10.200.100.1/255.255.254.0	2801:1e2:1:1025::1/64
•	Vlan_240	VLAN	192.168.20.15/255.255.255.0	2801:1e2:0:240::2/64
•	Vlan_1022_WAN_2	VLAN	172.32.70.4/255.255.255.248	2801:1e2:0:1022::4/64
•	vlan_1023_WAN_1	VLAN	172.32.80.4/255.255.255.248	2801:1e2:0:1023::4/64
•	WAF	VLAN	10.200.150.1/255.255.254.0	2801:1e2:1:1026::1/64
📁	Po_Ch_DMZ	802.3ad Aggregate	0.0.0.0/0.0.0.0	::/0
•	certificacion_dos (DMZ_INT_2.1)	VLAN	192.168.214.1/255.255.254.0	2801:1e2:1:214::1/64
•	DMZ_INT	VLAN	192.168.30.1/255.255.255.0	2801:1e2:1:210::1/64
•	DMZ_INT_2	VLAN	192.168.31.2/255.255.255.0	2801:1e2:1:211::1/64
•	DMZ_INT_3	VLAN	192.168.32.2/255.255.255.0	2801:1e2:1:212::1/64
•	INTER_FW	VLAN	172.16.75.6/255.255.255.248	2801:1e2:0:750::1/64
•	VIRTUAL_DESKTOP	VLAN	10.1.164.1/255.255.254.0	2801:1e2:2:164::1/64

Ilustración 6. Configuración interfaces del Firewall CAN

From	To	Source	Destination Address	Schedule	Service	Action	Security Profiles
<input type="checkbox"/> WAN	<input type="checkbox"/> LAN	all	all	always	ALL	DENY	
<input type="checkbox"/> WAN	<input type="checkbox"/> DMZ_VIP	all	2801:1e2:1:1026::167	always	HTTP HTTPS	ACCEPT	default IPS_WINDOWS_IIS certificate-inspection
<input type="checkbox"/> WAN	<input type="checkbox"/> DMZ_VIP	all	2801:1e2:1:1026::155	always	HTTP HTTPS	ACCEPT	default Block_Critical_High_Medium certificate-inspection

Ilustración 7. Políticas del Firewall del CAN a nivel de IPV6

- **WAF - FortiWeb:** Dispositivo de Infraestructura de Seguridad con el que se protege a las publicaciones WEB realizadas por el Ministerio de Educación, controlando ataques como SQL Injection, Cross Site Scripting, Exploits conocidos, Troyanos, Ataques genéricos, Protección de Hostname, entre otros. Al igual que el firewall Fortigate, se cuenta con IPV4 e IPV6 para protección de las publicaciones sobre ambos protocolos.

	Name	Members	IPv4	IPv6
Aggregate (4)				
	Aggregate1	port1,port2	0.0.0.0/0	::/0
	Agg1-Vlan240		192.168.20.29/24	::/0
	WAF		10.200.150.2/23	2801:1e2:1:1026::2/64
	ADC		10.200.100.2/23	2801:1e2:1:1025::2/64

Ilustración 8. Interfaces WAF

Virtual Server	VIP	Port	Protocol	Protected Hostnames
VS_REST_SINEB_CERT	10.200.150.183/23	WAF	HTTP,HTTPS	VS_REST_SINEB_CERT
VS_REST_SINEB_CERT_IPV6	2801:1e2:1:1026::183/64	WAF	HTTP,HTTPS	VS_REST_SINEB_CERT

Ilustración 9. Políticas de WAF

- **AntiDDoS - FortiDDoS:** Este corresponde a un dispositivo de Infraestructura de Seguridad con el que se evitan ataques de denegación de servicios distribuidos desde Internet hacia la infraestructura del Ministerio de Educación. Dado que este equipo funciona de manera transparente, a este no se le asigna direccionamiento sobre las interfaces de operación, pero mediante los logs, se confirma análisis de tráfico IPV6.

Filter Setting			
SPP	Source IP Address	Protected IP Address	Associated Port
SPP-0	2801:1e2:0:1023::4	2800:3f0:4005:401::2003	443
SPP-0	2801:1e2:0:1023::4	2800:3f0:4005:407::200a	443
SPP-0	2801:1e2:0:1023::4	2620:1ec:c::11	443
SPP-0	2801:1e2:0:1023::4	2a03:2880:f22b:c5:face:b00c:0:167	443
SPP-0	2801:1e2:0:1023::4	2800:3f0:4005:401::200e	443
SPP-0	2801:1e2:0:1023::4	2607:f8b0:400c:c0a::bd	443
SPP-0	2801:1e2:0:1023::4	2603:1036:404:a2::2	443
SPP-0	2801:1e2:0:1023::4	2800:3f0:4005:408::200a	443

Ilustración 10. Bloqueos a nivel de ataques de denegación de servicio.

4.1.2.2. DATACENTER EXTERNO

- **Firewall - FORTIGATE:** Dispositivo de Infraestructura de Seguridad con el que se controla el tráfico dirigido desde y hacia internet de la infraestructura del Ministerio de Educación, así como desde la LAN hacía las DMZs. En este se cuenta además con controles de IPS, Antivirus y Filtrado WEB. Sobre este dispositivo se encuentra configurado direccionamiento IPV4 e IPV6 y se replican los perfiles de seguridad sobre ambos protocolos.

	Name	Type	Members	IP/Netmask	IPv6 Address
	port5	Physical Interface		0.0.0.0/0.0.0.0	::/0
	DMZ_1 (Port5-Vlan200)	VLAN		10.100.100.1/255.255.255.0	2801:1e2:5:4200::1/64
	EXCHANGE_2 (Port5-Vlan208)	VLAN		192.168.208.1/255.255.255.0	2801:1e2:5:4208::1/64
	INTERFW_FG_ASA	VLAN		172.16.75.1/255.255.255.248	2801:1e2:0:750::2/64
	MONTIC_BD (Port5-Vlan401)	VLAN		10.100.120.1/255.255.255.0	2801:1e2:5:4401::1/64
	Port5-Vlan901	VLAN		10.100.150.1/255.255.255.0	2801:1e2:5:8000::1/50
	PWMEN (Port5-Vlan410)	VLAN		10.125.10.1/255.255.255.0	2801:1e2:5:4410::1/64
	SIGSE_APP (Port5-Vlan421)	VLAN		10.40.4.1/255.255.255.0	2801:1e2:5:4421::1/64
	SIGSE_BD (Port5-Vlan422)	VLAN		10.40.5.1/255.255.255.0	2801:1e2:5:422::1/64
	SIGSE_HB (Port5-Vlan201)	VLAN		192.168.253.1/255.255.255.0	2801:1e2:5:4201::1/64
	SINECO_APP (Port5-Vlan430)	VLAN		192.168.55.1/255.255.255.0	2801:1e2:5:4430::1/64
	SINECO_BD (Port5-Vlan431)	VLAN		192.168.60.1/255.255.255.0	2801:1e2:5:4431::1/64
	WEB_HOSTING (Port5-Vlan420)	VLAN		10.40.2.1/255.255.255.0	2801:1e2:5:4420::1/64
	port7	Physical Interface		0.0.0.0/0.0.0.0	::/0
	WAN_1 (Port7-Vlan101)	VLAN		172.20.1.4/255.255.255.240	2801:1e2:5:101::4/64
	WAN_2 (Port7-Vlan103)	VLAN		172.20.1.52/255.255.255.248	2801:1e2:5:103::4/64
	port8	Physical Interface		0.0.0.0/0.0.0.0	::/0
	WAN_3 (Port8-Vlan104)	VLAN		172.20.1.60/255.255.255.248	2801:1e2:5:104::4/64
	WAN_4 (Port8-Vlan106)	VLAN		172.20.1.76/255.255.255.248	2801:1e2:5:106::4/64

