

DOCUMENTO DE MANTENIMIENTO PREVENTIVO
FORTIGATE 601E
MINISTERIO DE AGRICULTURA Y DESARROLLO RURAL

Fecha:
MAYO 13/2022

Gamma Ingenieros S.A.
U.E.N. Tecnología



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000

Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147

Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906

Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927

Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

CLIENTE:	MINISTERIO DE AGRICULTURA Y DESARROLLO RURAL
----------	--

Datos de la visita

Nombre:	MINISTERIO DE AGRICULTURA Y DESARROLLO RURAL
Contacto:	MARISOL GAONA
Teléfono:	3213900547
Fecha:	13/05/2022
Ciudad:	Bogotá
Serial:	FG6H1E5819900665
Ingeniero encargado:	ROBINSON MURILLO GALVIS
Contacto:	3176362823

Información Recolectada	Observaciones
-------------------------	---------------

1. Información básica del sistema

1.1	Versión de firmware	V6.4.8 build1914(GA)	
1.2	Configuración Fecha, hora y zona	GTM-5:00 Bogotá-Lima-Quito	
1.3	Estado de CPU	1%	
1.4	Estado de memoria	39%	
1.5	Total, de sesiones	25882	
1.6	Nombre de Host	FortiGate-601E_01	

2. Licenciamiento

2.1	Estado del licenciamiento	LICENCIA VALIDA HASTA 2024/11/12	
-----	---------------------------	----------------------------------	--

3. Interfaces

3.1	Total de Interfaces en uso	13	HA, MGMT, port1, port2, port3, port4, port5, port6, port8, port9, port10, port11, port12
3.2	Total de Interfaces libres	7	S1, S2, VW1, VW2, X1, X2, port7
3.3	Total Subinterfaces Vlan	9	



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000

Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147

Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906

Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927

Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

3.4	Prevencción de Botnet y C&C en interfaz con rol WAN	Disable	No se encuentra habilitado la característica
-----	---	---------	--

4. System DNS

4.1	DNS Primario	172.20.50.222	
4.2	DNS Secundario	172.20.50.11	
4.3	Dominio local	Minagricultura.gov.co	

5. Accesos Administrativos

5.1	Ping	15	fortilink / DMZ_F5-VLAN130 /DMZ_INT-VLAN34 / port5 / port6 / VLAN_LACP_INSIDE(VLAN_INSIDE) / port3 / port4 / VLAN_INTERNET / port11 / port12 / VLAN_SERVER_ANT / VLAN_SERVER_NUE / VLAN 16-SEDES(sedes) / VLAN 200-Mesa_Ayuda(COMWARE)
5.2	SSH	4	port5 / port6 / VLAN_LACP_INSIDE(VLAN_INSIDE) / mgmt
5.3	HTTP	4	port5 / port6 / VLAN_LACP_INSIDE(VLAN_INSIDE) / mgmt
5.4	HTTPS	4	port5 / port6 / VLAN_LACP_INSIDE(VLAN_INSIDE) / mgmt
5.5	TELNET	N/A	

6. System settings

6.1	HTTP Port	80
6.2	HTTPS Port	10433
6.3	SSH Port	1022
6.4	Telnet Port	23
6.5	Redirect to https Option	On
6.6	Idle Timeout	480
6.7	Password policy	Admin
6.8	Language	English
6.9	Theme	Green
6.10	Inspection Mode	N/A
6.11	Virtual Domains	Off



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000
Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147
Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906
Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927
Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

7. Conectores Security Fabric

7.1	Forti Connectors (FSSO ...)	On
7.2	FortiAnalyzer logging	On
7.3	FortiAP/Fortiswitch	Off
7.4	Cloud Logging	On
7.5	Fortimail	Off
7.6	FortiManager	On
7.7	Fortiweb/Forticache	Off

8. Logs

8.1	Disco	On	43.83% usado
8.2	Memoria	Off	
8.3	Forticloud	On	
8.4	Fortianalyzer	On	172.20.50.208
8.5	Syslog	Off	

9. Antivirus

9.1	Envío de archivos a FortiSandbox	On	default / wifi-default
9.2	Uso de base de datos FortiSandbox	Off	
9.3	Virus Outbreak Prevention Database	Off	

