

INNOVACION TECNOLOGICA COLOMBIANA
INTEGCO LTDA. - NIT 830.076.864-4
CALLE 76 No 16A-39 TEL. No.: 6018097358 - 6014044492
WhatsApp Corporativo No.3112916336
Línea Nacional gratuita 018000413652
Correo: gerencia@integco.com.co
Integco16@gmail.com
Bogotá D.C (Colombia)



Zyxel Security Report

Organization

Alcaldia FACATATIVA

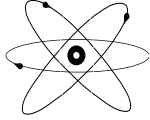
Device

Facatativá

Report Period

2026-03-02 - 2026-04-03

"Somos la garantía de su desarrollo"



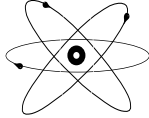
INNOVACION TECNOLOGICA COLOMBIANA
INTEGCO LTDA. - NIT 830.076.864-4
CALLE 76 No 16A-39 TEL. No.: 6018097358 - 6014044492
WhatsApp Corporativo No.3112916336
Línea Nacional gratuita 018000413652
Correo: gerencia@integco.com.co
Integco16@gmail.com
Bogotá D.C (Colombia)



Tabla de contenido

1. Indicador de Seguridad
- 1.1 IP Reputation
2. IPS Hits
3. Top Attack
4. Trafico de red
5. Conclusiones.
6. Recomendaciones

"Somos la garantía de su desarrollo"



INNOVACION TECNOLOGICA COLOMBIANA
INTEGCO LTDA. - NIT 830.076.864-4
CALLE 76 No 16A-39 TEL. No.: 6018097358 - 6014044492
WhatsApp Corporativo No.3112916336
Línea Nacional gratuita 018000413652
Correo: gerencia@integco.com.co
Integco16@gmail.com
Bogotá D.C (Colombia)



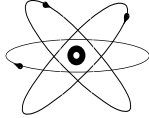
1. Indicador de Seguridad

Anomaly Detection and Prevention ADP significa "Anomaly Detection and Prevention", puede detectar anomalías basadas en violaciones de los estándares de protocolo, y flujos anormales como el escaneo de puertos.

Security Indicator			Last 30 days
ADP Hits	Antivirus / Malware Hits	URL Threat Filter Hits	IP Reputation Hits
0	2 219,943 scanned	2,023 12M scanned	180 19M scanned
IPS Hits	Sandboxing Hits	DNS Threat Filter Hits	
54 19M scanned	0 3,252 scanned	26,259 12M scanned	

La gráfica anterior nos muestra la detección y prevención de 0 anomalías (ADP), 2023 URL maliciosas y 54 ataques a la red que han sido bloqueadas

"Somos la garantía de su desarrollo"



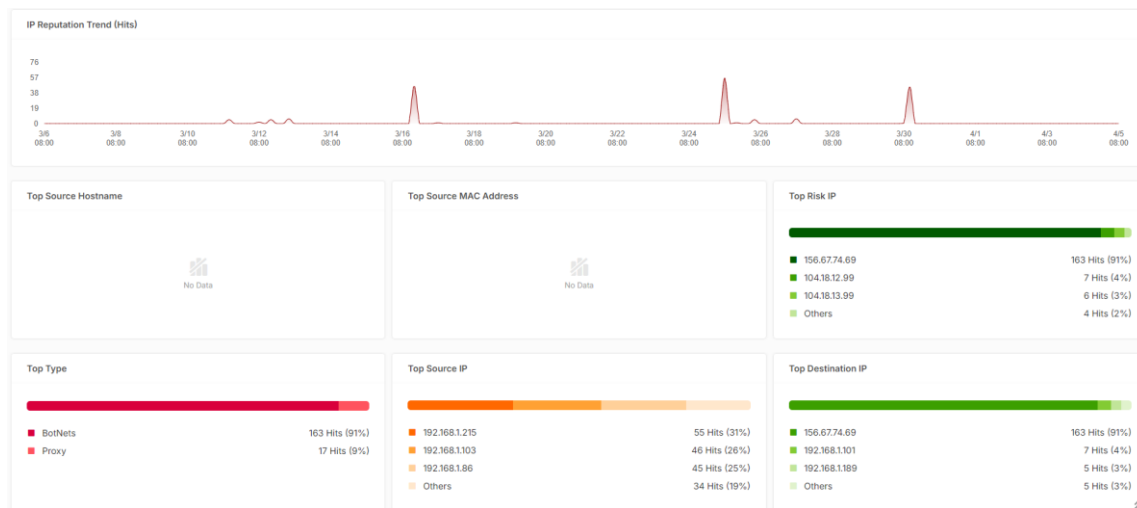
INNOVACION TECNOLOGICA COLOMBIANA
INTEGCO LTDA. - NIT 830.076.864-4
CALLE 76 No 16A-39 TEL. No.: 6018097358 - 6014044492
WhatsApp Corporativo No.3112916336
Línea Nacional gratuita 018000413652
Correo: gerencia@integco.com.co
Integco16@gmail.com
Bogotá D.C (Colombia)