Ilustración 11. Configuración interfaces del Firewall

From	To	Source	Destination Address	Schedule	Service	Action	Security Profiles
WAN	DMZ	all	2801:1e2:5:8104::133	always	HTTP HTTPS	ACCEPT	AV: AV_MEN2 IPS: IPS-LINUX_APACH... SSL: certificate-inspection
WAN	DMZ	all	2801:1e2:5:8281::19	always	HTTP HTTPS	ACCEPT	AV: AV_MEN2 IPS: IPS-LINUX_APACH... SSL: certificate-inspection

Ilustración 12. Políticas del Firewall del CAN a nivel de IPV6

- WAF - FortiWEB:** Dispositivo de Infraestructura de Seguridad con el que se protege a las publicaciones WEB realizadas por el Ministerio de Educación, controlando ataques como SQL Injection, Cross Site Scripting, Exploits conocidos, Troyanos, Ataques genéricos, Protección de Hostname, entre otros. Al igual que el firewall Fortigate, se cuenta con IPV4 e IPV6 para protección de las publicaciones sobre ambos protocolos.

	Name	Members	IPv4	IPv6
	port3		0.0.0.0/0	::/0
	MGTM		192.168.255.11/24	::/0
	DMZ		10.100.150.2/24	2801:1e2:5:8000::2/50
	DMZ1_SIGSE-SINE		10.100.100.10/24	2801:1e2:5:4200::3/64

Ilustración 13. Interfaces WAF

Virtual Server	VIP	Port	Protocol	Web Protection Profile	Protected Hostnames
vs_lb_minedubck_80	10.100.150.113/24	DMZ	HTTP,HTTPS	MINEDUCACION	MINEDUCACION
vs_lb_nuevoole_IPV6	2801:1e2:5:8104::143/64	DMZ	HTTP,HTTPS	MINEDUCACION	MINEDUCACION

Ilustración 14. Políticas de WAF

- **AntiDDoS - FortiDDoS:** Este corresponde a un dispositivo de Infraestructura de Seguridad con el que se evitan ataques de denegación de servicios distribuidos desde Internet hacia la infraestructura del Ministerio de Educación. Dado que este equipo funciona de manera transparente, a este no se le asigna direccionamiento sobre las interfaces de operación, pero mediante los logs, se confirma análisis de tráfico IPV6.

SPP	Source IP Address	Protected IP Address	Associated Port
SPP-0	2800:484:2483:3000:3c03:ce46:b61:26ad	2801:1e2:5:8104::143	443
SPP-0	2800:484:3b78:6980:ded:80c1:2697:f874	2801:1e2:5:8103::71	80
SPP-0	2806:102e:a:1c76:5caa:8ac0:b145:1559	2801:1e2:5:8104::143	443
SPP-0	2800:484:a184:cf00:4522:4f51:991c:fcd0	2801:1e2:5:8104::143	443
SPP-0	2800:484:2c90:4d00:5c85:648e:79b3:f663	2801:1e2:5:8104::143	443
SPP-0	2800:484:7285:ec00:1cdf:e043:d7d4:fc08	2801:1e2:5:8104::143	443
SPP-0	2800:484:9087:c700:cd1d:d3ef:1b84:39e7	2801:1e2:5:8104::143	443
SPP-0	2803:d100:e310:1a15:bdfc:bd76:fbf:45d2	2801:1e2:5:8104::143	443
SPP-0	2800:4b0:8035:ded8:f3bc:b747:e3db:300d	2801:1e2:5:8104::143	443

Ilustración 15. Bloqueos a nivel de ataques de denegación de servicio

4.1.3. SISTEMAS OPERATIVOS – SERVICIOS

4.1.3.1. DNS

A nivel del DNS interno se evidencian las zonas que se tienen actualmente configuradas, y su respectiva asignación de direccionamiento IPV6 para las aplicaciones y equipos del MEN.

DNS	Name	Type	Data	Timestamp
M1MENDC04	rpaprosocert	IPv6 Host (AAAA)	2801:01e2:0001:1026:0000:0000:0000:0156	static
Forward Lookup Zones	intranetmencert	IPv6 Host (AAAA)	2801:01e2:0001:1026:0000:0000:0000:0161	static
> _msdcs.minedu.gov.co	intranetmen	IPv6 Host (AAAA)	2801:01e2:0001:1026:0000:0000:0000:0167	static
> cna.gov.co	covidcert	IPv6 Host (AAAA)	2801:01e2:0001:1026:0000:0000:0000:0173	static
> colombiaaprende.edu.co	restsimat	IPv6 Host (AAAA)	2801:01e2:0001:1026:0000:0000:0000:0182	static
> men.co	restsineb	IPv6 Host (AAAA)	2801:01e2:0001:1026:0000:0000:0000:0183	static
> men.gov.co	encuestas	IPv6 Host (AAAA)	2801:01e2:0001:1026:0000:0000:0000:0185	static
> men.local	vumen1	IPv6 Host (AAAA)	2801:01e2:0001:1026:0000:0000:0000:0186	static
> minedu.gov.co	convalidacion	IPv6 Host (AAAA)	2801:01e2:0005:8103:0000:0000:0000:0071	static
> mineducacion.gov.co	saces	IPv6 Host (AAAA)	2801:01e2:0005:8103:0000:0000:0000:0081	static
> plandecenal.edu.co	convalidacionesbasica	IPv6 Host (AAAA)	2801:01e2:0005:8103:0000:0000:0000:0082	static
Reverse Lookup Zones	pae	IPv6 Host (AAAA)	2801:01e2:0005:8103:0000:0000:0000:0093	static
Trust Points	bi	IPv6 Host (AAAA)	2801:01e2:0005:8103:0000:0000:0000:0161	static
Conditional Forwarders	siucecert	IPv6 Host (AAAA)	2801:01e2:0005:8103:0000:0000:0000:0171	static
	vumen	IPv6 Host (AAAA)	2801:01e2:0005:8103:0000:0000:0000:0188	static
	appobseducit	IPv6 Host (AAAA)	2801:01e2:0005:8104:0000:0000:0000:0133	static
	obseducit	IPv6 Host (AAAA)	2801:01e2:0005:8104:0000:0000:0000:0133	static
	dialogoeducacionsuperior	IPv6 Host (AAAA)	2801:01e2:0005:8104:0000:0000:0000:0143	static
	ole	IPv6 Host (AAAA)	2801:01e2:0005:8104:0000:0000:0000:0143	static
	snies	IPv6 Host (AAAA)	2801:01e2:0005:8104:0000:0000:0000:0143	static
	www	IPv6 Host (AAAA)	2801:01e2:0005:8104:0000:0000:0000:0143	static
	cms	IPv6 Host (AAAA)	2801:01e2:0005:8104:0000:0000:0000:0221	static
	cooperativas	IPv6 Host (AAAA)	2801:01e2:0005:8106:0000:0000:0000:0085	static
	convocatoriasuperior	IPv6 Host (AAAA)	2801:01e2:0005:8106:0000:0000:0000:0230	static
	eventos	IPv6 Host (AAAA)	2801:01e2:0005:8106:0000:0000:0000:0230	static
	inmadrastica	IPv6 Host (AAAA)	2801:01e2:0005:8281:0000:0000:0000:0010	static