10. Políticas

10.1	Total de políticas	432	3,16,17,522,519,18,21,429,15,4,70,71,442,387,443,72,388,389,75,78,395,461,524,332,392,430,394,390,440,79,100,101,397,593,420,402,594,396,383,13,399,398,12,197,579,577,548,415,142,91,595,365,198,571,202,201,134,200,573,203,404,356,457,450,491,209,417,418,416,377,400,92,357,207,128,359,204,117,116,115,121,528,531,537,534,533,532,535,122,123,124,125,120,588,11,58,59,60,61,62,65,574,66,67,80,84,87,88,90,333,102,334,452,103,104,105,195,413,106,426,403,3
------	--------------------	-----	--



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000
Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147
Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906
Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927
Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

	84,107,547,549,108,109,459,68,422,421,7,33,34,35,36,41,42,414,410,411,409,43,428,39,482,382,40,590,6,49,425,424,5,22,23,427,28,432,401,29,30,31,439,32,24,25,94,423,95,98,222,500,233,493,589,99,460,412,575,96,438,322,320,445,97,146,434,152,150,153,182,572,161,339,166,168,494,169,171,580,591,599,592,449,172,173,436,578,175,177,433,294,345,468,215,241,242,245,246,248,249,251,252,253,254,257,274,181,184,186,187,190,453,191,499,496,517,228,193,210,485,219,221,220,234,264,266,271,279,298,312,317,319,329,337,355,362,363,366,373,381,405,435,444,455,464,477,478,526,540,550,511,447,231,489,463,458,541,509,508,505,502,475,471,470,466,465,462,451,446,408,407,406,371,364,323,304,301,291,282,278,283,284,285,286,287,510,295,341,340,314,487,456,288,289,338,347,351,352,367,369,368,378,379,380,419,437,441,335,296,307,308,309,310,311,313,328,327,326,316,276,275,272,268,262,260,259,350,256,238,467,469,476,480,596,497,481,488,473,501,504,516,520,521,536,454,293,492,554,349,232,506,542,543,546,544,545,551,552,582,555,556,431,557,558,498,513,514,474,479,472,490,495,503,507,584,512,515,483,484,527,518,523,525,529,530,538,539,553,559,560,561,563,562,564,565,566,567,568,569,570,576,581,448,598,587,586,585,597,583,0,
10.2 políticas con cero tráficos	155
	436,428,169,460,578,478,286,260,545,443,558,184,166,241,550,347,238,431,72,440,168,246,511,351,467,513,79,334,186,468,249,489,352,469,514,70,499,251,458,378,476,474,388,203,541,380,480,479,78,389,450,453,293,252,287,492,253,509,309,488,495,75,491,523,502,311,520,515,341,557,234,395,525,340,498,264,471,313,521,484,



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000
Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147
Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906
Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927
Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