1.1 IP Reputation

La “ip reputation” es una función de seguridad proactiva que evalúa la confiabilidad de las direcciones ip con las que tu red intenta comunicarse.

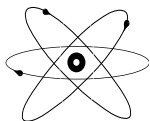
Cada dirección ip en internet tiene un “historial de comportamiento”. Algunos servidores e ips son confiables (como google o microsoft), mientras que otros pueden estar comprometidos y ser usados para spam, malware, botnets, ataques ddos, phishing u otras amenazas.



- La tabla anterior nos muestra que 31% proviene de la ip **192.168.1.215**, 26% de la ip **192.168.1.103**, 25% de la ip **192.168.1.86** y el 19% desde diferentes direcciones relacionadas a continuación, las cuales fueron bloqueadas por el firewall:

Source IP	Hits	%
192.168.1.215	55	31%
192.168.1.103	46	26%
192.168.1.86	45	25%
192.168.1.143	11	6%
104.18.12.99	7	4%
104.18.13.99	6	3%
192.168.1.249	6	3%
172.67.218.2	1	1%
172.67.139.119	1	1%
23.227.38.65	1	1%
216.24.57.251	1	1%

“Somos la garantía de su desarrollo”



INNOVACION TECNOLOGICA COLOMBIANA
INTEGCO LTDA. - NIT 830.076.864-4
CALLE 76 No 16A-39 TEL. No.: 6018097358 - 6014044492
WhatsApp Corporativo No.3112916336
Línea Nacional gratuita 018000413652
Correo: gerencia@integco.com.co
Integco16@gmail.com
Bogotá D.C (Colombia)

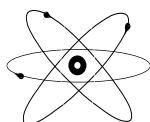


Botnet, Spam, Anonymizers, ip origen la cantidad de hits y conexiones

Threat Website	Hits	%
perr.hola.org	190	46%
authentication.urban-vpn.com	37	9%
watersort.live	21	5%
perr.su89-cdn.net	15	4%
perr.zspeed-cdn.com	15	4%
perr.c6gj-static.net	14	3%
perr.kbz0pwvxmv.com	14	3%
perr.x-cdn-static.com	14	3%
hola.org	14	3%
perr.yg5sjx5kzy.com	13	3%
analytics-toolbar.urban-vpn.com	11	3%
su89-cdn.net	5	1%
zspeed-cdn.com	5	1%
x-cdn-static.com	4	1%
kbz0pwvxmv.com	4	1%
c6gj-static.net	4	1%
yg5sjx5kzy.com	4	1%
client-cdn4.hola.org	4	1%
http-test1.hola.org	3	1%
proxyjs.hola.org	3	1%
proxyjs.zspeed-cdn.com	3	1%
proxyjs.su89-cdn.net	3	1%
anti-phishing-protection-toolbar.urban-vpn.com	2	0%
govco-and.xyz	2	0%
image.mailcruzverde.com.co	1	0%
scripts.icommkt.online	1	0%
client.hola.org	1	0%
client.su89-cdn.net	1	0%
client.zspeed-cdn.com	1	0%
update.drp.su	1	0%

Sitios BOTNET BLOQUEADOS por el firewall.