Ilustración 16. DNS configurados

DNS	Name	Type	Data	Timestamp
M1MENDC04	MEN314672	IPv6 Host (AAAA)	2801:01e2:0002:0145:fbdb9:c957:e94e:45c2	3/05/2021 12:00:00 p. m.
Forward Lookup Zones	MEN314676	IPv6 Host (AAAA)	2801:01e2:0002:0130:ad2d2:6dd2:4025:64...	14/04/2021 12:00:00 a. m.
> _msdcs.minedu.gov.co	MEN314680	IPv6 Host (AAAA)	2801:01e2:0002:0135:acbe8c71:6bb3:e9f0	24/07/2020 10:00:00 a. m.
> cna.gov.co	MEN314685	IPv6 Host (AAAA)	2800:0490:4001:8310:ff94:fc15:69ae:2730	13/11/2019 6:00:00 a. m.
> colombiaaprende.edu.co	MEN314686	IPv6 Host (AAAA)	2801:01e2:0002:0140:c765:eb0b:97a7:2607	12/05/2021 11:00:00 a. m.
> men.co	MEN314687	IPv6 Host (AAAA)	2800:0490:4001:8500:6003:c498:eb7d:07b5	24/09/2019 8:00:00 a. m.
> men.gov.co	MEN314688	IPv6 Host (AAAA)	2800:0490:4001:8110:ff9f:2adb:0daa:79ce	10/09/2019 4:00:00 p. m.
> men.local	MEN314690	IPv6 Host (AAAA)	2801:01e2:0002:0130:c267:261c:0716:f4f2	8/05/2021 3:00:00 p. m.
> minedu.gov.co	MEN314701	IPv6 Host (AAAA)	2801:01e2:0002:0130:ddcb:ab71:3acd:52...	19/04/2021 9:00:00 a. m.
> mineducacion.gov.co	MEN314797	IPv6 Host (AAAA)	2801:01e2:0002:0110:d1b3:9b61:d38b:44...	12/05/2021 6:00:00 p. m.
> plandecenal.edu.co	MEN315085	IPv6 Host (AAAA)	2801:01e2:0002:0120:b89c:0c78:2606:7ee8	18/06/2020 11:00:00 a. m.
Reverse Lookup Zones	MEN315087	IPv6 Host (AAAA)	2801:01e2:0002:0004:b8e9:0abc:bb6b:25...	24/01/2020 2:00:00 p. m.
Trust Points	MEN315090	IPv6 Host (AAAA)	2801:01e2:0002:0004:f0aa:6c6d:23d6:31e6	18/05/2020 1:00:00 p. m.
Conditional Forwarders	MEN315090	IPv6 Host (AAAA)	2801:01e2:0002:0004:e614:3036:0104:7cd7	18/05/2020 1:00:00 p. m.
	MEN315102	IPv6 Host (AAAA)	2801:01e2:0002:0004:f90f:37e9:a99c:6d7c	11/06/2020 8:00:00 a. m.
	MEN315111	IPv6 Host (AAAA)	2801:01e2:0002:0004:ce2a:f96a:33e7:bac1	13/03/2020 8:00:00 a. m.
	MEN315115	IPv6 Host (AAAA)	2801:01e2:0002:0004:abe5:9b96:965d:8c...	24/03/2020 1:00:00 a. m.
	MEN315116	IPv6 Host (AAAA)	2801:01e2:0002:0120:d07f:5d0f:54c5:0640	21/01/2021 3:00:00 p. m.
	MEN315126	IPv6 Host (AAAA)	2801:01e2:0002:0120:cbe5:bbfb:28fe:abce	19/05/2020 10:00:00 a. m.
	MEN315131	IPv6 Host (AAAA)	2801:01e2:0002:0004:c386:a3d2:99fc:2923	12/03/2020 9:00:00 a. m.
	MEN315142	IPv6 Host (AAAA)	2801:01e2:0002:0004:e4de:7cad:a9a6:7b40	11/02/2020 6:00:00 p. m.
	MEN315147	IPv6 Host (AAAA)	2801:01e2:0002:0004:e1d6:1f6f:3f9c:3267	7/03/2020 1:00:00 p. m.
	MEN315147	IPv6 Host (AAAA)	2801:01e2:0002:0004:d3f2:81f2:54a4:6baf	7/03/2020 1:00:00 p. m.
	MEN315227	IPv6 Host (AAAA)	2801:01e2:0002:0135:de14:f954:8ace:454e	13/05/2021 4:00:00 a. m.
	MEN315229	IPv6 Host (AAAA)	2801:01e2:0002:0130:c875:4f2a:6cf1:9375	15/09/2020 2:00:00 p. m.
	MEN315233	IPv6 Host (AAAA)	2801:01e2:0002:0150:d7a3:a8a0:3602:20c9	12/02/2021 8:00:00 a. m.

Ilustración 17. Equipos de usuario final agregados en el dominio

4.1.3.2. ACTIVE DIRECTORY

A nivel de la arquitectura de AD en producción, se evidencia la configuración que se tiene implementada a nivel de IPV4 e IPV6 para los Controladores de Dominio Locales.

Name servers:

Server Fully ...	IP Address
c1mendc01....	[10.22.3.4]
m1mendc01....	[192.168.208.12] [2801:1e2:5:4208::12]
m1mendc02....	[192.168.30.201] [2801:1e2:1:210::201]
m1mendc03....	[192.168.208.10] [2801:1e2:5:4208::10]
m1mendc04....	[192.168.30.200] [192.168.30.40] [2801:1e2:1:210::200]

Ilustración 18. Directorios activos

4.1.3.3. DHCP

A nivel del servidor DHCP, se evidencia la segmentación que se tiene implementada para IPV6 por cada VLAN, dicha distribución permite que el direccionamiento IP sea específicamente entregado en cada sector y nivel del Ministerio de Educación.