		461,571,445,470,328,536,597,524,202,204,487,271,448,322,355,451,327,506,332,593,485,171,366,301,326,542,71,392,564,383,569,349,580,373,291,316,543,430,449,381,284,268,546,442,394,413,595,207,589,172,464,285,262,544,387,390,567,518,570,16,15,200,522,24,519,23,565,427,539,198,34,584,566,568,438,	
10.3	políticas deshabilitadas	8	565,539,506,514,564,518,523,485
10.4	Políticas (Source/destination ALL)	49	102,564,553,565,341,567,563,49,539,493,561,91,595,568,337,573,365,505,356,92,482,450,152,382,134,209,150,40,66,417,527,538,418,518,432,416,523,401,571,377,525,29,88,333,529,530,204,207,0,
10.5	Políticas con (Services ALL)	177	410,24,49,411,539,409,25,43,33,566,30,568,36,39,35,31,95,200,41,482,32,96,382,34,40,28,16,17,15,598,21,522,18,565,42,22,23,401,29,219,220,503,512,438,168,169,177,61,184,191,198,187,80,94,71,106,186,193,109,84,567,557,72,190,594,67,90,104,453,322,403,70,97,384,459,87,554,98,447,107,68,78,558,561,582,571,589,514,65,461,202,547,100,203,99,332,88,549,593,404,572,58,201,430,108,7,402,134,79,195,356,383,574,334,450,5,13,66,388,105,452,418,563,538,75,564,103,377,588,562,60,59,499,62,333,11,102,576,553,581,3,4,101,12,590,6,197,579,529,577,530,548,142,359,595,204,365,569,400,92,123,146,124,152,125,150,120,527,518,357,523,207,525,559,560,570,0,
10.6	Políticas con NAT deshabilitado	352	16,17,18,42,565,414,410,539,411,409,43,566,568,15,598,33,587,36,586,585,21,522,35,39,41,22,34,24,25,30,23,31,439,32,28,95,153,500,181,575,510,233,191,96,295,493,499,438,341,589,496,494,340,99,517,169,314,460,228,184,487,412,193,187,456,182,454,552,161,293,94,448,339,492,



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000

Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147

Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906

Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927

Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

423,166,557,186,98,168,490,349,177,190,232,34
5,322,453,468,320,287,222,215,97,317,478,471,
171,248,319,526,470,282,580,249,329,540,466,2
78,591,251,337,550,465,283,599,252,355,511,46
2,284,592,253,362,447,451,285,449,254,363,231
,446,286,172,257,366,489,408,288,173,274,373,
463,407,289,436,234,381,458,406,338,578,264,4
05,541,371,347,175,266,435,509,364,351,241,27
1,444,508,323,352,242,279,455,505,304,367,245
,298,464,502,301,369,246,312,477,475,291,368,
378,480,379,326,596,544,597,380,316,497,545,4
19,276,481,551,437,275,488,582,441,272,555,47
3,335,268,556,501,296,262,504,431,62,307,260,
516,513,308,259,520,514,60,309,350,521,472,31
0,256,536,495,59,311,238,506,507,313,467,542,
515,67,328,469,543,483,327,476,546,484,459,58
,61,549,195,108,430,394,105,334,390,564,452,4
40,413,75,106,109,7,567,80,594,425,104,403,42
4,84,384,5,78,554,107,524,90,558,561,445,332,
392,547,553,87,588,68,65,442,387,443,72,70,3,
6,103,422,421,485,396,583,13,532,563,535,562,
121,518,122,523,123,525,124,529,125,120,11,57
6,383,581,4,399,398,12,100,537,397,117,534,59
3,116,128,533,420,115,528,559,402,210,531,560

11. Virtual IP

11.1 Cantidad de VIP

22

186.30.118.218 / 186.30.118.240 /
186.30.118.198 / 186.30.118.219 /
186.30.118.243 / 186.30.118.241 /
186.30.118.212 / 186.30.118.214 /
186.30.118.246 / 186.30.118.238 /
186.30.118.217 / 186.30.118.215 / SKYPE_EDGE
/ SKYPE_DISCOVER / SKYPE_WEBCONF /
SKYPE_AV / 186.30.118.227 / 186.30.118.228 /



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000

Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147

Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906

Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927

Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

		186.30.118.221 / Minagricultura_www_ipv6 / Agronet_www.ipv6 / SERVICIOS-PUBLICADOS
11.2 VIP con interfaz ANY	20	186.30.118.218 / 186.30.118.240 / 186.30.118.198 / 186.30.118.219 / 186.30.118.243 / 186.30.118.241 / 186.30.118.212 / 186.30.118.214 / 186.30.118.246 / 186.30.118.238 / 186.30.118.217 / 186.30.118.215 / SKYPE_EDGE / SKYPE_DISCOVER / SKYPE_WEBCONF / SKYPE_AV / 186.30.118.227 / 186.30.118.228 / 186.30.118.221 / SERVICIOS-PUBLICADOS
11.3 VIP con 0 referencia		0