"Somos la garantía de su desarrollo"



INNOVACION TECNOLOGICA COLOMBIANA
INTEGCO LTDA. - NIT 830.076.864-4
CALLE 76 No 16A-39 TEL. No.: 6018097358 - 6014044492
WhatsApp Corporativo No.3112916336
Línea Nacional gratuita 018000413652
Correo: gerencia@integro.com.co
Integro16@gmail.com
Bogotá D.C (Colombia)



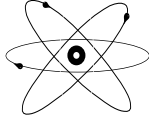
IPS DE ORIGEN

Source IP	Hits	%	Source IP	Hits	%	Source IP	Hits	%
192.168.1.70	350	17%	192.168.1.126	35	2%	192.168.1.149	3	0%
192.168.1.59	150	7%	192.168.1.159	34	2%	192.168.1.114	3	0%
192.168.1.35	136	7%	192.168.1.56	30	1%	192.168.1.122	3	0%
192.168.1.63	136	7%	192.168.1.157	25	1%	192.168.1.110	3	0%
192.168.1.97	134	7%	192.168.1.247	22	1%	192.168.1.102	2	0%
192.168.1.229	126	6%	192.168.1.172	21	1%	192.168.1.133	2	0%
192.168.1.185	105	5%	192.168.1.228	20	1%	192.168.1.125	2	0%
192.168.1.21	100	5%	192.168.1.58	19	1%	192.168.1.109	2	0%
192.168.1.55	91	4%	192.168.1.80	17	1%	192.168.1.184	2	0%
192.168.1.53	64	3%	192.168.1.82	13	1%	192.168.1.246	2	0%
192.168.1.61	56	3%	192.168.1.118	12	1%	192.168.1.213	2	0%
192.168.1.225	45	2%	192.168.1.12	12	1%	192.168.1.223	2	0%
192.168.1.69	44	2%	192.168.1.100	11	1%	192.168.1.171	2	0%
192.168.1.124	42	2%	192.168.1.112	10	0%	192.168.1.99	2	0%
192.168.1.137	40	2%	192.168.1.89	8	0%	192.168.1.75	1	0%
192.168.1.138	40	2%	192.168.1.94	8	0%	192.168.1.170	1	0%
			192.168.1.15	7	0%	192.168.1.197	1	0%
			192.168.1.101	4	0%	192.168.1.241	1	0%
			192.168.1.77	4	0%	192.168.1.206	1	0%
			192.168.1.79	4	0%	192.168.1.66	1	0%
			192.168.1.24	4	0%	192.168.1.236	1	0%
						192.168.1.115	1	0%
						192.168.1.31	1	0%
						192.168.1.131	1	0%
						192.168.1.250	1	0%
						192.168.1.128	1	0%