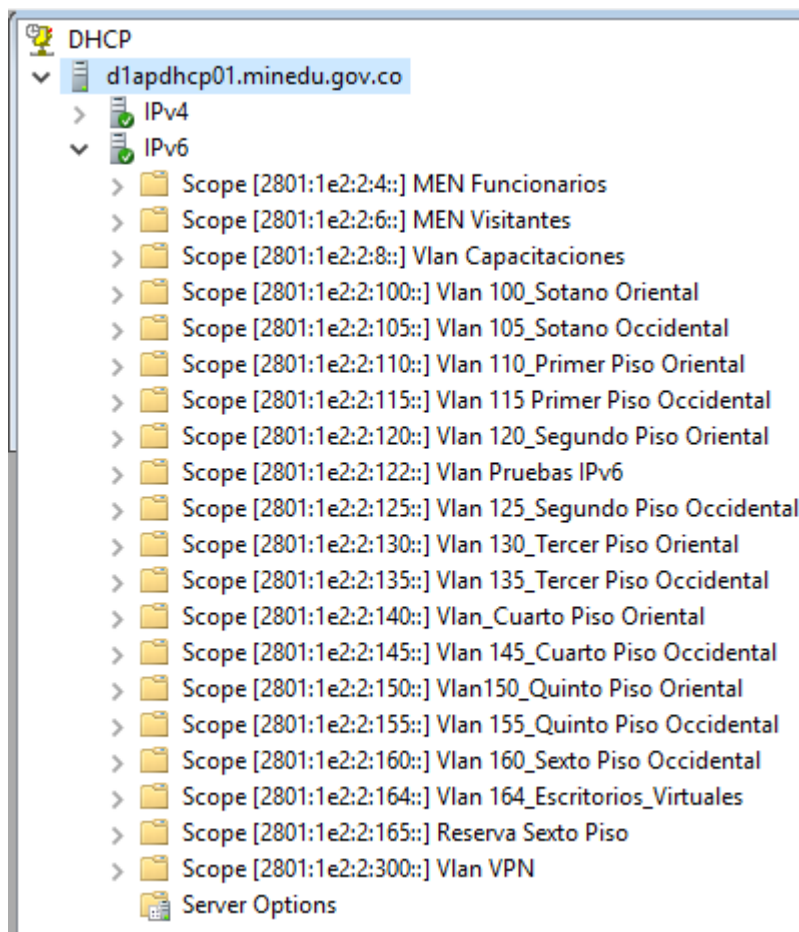


Ilustración 19. Arrendamiento de direcciones IP para los equipos de usuario final

4.1.4. APLICACIONES DE INFRAESTRUCTURA

El área de infraestructura cuenta con aplicaciones propias que dan los siguientes servicios:

- Mesa de servicios
- Monitoreo
- Comisiones

4.1.4.1. MESA DE SERVICIOS

El Ministerio de Educación Nacional cuenta con la plataforma de mesa de servicios de tecnología de CA, la cual en este momento se encuentra configurada con IPV4, ya que, la solución en la actualidad no es compatible con el protocolo IPV6, por esta razón se encuentra en un proceso de actualización con el proveedor MSL.

4.1.4.2. MONITOREO

El Ministerio cuenta con la plataforma de monitoreo llamada spectrum, la cual, tiene CI descubiertos por IPV6, se toma una muestra de estos elementos:

Condition	Name	Network Address IP v4	Manufacturer	Model Class	Address
Normal	NEXUS-A.minedu.gov.co	10.1.99.253	Cisco Systems, Inc.	Switch	2800:490:4001:8700::1
Normal	NEXUS-B.minedu.gov.co	10.1.99.254	Cisco Systems, Inc.	Switch	2800:490:4001:8700::3
Normal	O1APPBK01.minedu.gov.co	10.1.120.251	Microsoft	Workstation-Server	2801:1e2:2:120:bc6d:2f31:4a63:e67
Suppressed	OKI-MPS5502mb-AC6BD1	10.1.145.10		Printer	2801:1e2:2:145:eda3:f46:632b:d69e
Normal	N9K_A_CAN	10.8.1.2	Cisco Systems, Inc.	Switch	2801:1e2:2:164::253
Normal	m1appublicadornew01	10.125.10.34	net-snmp	Workstation-Server	2801:1e2:5:4410::34
Normal	m1apcmsv301	10.125.10.35	net-snmp	Workstation-Server	2801:1e2:5:4410::35
Minor	MEN_CAN_Ppal-Int_Bk-Datos	172.32.70.2	Cisco Systems, Inc.	Switch-Router	2800:490:4001:1001::2
Normal	MEN_CAN_Bk-Int_Ppal-Datos	172.32.70.3	Cisco Systems, Inc.	Switch-Router	2800:490:4001:1001::3
Maintenance	SW-MEN-4500.minedu.gov.co	192.168.20.1	Cisco Systems, Inc.	Switch-Router	2801:1e2:0:240::1
Normal	M1APRPA01.minedu.gov.co	192.168.30.36	Microsoft	Workstation-Server	2801:1e2:1:210::36
Normal	D1APCASPEC01.minedu.gov.co	192.168.30.63	Microsoft	Workstation-Server	2801:1e2:1:210::63
Normal	M1APSERVI01.minedu.gov.co	192.168.30.72	Microsoft	Workstation-Server	2801:1e2:1:210::72
Normal	M1APSERVI02.minedu.gov.co	192.168.30.73	Microsoft	Workstation-Server	2801:1e2:1:210::73
Normal	SP-WEBFRONT.minedu.gov.co	192.168.30.82	Microsoft	Workstation-Server	2801:1e2:1:210::82

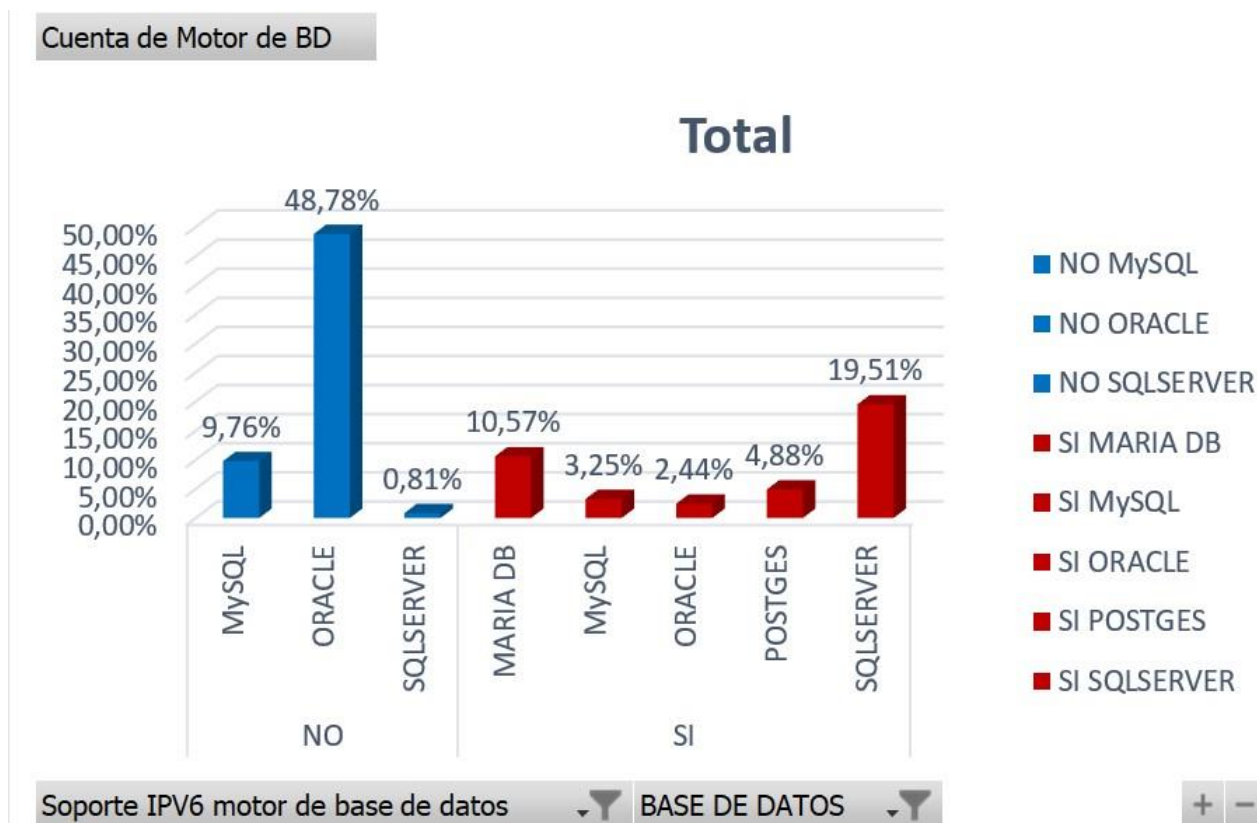
Tabla 6. Muestra de CI configurados en herramienta de monitoreo.

