



RV: [TLP:RED]Network Scan - INC # 755446

Desde JOAN RENE CARVAJAL RAMIREZ <jrcarvajal@minenergia.gov.co>

Fecha Jue 5/03/2026 10:02 AM

Para TANIA SIERRA HUERTAS <tsierra@minenergia.gov.co>

Cordial saludo,

Para tu información y seguimiento.

Cordialmente,

**Joan Rene Carvajal Ramírez**

Contratista - Líder de Operaciones

Grupo de Tecnologías de la Información y las Comunicaciones

 jrcarvajal@minenergia.gov.co

 (+57) 601 2200 300

 Calle 43 No. 57-31 CAN. Bogotá, Colombia

 www.minenergia.gov.co

Desbloqueando el poder de los datos del sector



De: NICOLAS MALDONADO RODRIGUEZ <nmaldonado@minenergia.gov.co>

Enviado: jueves, 5 de marzo de 2026 9:26 a. m.

Para: soc.minminas <soc.minminas@rotorr.co>; HERNAN HUMBERTO GARZON BONILLA <hhgarzon@minenergia.gov.co>; Mesa de Ayuda <mesadeayuda@minenergia.gov.co>

Cc: OSCAR SANCHEZ SANCHEZ <osanchez@minenergia.gov.co>; JUAN JOSE CEDEÑO LOPEZ <jjcedeno@minenergia.gov.co>; JOAN RENE CARVAJAL RAMIREZ <jrcarvajal@minenergia.gov.co>; OSCAR FABIAN RAMIREZ TORRES <oframirez@minenergia.gov.co>

Asunto: RE: [TLP:RED]Network Scan - INC # 755446

Cordial Saludo.

Se realiza validación del equipo el cual se evidencia no contiene software malicioso.
Se realiza examen con Windows Defender sin presentarse novedad.
Se validan archivos y extensiones sin identificarse contenido malicioso.
Se

[@soc.minminas](#) amablemente solicito realizar el desbloqueo del equipo en mención.

Gracias.

Cordialmente;



Nicolás Maldonado Rodríguez

Mesa de Ayuda
Grupo de Tecnologías de la Información y las Comunicaciones

- nmaldonado@minenergia.gov.co
- (+57) 601 2200 300 Ext 2408
- Calle 43 No. 57-31 CAN. Bogotá, Colombia
- www.minenergia.gov.co

 Desbloqueando el poder de los datos del sector 

De: soc.minminas <soc.minminas@rotorr.co>
Enviado: jueves, 5 de marzo de 2026 8:46 a. m.
Para: HERNAN HUMBERTO GARZON BONILLA <hhgarzon@minenergia.gov.co>; Mesa de Ayuda <mesadeayuda@minenergia.gov.co>
Cc: OSCAR SANCHEZ SANCHEZ <osanchez@minenergia.gov.co>; JUAN JOSE CEDEÑO LOPEZ <jjcedeno@minenergia.gov.co>; JOAN RENE CARVAJAL RAMIREZ <jrcarvajal@minenergia.gov.co>; OSCAR FABIAN RAMIREZ TORRES <oframirez@minenergia.gov.co>
Asunto: RE: [TLP:RED]Network Scan - INC # 755446

TLP:RED

Cordial saludo,

Agradecemos la información brindada, por parte del SOC se mantiene el dispositivo en cuarentena.

Pending Actions 0 Active Actions 3 Cleared Actions 0 Expired Actions 15								
Device	IP	Action	History	Start / Expiration	Type	Source	Actions	Current Status
Diana	No IP	Enforce group pattern of life	View History	▶ Thu Mar 5 2026, 06:59:54 -05:00 ◀ Fri Mar 5 2027, 12:59:54 -05:00	Network	Manual trigger	Extend Clear	No Message

--
Cordialmente,

**SOC**

Security Operation Center

email: soc.minminas@rotorr.co

Corporación Rotorr – Motor de Innovación

Hemeroteca Universidad Nacional

Av. El Dorado No. 44ª – 40, Bogotá, Colombia, 111321

Teléfono:

TLP:RED**De:** HERNAN HUMBERTO GARZON BONILLA <hhgarzon@minenergia.gov.co>**Enviado:** jueves, 5 de marzo de 2026 8:42**Para:** soc.minminas <soc.minminas@rotorr.co>; Mesa de Ayuda <mesadeayuda@minenergia.gov.co>**Cc:** OSCAR SANCHEZ SANCHEZ <osanchez@minenergia.gov.co>; JUAN JOSE CEDEÑO LOPEZ <jjcedeno@minenergia.gov.co>; JOAN RENE CARVAJAL RAMIREZ <jrcarvajal@minenergia.gov.co>; OSCAR FABIAN RAMIREZ TORRES <oframirez@minenergia.gov.co>**Asunto:** RE: [TLP:RED]Network Scan - INC # 755446

Buenas tardes

Se realiza bloqueo del dispositivo personal en la red del Ministerio teniendo en cuenta que no es un comportamiento normal y tampoco esta permitido.