IP DESTINO

Destination IP	Hits	%	Destination IP	Hits	%	Destination IP	Hits	%
3.91.129.53	247	12%	148.72.165.228	9	0%	172.240.212.94	2	0%
3.230.112.143	242	12%	148.72.164.12	9	0%	172.240.212.197	2	0%
54.163.144.140	160	8%	54.145.65.54	9	0%	45.133.44.2	2	0%
52.1.213.44	157	8%	18.235.56.118	8	0%	3.170.19.7	2	0%
98.90.16.141	122	6%	104.26.11.133	7	0%	69.147.224.31	2	0%
34.192.239.218	121	6%	148.72.168.104	6	0%	54.230.144.118	2	0%
34.231.82.190	115	6%	148.72.133.132	6	0%	3.162.112.65	2	0%
173.45.77.74	60	3%	148.72.166.236	6	0%	148.72.152.76	2	0%
54.167.136.2	56	3%	148.72.164.13	5	0%	18.185.155.101	1	0%
173.45.77.90	55	3%	148.72.168.105	5	0%	167.172.235.33	1	0%
207.182.128.178	55	3%	172.67.69.246	5	0%	104.20.2.154	1	0%
173.45.77.66	54	3%	104.26.10.133	4	0%	178.63.248.49	1	0%
34.196.242.189	53	3%	148.72.140.75	4	0%	157.90.33.78	1	0%
207.182.128.202	52	3%	3.170.19.123	4	0%	172.240.212.84	1	0%
34.193.117.164	51	3%	54.230.144.119	4	0%	18.239.6.18	1	0%
54.157.143.132	44	2%	54.172.33.39	4	0%	3.170.19.83	1	0%
34.234.221.175	44	2%	5.45.75.80	4	0%	108.156.245.95	1	0%
92.122.157.208	42	2%	148.72.172.31	3	0%	108.156.245.81	1	0%
54.152.214.247	34	2%	44.214.0.0	3	0%	148.72.165.78	1	0%
172.240.127.243	33	2%	172.64.150.21	3	0%	128.245.147.201	1	0%
34.228.101.202	31	2%	45.133.44.1	3	0%	172.240.127.242	1	0%
13.216.144.68	12	1%	45.88.1.105	3	0%	172.240.41.97	1	0%
178.63.248.55	12	1%	148.72.133.133	2	0%	172.240.253.132	1	0%
34.194.183.84	10	0%				148.72.170.52	1	0%
64.120.31.25	10	0%				18.155.252.97	1	0%
						54.230.253.22	1	0%
						37.9.8.75	1	0%

“Somos la garantía de su desarrollo”



INNOVACION TECNOLOGICA COLOMBIANA
INTEGCO LTDA. - NIT 830.076.864-4
CALLE 76 No 16A-39 TEL. No.: 6018097358 - 6014044492
WhatsApp Corporativo No.3112916336
Línea Nacional gratuita 018000413652
Correo: gerencia@integro.com.co
Integro16@gmail.com
Bogotá D.C (Colombia)



TIPO

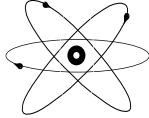
URL Threat Filter Hit Detail		
by Hostname	by MAC Address	by Threat Website
by Type	by Source IP	by Destination IP
Type	Hits	%
Anonymizers	996	49 %
Malicious Sites	864	43 %
Spam URLs	92	5 %
Phishing	41	2 %
Malicious Downloads	30	1 %

2. IPS HITS

Intrusion Prevention System actúa en el entorno de red de su empresa con la detección de tráfico anómalo de una amplia gama de actividades sospechosas, como inyección SQL, DoS y aplicaciones maliciosas de puerta trasera, relacionadas a continuación