4.2. DIAGNÓSTICO PLATAFORMA ACTUAL

Este ítem hace referencia a la 7. Fases de transición y 7.1 Fase I. Planeación de IPv6 de la guía de MinTIC (Guía 1: Guía de Transición de IPv4 a IPv6 – MinTIC, febrero 2021).

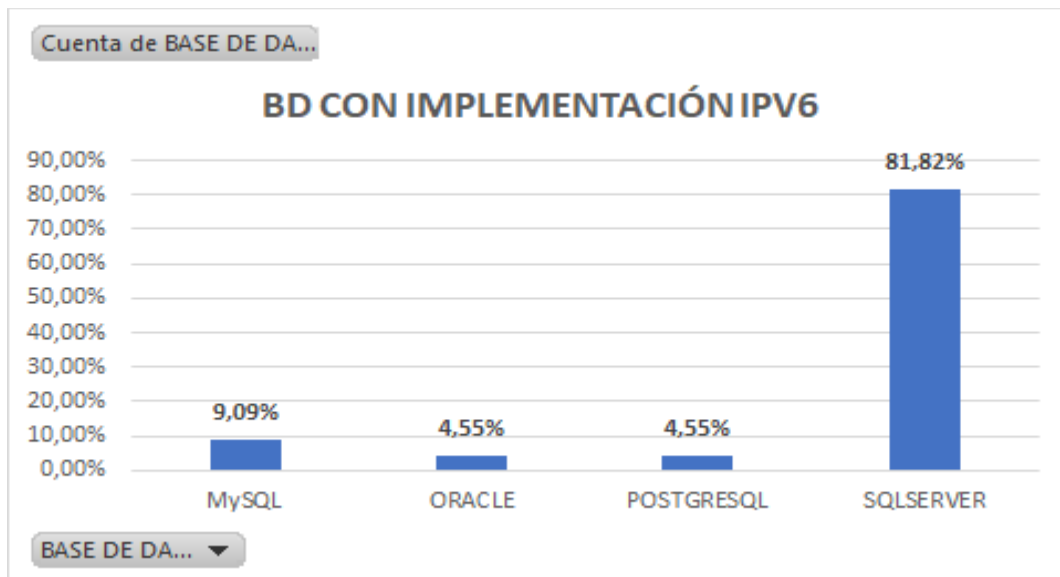
Se realiza análisis y diagnóstico sobre las aplicaciones del ministerio de Educación Nacional que están bajo la administración del operador UT Gestión Integral MEN, según versión del inventario de aplicaciones No 76.

Se realiza la tabulación de los diferentes motores de base de datos con los que cuenta actualmente el MEN describiendo su porcentaje, cantidad, tipo y factibilidad para implementar IPV6 considerando la compatibilidad de su versión del fabricante.



Gráfica 1 Soporte IPV6 Fabricante BD

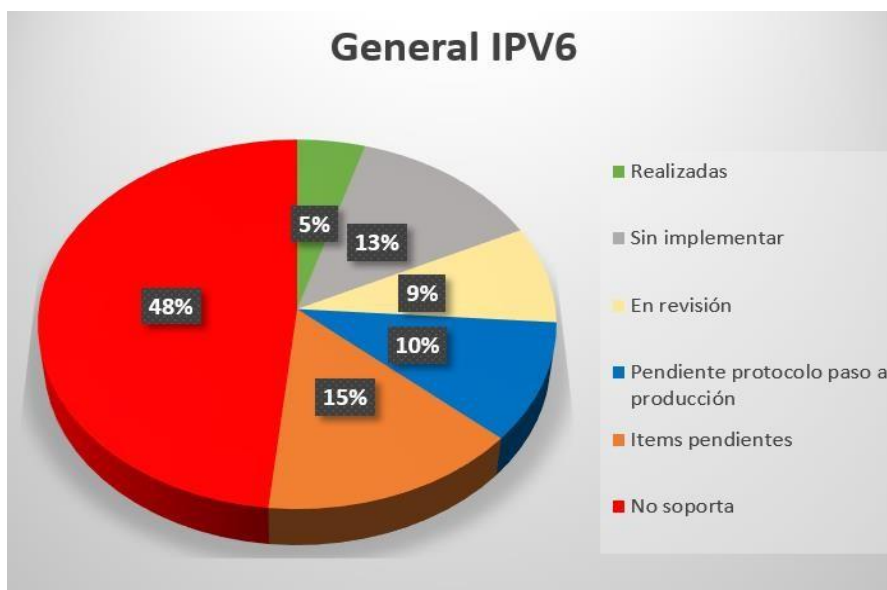
Dando alcance a la anterior gráfica se identifica que el 59.35 % de los motores de BD no soportan la implementación de IPV6, además de evidenciar que más del 95% de los motores de Base datos Oracle administrados no cuentan con compatibilidad para implementar IPV6.



Gráfica 2 Motores BD implementados en IPV6

De los motores que cuentan con IPV6 en su mayoría son Microsoft SQLServer, con un 81.82%, seguido por MySQL con 9.09%, Oracle con 4.55% y PostgreSQL con un 4.55%, bajo un total de 22 aplicaciones de las cuales sus motores de Bases de datos cuentan con la implementación del protocolo IPV6.

En el proceso de evaluación se identifican que setenta y cuatro (74) aplicaciones que no soportan la implementación de IPV6 y setenta y nueve (79) aplicaciones que soportan IPV6 o se encuentran en revisión, las cuales según su estado se organizan de la siguiente forma:



Gráfica 3 Estados generales de implementación IPV6

Los estados presentados en **Gráfica 3** corresponden a los siguientes:

Realizadas. Corresponde a las aplicaciones que cuenta con su implementación de protocolo IPV6 en su totalidad.