12. Traffic Shapers

12.1 Total, de objetos de traffic shaper	5	100-Megas / IMPRESION_MEZANINE / Guarantee-100kbs / high-priority / low-priority / medium-priority / shared-1M-pipe / teams
12.2 Políticas de traffic Shaper	5	La única habilitada es la implícita
12.3 Objetos sin referencia	5	100-Megas / Guarantee-100kbs / low-priority / medium-priority / shared-1M-pipe

13. Configuración HA

13.1 Modo HA		Active/Active						
13.2 Interfaces Heartbeat	2	HA, port8						
13.3 Checksum	OK	Checksum 97079c111fa7bdbea71a97ba53b3aafe 97079c111fa7bdbea71a97ba53b3aafe						
13.4 Estado Master/Slave	OK	<table border="1"> <thead> <tr> <th>Serial No.</th> <th>Role</th> </tr> </thead> <tbody> <tr> <td>FG6H1E5819900665</td> <td>Primary</td> </tr> <tr> <td>FG6H1ETB20907192</td> <td>Secondary</td> </tr> </tbody> </table>	Serial No.	Role	FG6H1E5819900665	Primary	FG6H1ETB20907192	Secondary
Serial No.	Role							
FG6H1E5819900665	Primary							
FG6H1ETB20907192	Secondary							
13.5 Simetría en Interface		N/A						



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000

Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147

Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

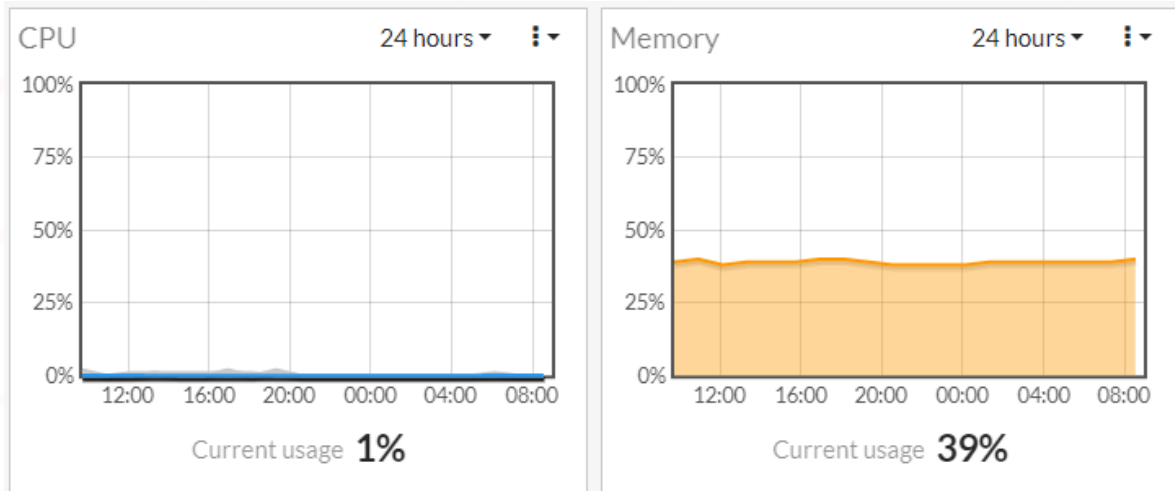
Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906

Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927

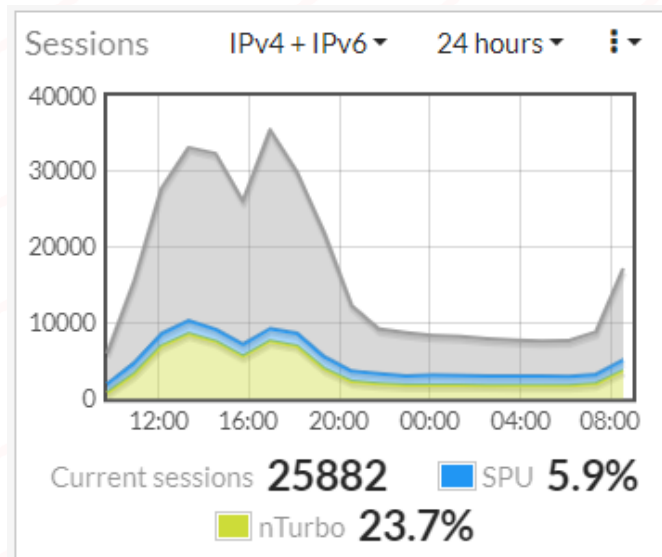
Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