#	Time	Signature Name	Threat Type	Severity	Source IP	Action
1	1/04/2026 7:54	HTTP Directory Traversal	Misc	4	192.168.1.187	Reject
2	30/03/2026 18:59	Microsoft Office BMP Header biClrUsed Integer Overflow	Buffer-Overflow	4	192.168.1.7	Reject
3	30/03/2026 18:08	HTTP Directory Traversal	Misc	4	192.168.1.31	Reject
4	30/03/2026 12:14	Microsoft Office Word CVE-2015-1649 Memory Corruption	Buffer-Overflow	4	192.168.1.192	Reject
5	30/03/2026 12:14	Microsoft Office Word CVE-2015-1649 Memory Corruption	Buffer-Overflow	4	192.168.1.192	Reject
6	30/03/2026 12:12	Microsoft Office Word CVE-2015-1649 Memory Corruption	Buffer-Overflow	4	192.168.1.192	Reject
7	30/03/2026 12:12	Microsoft Office Word CVE-2015-1649 Memory Corruption	Buffer-Overflow	4	192.168.1.192	Reject
8	30/03/2026 11:04	SSL request for export grade ciphersuite attempt -2	MISC	4	192.168.1.208	Reject
9	30/03/2026 10:20	SSL request for export grade ciphersuite attempt -2	MISC	4	192.168.1.142	Reject
10	30/03/2026 8:37	Microsoft Office BMP Header biClrUsed Integer Overflow	Buffer-Overflow	4	192.168.1.233	Reject
11	30/03/2026 8:37	Microsoft Office BMP Header biClrUsed Integer Overflow	Buffer-Overflow	4	192.168.1.233	Reject
12	27/03/2026 10:38	SSL request for export grade ciphersuite attempt -2	MISC	4	192.168.1.66	Reject
13	27/03/2026 9:36	Microsoft Office BMP Header biClrUsed Integer Overflow	Buffer-Overflow	4	192.168.1.101	Reject
14	27/03/2026 9:28	SSL request for export grade ciphersuite attempt -2	MISC	4	192.168.1.208	Reject
15	26/03/2026 17:52	HTTP Directory Traversal	Misc	4	192.168.1.59	Reject
16	26/03/2026 17:50	HTTP Directory Traversal	Misc	4	192.168.1.59	Reject
17	26/03/2026 17:46	HTTP Directory Traversal	Misc	4	192.168.1.59	Reject
18	26/03/2026 17:03	SSL request for export grade ciphersuite attempt -2	MISC	4	192.168.1.136	Reject
19	26/03/2026 15:53	SSL request for export grade ciphersuite attempt -2	MISC	4	192.168.1.130	Reject
20	26/03/2026 12:24	OpenSSL TLS Connection Record Handling Denial of Service	Dos-DDoS	4	192.168.1.249	Reject
21	26/03/2026 12:23	OpenSSL TLS Connection Record Handling Denial of Service	Dos-DDoS	4	192.168.1.249	Reject
22	26/03/2026 7:35	HTTP Directory Traversal	Misc	4	192.168.1.236	Reject
23	26/03/2026 7:34	HTTP Directory Traversal	Misc	4	192.168.1.236	Reject
24	26/03/2026 1:37	Microsoft Office BMP Header biClrUsed Integer Overflow	Buffer-Overflow	4	192.168.1.31	Reject
25	25/03/2026 18:02	SSL request for export grade ciphersuite attempt -2	MISC	4	192.168.1.151	Reject
26	25/03/2026 15:37	HTTP Directory Traversal	Misc	4	192.168.1.236	Reject
27	25/03/2026 14:25	HTTP Directory Traversal	Misc	4	192.168.1.236	Reject
28	25/03/2026 14:22	HTTP Directory Traversal	Misc	4	192.168.1.236	Reject