Sin Implementar. Hacen parte las aplicaciones a las cuales no se evidencia la implementación del protocolo IPV6 o sus ítems relevantes de capa media (Registro DNS ISP o DNS Interno MEN, archivos de configuración y string de conexión a bbdd) o bases de datos (Registro DNS y Configuración Motor Base de Datos) no fueron contemplados.

En Revisión. Pertenecen las aplicaciones que aunque su estado de compatibilidad es relacionado como **NO**, no cuenta con los soportes correspondientes a nivel de su documentación.

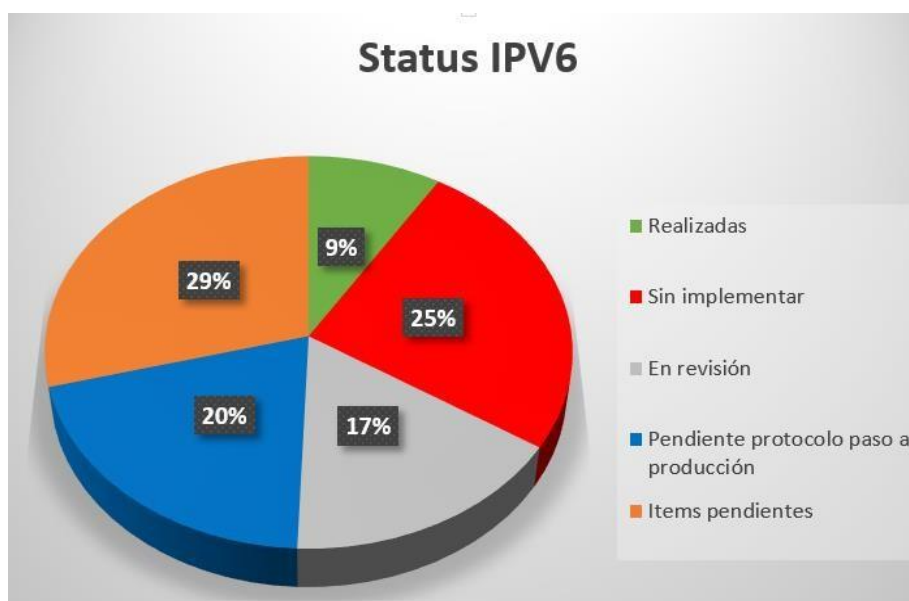
Pendiente Protocolo Paso a Producción. Corresponden las aplicaciones que se encuentran en estado de revisión de su protocolo paso a producción.

Ítems Pendientes. La implementación IPV6 de la aplicación no fue realizada en su totalidad.

No Soporta. La aplicación no es compatible con el protocolo IPV6 y cuenta con los soportes correspondientes.

Permitiendo identificar que el 48% de las aplicaciones no soportan IPV6, el 5 % se han implementado completamente, el 13% está sin implementar, el 9% está en revisión, el 10% está pendiente protocolo paso a producción y el 15 % se encuentran con ítems pendientes.

A partir de las aplicaciones que soportan IPV6 o se encuentran en validación se obtiene la siguiente gráfica:



Gráfica 4 Estado implementación de aplicaciones que soportan IPV6

En el estado Realizadas, se encuentran las aplicaciones que cuentan con IPV6 implementado, correspondiendo al 9 % de las aplicaciones, en el estado sin implementar están las aplicaciones que soportan IPV6, pero aún no se ha implementado y que corresponden al 25% del total, en el estado en revisión un 17% del total, en el estado de pendiente protocolo paso a producción el 20% del total, en el estado ítems pendientes se encuentran las aplicaciones que es necesario terminar de configurar sus parámetros para que se complete la apropiación del protocolo IPV6, las cuales son el 29 % de aplicaciones que soportan IPV6.

5. ESTRATEGIA DE CUMPLIMIENTO

5.1. ESTRATEGIA PARA IMPLEMENTACIÓN DE IPV6 SISTEMAS

Este ítem hace referencia a la 7.2 Fase II. Implementación del protocolo IPv6 de la guía de MinTIC (Guía 1: Guía de Transición de IPv4 a IPv6 – MinTIC, febrero 2021).

Las soluciones que se encuentran pendientes de implementación de IPV6 corresponden a sistemas de información implementados por el proveedor MSL, quienes en el momento se encuentran trabajando para realizar las correspondientes mejoras para que este producto acepte el nuevo protocolo.

Para el equipo antispam, el cual, no cuenta con IPV6 pero si lo soporta de acuerdo al siguiente reporte:

https://www.cisco.com/c/es_mx/support/docs/security/email-security-appliance/118519-ga-esa-00.html

Se realizarán las siguientes actividades

- Solicitar direccionamiento IPV6
- Configuración de direccionamiento
- Creación de registros SPF con la dirección IPV6 asignada
- Validación de salida de correos por medio de IPV6
- Creación de registros MX para entrada de correo mediante IPV6
- Configuración de políticas de Firewall para el acceso de tráfico SMTP

Cada actividad tendrá una duración de una semana a partir del 10 de Junio de 2021.

Se anexa el archivo de plan de trabajo establecido para dar cumplimiento a los sistemas que se encuentran pendientes de implementación. (**Anexo 1 PDT_IPV6_v311052021**)

5.2. ESTRATEGIA PARA IMPLEMENTACIÓN DE IPV6 APLICACIONES

Este ítem hace referencia a la 7.2 Fase II. Implementación del protocolo IPv6 de la guía de MinTIC (Guía 1: Guía de Transición de IPv4 a IPv6 – MinTIC, febrero 2021).

La estrategia propuesta para garantizar la completitud de implementación del protocolo IPV6 es la ejecución y cumplimiento de las siguientes fases:

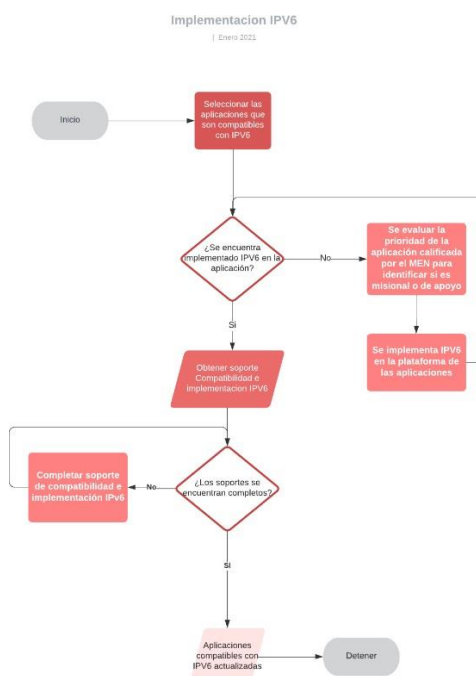
- Identificación y documentación del estado de compatibilidad IPV6 de las plataformas o aplicaciones del MEN que se encuentran en estado no soporta y en revisión.
- Completar la instalación IPV6 a nivel de las aplicaciones que tienen ítems pendientes siendo consideradas inicialmente aplicaciones misionales.
- Completar la instalación IPV6 a nivel de las aplicaciones que tienen ítems pendientes y corresponden a aplicaciones de apoyo.
- Implementar IPV6 a nivel de aplicaciones las aplicaciones que aún no cuentan con ella.