14. Capturas de pantalla (CPU, Memoria, Sesiones, Licenciamiento.)

➤ CPU - MEMORIA



➤ SESIONES



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000

Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147

Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906

Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927

Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

➤ LICENCIAMIENTO

License Information	
Entitlement	Status
+ FortiCare Support	✓ Registered
+ Firmware & General Updates	✓ Licensed (Expiration Date: 2024/11/12)
+ Intrusion Prevention	✓ Licensed (Expiration Date: 2024/11/12)
+ AntiVirus	✓ Licensed (Expiration Date: 2024/11/12)
+ Web Filtering	✓ Licensed (Expiration Date: 2024/11/12)
Outbreak Prevention	✓ Licensed (Expiration Date: 2024/11/12)
SD-WAN Network Monitor	⚠ Not Licensed
Security Rating	⚠ Not Licensed
+ Industrial DB	⚠ Not Licensed
FortiIPAM	⚠ Not Licensed
IoT Detection Service	⚠ Not Licensed
FortiGate Cloud	✓ Activated

16. Evidencias fotográficas (Fotos de ubicación de dispositivos, Ocupación de interfaces, fuentes de alimentación y polos a tierra).

➤ N/A



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000

Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147

Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906

Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927

Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

17. Recomendaciones generales

- A pesar de que el sistema es compatible con el español para la nomenclatura de los objetos evitar usar caracteres especiales comunes como: ñ, Ñ, á, é, í, ó, ú, Á, É, Í, Ó, Ú, debido a que es probable que en escenarios de actualización de firmware puedan ocasionar fallas en los objetos involucrados.
- Conservar las condiciones ambientales con las que trabaja el equipo:
 - Temperatura de 0 a 40 grados C
 - Temperatura de almacenamiento -25 a 70 grados C
 - Humedad 5 a 95% sin condensación.
- Realizar Backup cada vez que se realice una actualización de Firmware.
- Realizar Backup antes de iniciar un cambio importante en la configuración más estable.
- Tratar, en lo posible; mantener el dispositivo actualizado con la última versión más estable; para ello se debe revisar los realase liberados por fabricante, analizando si pueden llegar a presentar fallas según la configuración existente.
- El equipo por sí solo no constituye una garantía de seguridad. Es fundamental su continua administración y análisis del tráfico que reporta, para efectuar mejoras a la implementación debido a las condiciones cambiantes de la red administrada.

18. Recomendaciones específicas

- Se recomienda ejercer seguimiento de los ID asociados de las políticas en la tabla anterior. En el apartado “En políticas con que no censan tráfico, políticas deshabilitadas y Políticas (Source/destination ALL)”.
- Validar si las políticas salen a internet, es recomendable habilitar el NAT.
- Se recomienda mantener activo el SSH únicamente en la interfaz destinada para la administración del dispositivo.
- Se recomienda mantener activo el HTTPS únicamente en la interfaz destinada para la administración del dispositivo.
- Se recomienda bajar el “Idle Timeout” de 480 Minutos a 5 Minutos.

Con la ejecución de lo anterior, se pretende aplicar el principio del menor privilegio que es una estrategia de seguridad, aplicable a distintos ámbitos, que se apoya en la idea de otorgar únicamente permisos cuando son necesarios para el desempeño de sus actividades cotidianas.



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000

Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147

Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906

Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927

Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

Elaborado por	Revisado por	Aprobado por	
Robinson Murillo Galvis Soporte Técnico Fecha: mayo 2022	Ing. Felipe Romero Líder Zona Centro Fecha: mayo 2022	FSPIT00 6	2016



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000

Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147

Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906

Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927

Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454