29	25/03/2026 8:35	Directory Traversal	Misc	4	192.168.1.158	Reject
30	24/03/2026 16:10	HTTP Directory Traversal	Misc	4	192.168.1.249	Reject
31	24/03/2026 12:18	Microsoft Office BMP Header biClrUsed Integer Overflow	Buffer-Overflow	4	192.168.1.21	Reject
32	19/03/2026 18:19	SSL request for export grade ciphersuite attempt -2	MISC	4	192.168.1.147	Reject
33	19/03/2026 8:27	SSL request for export grade ciphersuite attempt -2	MISC	4	192.168.1.141	Reject
34	18/03/2026 11:40	Microsoft Office BMP Header biClrUsed Integer Overflow	Buffer-Overflow	4	192.168.1.59	Reject
35	17/03/2026 10:14	SSL request for export grade ciphersuite attempt -2	MISC	4	192.168.1.79	Reject
36	12/03/2026 17:31	HTTP Directory Traversal	Misc	4	192.168.1.108	Reject
37	11/03/2026 8:12	Microsoft Office BMP Header biClrUsed Integer Overflow	Buffer-Overflow	4	192.168.1.87	Reject
38	10/03/2026 16:36	HP Data Protector CRS Multiple Stack Buffer-Overflows	Buffer-Overflow	4	192.168.1.188	Reject
39	10/03/2026 12:17	HTTP Directory Traversal	Misc	4	192.168.1.197	Reject
40	9/03/2026 15:05	Microsoft Office Word CVE-2015-1649 Memory Corruption	Buffer-Overflow	4	192.168.1.206	Reject
41	9/03/2026 15:05	Microsoft Office Word CVE-2015-1649 Memory Corruption	Buffer-Overflow	4	192.168.1.206	Reject
42	9/03/2026 15:04	Microsoft Office Word CVE-2015-1649 Memory Corruption	Buffer-Overflow	4	192.168.1.206	Reject
43	9/03/2026 15:04	Microsoft Office Word CVE-2015-1649 Memory Corruption	Buffer-Overflow	4	192.168.1.206	Reject
44	9/03/2026 15:04	Microsoft Office Word CVE-2015-1649 Memory Corruption	Buffer-Overflow	4	192.168.1.206	Reject
45	9/03/2026 15:04	Microsoft Office Word CVE-2015-1649 Memory Corruption	Buffer-Overflow	4	192.168.1.206	Reject
46	9/03/2026 15:04	Microsoft Office Word CVE-2015-1649 Memory Corruption	Buffer-Overflow	4	192.168.1.206	Reject
47	9/03/2026 14:05	SSL request for export grade ciphersuite attempt -2	MISC	4	192.168.1.187	Reject
48	9/03/2026 13:30	Microsoft Windows NT SNMP Community Name Vulnerability	Access-Control	4	192.168.1.93	Reject
49	9/03/2026 13:30	Microsoft Windows NT SNMP Community Name Vulnerability	Access-Control	4	192.168.1.93	Reject
50	9/03/2026 13:29	Microsoft Windows NT SNMP Community Name Vulnerability	Access-Control	4	192.168.1.93	Reject
51	9/03/2026 10:00	Microsoft Office BMP Header biClrUsed Integer Overflow	Buffer-Overflow	4	192.168.1.151	Reject
52	6/03/2026 18:11	Microsoft Office BMP Header biClrUsed Integer Overflow	Buffer-Overflow	4	192.168.1.103	Reject
53	6/03/2026 17:29	HP Data Protector CRS Multiple Stack Buffer-Overflows	Buffer-Overflow	4	192.168.1.65	Reject
54	6/03/2026 12:20	CA BrightStor ARCserve Backup LGServe Stack Buffer Overflow -1	Buffer-Overflow	4	192.168.1.160	Reject