Servicio	Plan implementación IPv6	Detalle de Actividades	Responsable	Febrero				Marzo				Abril				Mayo			
				Sem 1	Sem 2	Sem 3	Sem 4	Sem 1	Sem 2	Sem 3	Sem 4	Sem 1	Sem 2	Sem 3	Sem 4	Sem 1	Sem 2	Sem 3	Sem 4
Gestión de Aplicaciones	Identificación y documentación del estado de compatibilidad IPv6 de las plataformas o aplicaciones del MEN que se encuentran en estado no soporte y en revisión.	Se revisan las condiciones con las que cuenta cada plataforma, ya que es necesario conocer las condiciones en las que se encuentran, esto con el fin de evaluar en cada aplicación si es posible implementar IPv6. A nivel de Base de datos se necesita identificar que motores de Base de datos soporta IPv6, adicionalmente se confirman los soportes que relacionan la compatibilidad e implementación IPv6 en la Hoja de vida de cada plataforma.	Especialistas de Aplicaciones / Líder Gestor de Aplicaciones																
	Identificación y documentación del estado de compatibilidad IPv6 de las plataformas o aplicaciones del MEN que se encuentran en estado no soporte y en revisión.	A partir de la evaluación realizada a las plataformas para identificar el estado con que cuentan en su implementación de IPv6 se identifican las aplicaciones que son compatibles con esta migración y que entre sus parámetros ya se encuentran configurados algunos ítems.	Especialistas de Aplicaciones / Líder Gestor de Aplicaciones																
	Identificación y documentación del estado de compatibilidad IPv6 de las plataformas o aplicaciones del MEN que se encuentran en estado no soporte y en revisión.	A partir de la evaluación realizada a las plataformas para identificar el estado con que cuentan en su implementación de IPv6 se identifican las aplicaciones que son compatibles con esta migración y que entre sus parámetros ya se encuentran configurados algunos ítems.	Especialistas de Aplicaciones / Líder Gestor de Aplicaciones																
	Identificación y documentación del estado de compatibilidad IPv6 de las plataformas o aplicaciones del MEN que se encuentran en estado no soporte y en revisión.	A nivel de los diferentes componentes middleware y base de datos será realizado el análisis correspondiente con la finalidad de identificar si se cuenta con soporte IPv6 por parte de los componentes middleware y base de datos además de ser realizada su respectiva implementación.	Especialistas de Aplicaciones / Líder Gestor de Aplicaciones																

Gráfica 5 Plan de implementación IPV6

En la Gráfica 5, se presenta el diagrama del plan de implementación IPV6 que se plantea para este proyecto. Para mayor detalle del diagrama, dirigirse al **Anexo 2 Diagrama Plan Implementación IPV6**.

Estas validaciones se llevarán a cabo como es presentado en el siguiente diagrama de flujo.



Gráfica 6 Diagrama de Flujo implementación IPV6

Con la información obtenida luego de generar el diagnóstico del estado actual se plantea sea posible implementar IPV6 en 72 aplicaciones, teniendo en cuenta que se pueden presentar restricciones por compatibilidades a nivel de sus componentes técnicos durante el proceso de la implementación.

Se plantea Cronograma de trabajo según Diagnóstico realizado anterior mencionado por grupos:

Se inicia con el grupo estado en **Revisión**, para este caso se tienen un total de 13 aplicaciones, y se plantea que la primera actividad en el cronograma para este estado tenga una fecha tentativa de inicio para el 05/04/21 y la última actividad se ejecute el 07/10/21. Paralelamente, se hará la apropiación IPV6 en Apps con estado **ítems Pendientes** (Parcialmente Implementado), son 26 aplicaciones que con anterioridad se desarrollaron

actividades de implementación de IPV6, pero que según los ítems planteados en el diagnostico no cuentan con la apropiación en su totalidad.

Las Apps con los estados **Sin Implementar y Pendiente Protocolo Paso a Producción**, son 17 y 16 aplicaciones en total, respectivamente, en las cuales se implementará la apropiación de IPV6 de forma paralela entre el 07/10/21 y el 09/06/22, enseguida se dará por finalizado este Cronograma.

Para la Implementación del Protocolo IPV6 se está proyectando RFCs (ordenes de cambio) la cual contemplan, inicialmente las siguientes actividades:

- Generar Snapshot a los servidores.
- Poner en mantenimiento los servidores y las URLs.
- Bajar servicios de la aplicación.
- Bajar servicio de base de datos.
- Actualización archivos de configuración y properties para resolver por hostname y dominios a nivel del servidor de aplicaciones.
- Ajustar string de conexión de base de datos para que resuelva por hostname y no por dirección IP.
- Registrar en DNS del MEN Hostname del servidor de base de datos para que responda por IPV6 y por IPV4.
- Configuración del motor de base de datos para que acepte conexiones por IPV4 e IPV6.
- subir servicio de base de datos.
- Subir servicios de la aplicación.
- Realizar escaneo de vulnerabilidades.
- Mitigación y/o aceptación de vulnerabilidades.
- Quitar de mantenimiento los servidores y las URLs.
- validación técnica de la aplicación a nivel de capa media bajo el protocolo IPV4 e IPV6.
- Realizar validación de despliegue de la aplicación por IPV6.
- Realizar validación de disponibilidad y navegación de la aplicación.
- Pruebas Funcionales por parte del líder Técnico del Ministerio de Educación, indicado por medio de un Checklist que la aplicación funciona correctamente por protocolo de IPV6.

5.3. PRUEBAS DE FUNCIONALIDAD POR IMPLEMENTACIÓN IPV6

Este ítem hace referencia a la 7.3 Fase III. Pruebas de funcionalidad de IPv6 de la guía de MinTIC (Guía 1: Guía de Transición de IPv4 a IPv6 – MinTIC, febrero 2021).

Se contempla la realización de pruebas de funcionalidad de la implementación del protocolo teniendo en cuenta el rol participativo de cada una de las partes involucradas en la ejecución del mismo.

Se presentará la siguiente documentación:

- Informe_Implementación_IPv6.
- Lista de chequeo.

Informe Implementación IPv6: Contempla la implementación del protocolo en la app respectiva, en función de dar claridad a la misma se debe evidenciar proceso que garanticen la correcta ejecución, dicho documento contendrá los siguientes ítems

- Introducción
- Objetivo
- Alcance
- Implementación en ambiente de certificación
- Implementación en ambiente de producción
- Pruebas de funcionamiento
- Conclusiones

Lista de chequeo: Check list de verificación de servicios contemplando los siguientes ítems de validación

	Ítem
01	Tiempo de respuesta de la aplicación (Si Aplica)
02	Ingreso URL Externa
03	Ingreso URL Interna
04	Logueo a la aplicación
05	Envío de Correo electrónico (Si aplica)
06	Generación de Reporte
07	Validar Servicios Web que Publique (Si aplica)
08	Verificar Servicios WEB que Consuma Internos (Si aplica)
09	Verificar Servicios WEB que Consuma Externos (Si aplica)
10	Comprobación de conexión con otros sistemas. (Si aplica)
11	Navegación Básica en el Sistema.
12	Permisos FTP (Si aplica)
13	Verificación de accesos a VPN. (Si Aplica)
14	Verificación IPs Fijas Usuarios VPN (Si aplica)
15	Verificación de Cargue de Archivos (Si aplica)
16	Verificación de Descargue de Archivos (Si aplica)
17	Verificación de Jobs (Si aplica)
18	Validación de Puertos de Publicación de Aplicación.
19	Verificación de conexión de la aplicación a la Base de Datos

Tabla 7. Ítems lista de chequeo validación funcionamiento de IPv6

El informe de implementación así como la lista de chequeo son almacenados por aplicación implementada en la siguiente ruta:

https://mineducaciongovco.sharepoint.com/:f:/r/sites/Proyecto_UTGI_MEN/Documentos%200compartidos/PROYECTO_UTGI_MEN/2.%20Planes%20-%20Listas%20de%20Chequeo/2.2%20Listas%20de%20Chequeo/2.2.2%20Gesti%C3%B3n%20de%20Aplicaciones?csf=1&web=1&e=x1LFmz

6. NO VIABILIDAD DE ADOPCIÓN IPV6

6.1. ESCRITORIOS VIRTUALES

El Ministerio cuenta con dos plataformas de escritorios virtuales on-premise y la nube, desarrolladas en VMware Horizon y Azure Windows Virtual Desktop.

A nivel de IPV6, las soluciones no cuentan con IPV6 por las siguientes razones técnicas:

Plataforma escritorios virtuales On-Premises – VMware Horizon versión 7.11: Horizon 7 admite IPV6 como alternativa a IPV4. El entorno debe ser únicamente IPV6 o únicamente IPV4. Horizon 7 no admite un entorno IPV6 y IPV4 mixto.

No todas las funciones de Horizon 7 admitidas en un entorno IPV4 se admiten en un entorno IPV6. Horizon 7 no admite la actualización de un entorno IPV4 a un entorno IPV6. Además, Horizon 7 no admite la migración entre entornos IPV4 e IPV6. Como esta solución fue implementada bajo versión IPV4 no puede ser modificada a IPV6.

Link con información de fabricante VMware: <https://docs.vmware.com/es/VMware-Horizon-7/7.11/horizon-installation/GUID-AE561E5A-786F-4BE5-AB63-1CD9F2FD3B67.html>

Plataforma escritorios virtuales – escritorios en nube Azure Windows Virtual Desktop: la solución cuando fue desplegada por proveedor externo sobre nube Azure solamente podía ser configurada sobre IPV4.

Esta situación fue notificada desde octubre de 2020 al MEN, a partir del ticket SOL494164 debido a la imposibilidad de asignación de escritorios IPV6 sobre servicio Windows Virtual Desktop en nube Azure.

6.2. APLICACIONES QUE NO SOPORTAN IPV6

Con el diagnostico se encuentra que hay aplicaciones que no cuentan con la capacidad para implementar IPV6. Esto se debe a que estas aplicaciones cuentan con versiones de middleware y motor de base de datos que no son compatibles con IPV6 para esta aplicación se tiene la documentación técnica como soporte en los Repositorios. Se adjunta el Anexo 3 Listado de chequeo para IPV6 en donde se encuentra relacionado las rutas de los repositorios de la documentación soporte mencionada anteriormente.

7. CONCLUSIONES Y RECOMENDACIONES

7.1. CONCLUSIONES

- El cuarenta y ocho por ciento (48%) de las aplicaciones no soportan la implementación de IPV6 en sus servidores.
- Del total de las aplicaciones que soportan IPV6 el 13% de las aplicaciones del MEN cuenta con una implementación completa de IPV6 a la fecha 13 de mayo de 2021.
- El 95% de los motores de Base datos Oracle administrados no cuentan con compatibilidad para implementar IPV6, por lo tanto, es requerido realizar inicialmente, la migración de los motores Oracle que se encuentran en las versiones 11g y 12c, para realizar su implementación IPV6.
- El plan de Actualización de IPV6 estaría ligado con el plan de migración a motores de base de datos MySQL/MariaDB, SQL Server y PostgreSQL, debido a que la compatibilidad en los aplicativos con el motor de base de datos va sujeto a ajustes requeridos del desarrollo y driver por parte de las fábricas de software.
- A excepción de escritorios virtuales toda la infraestructura del Ministerio tiene la capacidad de soportar IPv6 para las aplicaciones actuales y futuras.

7.2. RECOMENDACIONES

- Dar completitud a los soportes de las implementaciones IPV6 que no se encuentran documentadas y no se encuentran llevadas a cabo en su totalidad.
- Migrar a nivel de los motores de Base de datos a las últimas versiones de motores de Bases de Datos de acuerdo con las recomendaciones del fabricante.
- Migrar a nivel de las APP a las versiones de contenedores que soporten IPV6 de acuerdo con las recomendaciones del fabricante.
- Solicitar a nivel del protocolo paso a producción que todas las nuevas aplicaciones o sistemas de información, sean compatibles e implementadas bajo el protocolo IPV6.
- Contar con el continuo apoyo de la OTSI, para la ejecución de paso a producción y ejecución de pruebas funcionales correspondientes.

8. REFERENCIAS

MinTIC – Viceministerio de Transformación Digital. (2021, febrero). *Guía 1 - Guía de Transición de IPv4 a IPv6 para Colombia. Dirección de Gobierno Digital.*

https://www.mintic.gov.co/portal/715/articles-162301_guia_transicion_ipv4_ipv6.pdf

MinTIC – Viceministerio de Transformación Digital. (2021b, febrero). *Guía 2 - Guía para el Aseguramiento del Protocolo IPv6. Dirección de Gobierno Digital.*

https://www.mintic.gov.co/portal/715/articles-162301_guia_aseguramiento_ipv6.pdf

9. ACCIONES FUTURAS

Para garantizar que se cumplan los tiempos indicados en el Cronograma se tienen sesiones de seguimiento y mesa de trabajo al Cronograma de IPV6, entre las partes Ministerio de Educación Nacional, Interventoría y UT Gestión integral MEN para presentar los avances de forma semanal.

La plataforma de mesa de servicios de tecnología de CA, la cual, en este momento se encuentra configurada con IPV4, ya que, la solución en la actualidad no es compatible con el protocolo IPV6, por esta razón se encuentra en un proceso de actualización con el proveedor MSL.

10. ANEXOS

A continuación, son relacionados anexos del informe.

- **Anexo 1 PDT_IPV6_v311052021.mpp**
- **Anexo 2 Diagrama Plan Implementación IPV6**
- **Anexo 3 Listado de chequeo para IPV6**

Información Del Documento

Fecha	Versión	Responsable	Revisado por	Aprobado por
20/05/2021	1.0	Líder de Gestión Técnica y Seguridad Líder Gestor de Aplicaciones.	Líder de integración	

Control de cambios

Fecha	Versión	Causa Cambio	Aprobado por
20/05/2021	1.0	Creación del documento	