"Somos la garantía de su desarrollo"



INNOVACION TECNOLOGICA COLOMBIANA
INTEGCO LTDA. - NIT 830.076.864-4
CALLE 76 No 16A-39 TEL. No.: 6018097358 - 6014044492
WhatsApp Corporativo No.3112916336
Línea Nacional gratuita 018000413652
Correo: gerencia@integco.com.co
Integco16@gmail.com
Bogotá D.C (Colombia)



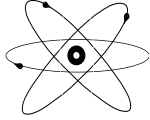
3. TOP ATTACK TYPES, TOP ATTACK TIME PERIOD, TOP ATTACKERS IP ADDRESS Y TOP ATTACKED IP ADDRESS

En la imagen anterior podemos evidenciar en periodo y tiempo el porcentaje de los principales ataques junto con la dirección IP de los atacantes y el origen hacia la Alcaldía Facatativá durante este mes.

Top Attack Origins		Top Attack Targets	
UNKNOWN	11 Hits (92%)	United States	454 Hits (100%)
United States	1 Hits (8%)	Russia	1 Hits (0%)
Top Attack Types		Top Attack Time Period	
URL Threat Filter	410 Hits (88%)	9:00 - 12:00	115 Hits (25%)
IP Reputation	46 Hits (10%)	9:00 - 12:00	85 Hits (18%)
IPS	11 Hits (2%)	15:00 - 18:00	65 Hits (14%)
		9:00 - 12:00	57 Hits (12%)
		Others	145 Hits (31%)
Top Attackers IP Address		Top Attacked IP Address	
192.168.1.70	313 Hits (67%)	3.230.112.143	242 Hits (52%)
192.168.1.86	45 Hits (10%)	34.231.82.190	115 Hits (25%)
192.168.1.59	23 Hits (5%)	156.67.74.69	45 Hits (10%)
192.168.1.126	21 Hits (4%)	207.182.128.202	10 Hits (2%)
Others	65 Hits (14%)	Others	55 Hits (12%)



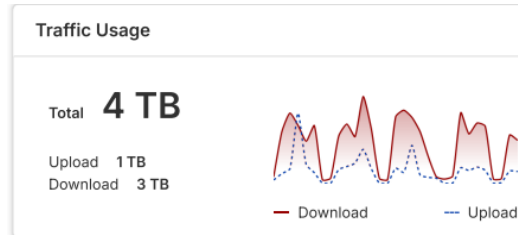
"Somos la garantía de su desarrollo"



INNOVACION TECNOLOGICA COLOMBIANA
INTEGCO LTDA. - NIT 830.076.864-4
CALLE 76 No 16A-39 TEL. No.: 6018097358 - 6014044492
WhatsApp Corporativo No.3112916336
Línea Nacional gratuita 018000413652
Correo: gerencia@integco.com.co
Integco16@gmail.com
Bogotá D.C (Colombia)



4. Trafico de red



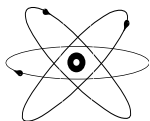
En la gráfica anterior podemos identificar el consumo de la red

Top Service Port				
Service Port	%	Traffic		
		Upload	Download	Total
443	87%	1 TB	3 TB	4 TB
80	7%	6 GB	326 GB	333 GB
8080	4%	113 GB	74 GB	187 GB
3478	1%	8 GB	17 GB	26 GB
3481	0%	227 MB	8 GB	8 GB

En la gráfica anterior podemos identificar en orden descendente los puertos que más se ha utilizado

Top Application				
Application	%	Traffic		
		Upload	Download	Total
WhatsApp Messe...	10%	70 GB	372 GB	443 GB
HyperText Transfe...	8%	47 GB	332 GB	380 GB
Microsoft SharePo...	8%	302 GB	44 GB	347 GB
Youtube.com	8%	11 GB	330 GB	342 GB
Facebook	5%	23 GB	212 GB	235 GB

“Somos la garantía de su desarrollo”



INNOVACION TECNOLOGICA COLOMBIANA
INTEGCO LTDA. - NIT 830.076.864-4
CALLE 76 No 16A-39 TEL. No.: 6018097358 - 6014044492
WhatsApp Corporativo No.3112916336
Línea Nacional gratuita 018000413652
Correo: gerencia@integco.com.co
Integco16@gmail.com
Bogotá D.C (Colombia)



- Sitios web más utilizados

5. CONCLUSIONES

- De acuerdo a la información, varios equipos están generando tráfico malicioso hacia internet

Las ips que generen tráfico malicioso se pondrán en lista negra provisional

6. RECOMENDACIONES

- Verificar las anteriores direcciones IP
- **Educación en ciberseguridad:** capacitar a los usuarios sobre prácticas como evitar clics en enlaces sospechosos y no descargar archivos de fuentes no verificadas.
- Verificar extensiones de navegadores, software de terceros, antivirus y actualizaciones del mismo
- Actualizaciones de sistemas operativos y sistemas operativos con soporte de Microsoft o el fabricante

"Somos la garantía de su desarrollo"