Cordialmente,

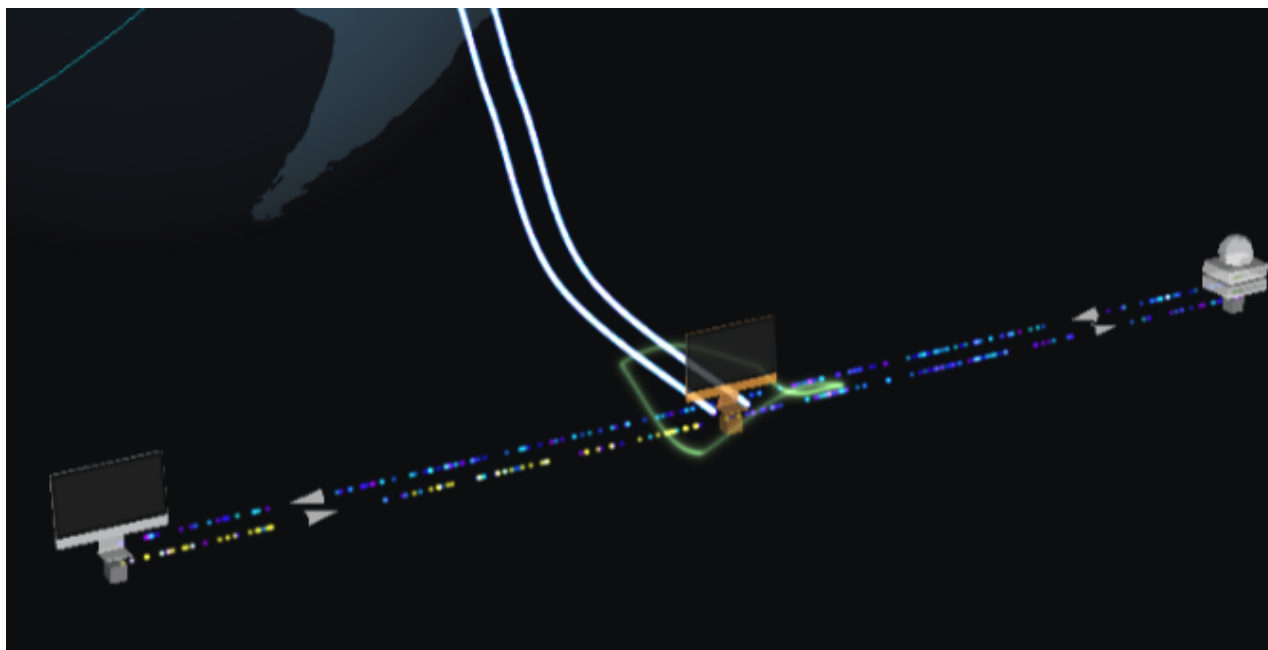
**De:** soc.minminas <soc.minminas@rotorr.co>**Enviado:** jueves, 5 de marzo de 2026 7:06**Para:** HERNAN HUMBERTO GARZON BONILLA <hhgarzon@minenergia.gov.co>; Mesa de Ayuda <mesadeayuda@minenergia.gov.co>**Cc:** OSCAR SANCHEZ SANCHEZ <osanchez@minenergia.gov.co>; JUAN JOSE CEDEÑO LOPEZ <jjcedeno@minenergia.gov.co>; JOAN RENE CARVAJAL RAMIREZ <jrcarvajal@minenergia.gov.co>; OSCAR FABIAN RAMIREZ TORRES <oframirez@minenergia.gov.co>**Asunto:** [TLP:RED]Network Scan - INC # 755446

TLP:RED

Cordial saludo,

Desde el **Centro de Operaciones de Seguridad** informamos que según la herramienta Darktrace se identificó una infracción en la cual un dispositivo ha sido visto escaneando la red, pero no está etiquetado como dispositivo de seguridad.

A continuación, el detalle:



Hostname: Diana

IP Address: 10.12.0.58 (Thu Mar 5, 06:00:00)

MAC Address: 38:8d:3d:86:87:35

Vendor: Wistron Neweb Corporation

Type: Desktop

Subnet: VLAN WIFI CORPORATIVO · 10.12.0.0/22

Thu Mar 5 2026, 06:45:37		All Events	
Thu Mar 5 2026, 06:43:34	▼ ▲ Diana triggered model	Device / Network Scan	
Thu Mar 5 2026, 06:43:33	▼ ➡ Diana failed to connect to 10.12.0.1		[1980]
A new failed connection to 10.12.0.1 on port 1980			
Thu Mar 5 2026, 06:43:33	▼ ➡ Diana failed to connect to 10.12.0.1		[2105]
A new failed connection to 10.12.0.1 on port 2105			
Thu Mar 5 2026, 06:43:33	▼ ➡ Diana failed to connect to 10.12.0.1		[1433]
A new failed connection to 10.12.0.1 on port 1433			
Thu Mar 5 2026, 06:43:30	▼ D Unusual Activity 50% due to Internal Connections to Closed Ports from Diana		
Thu Mar 5 2026, 06:43:29	▼ ➡ Diana failed to connect to 10.12.0.1		[135]
Thu Mar 5 2026, 06:43:29	▼ ➡ Diana failed to connect to 10.12.0.1		[21]
Thu Mar 5 2026, 06:43:29	▼ ➡ Diana failed to connect to 10.12.0.1		[23]
Thu Mar 5 2026, 06:43:29	▼ ➡ Diana failed to connect to 10.12.0.1		[53]
Thu Mar 5 2026, 06:43:29	▼ ➡ Diana failed to connect to 10.12.0.1		[22]
Thu Mar 5 2026, 06:43:29	▼ ➡ Diana failed to connect to 10.12.0.1		[8000]
Thu Mar 5 2026, 06:43:29	▼ ➡ Diana failed to connect to 10.12.0.1		[62078]
hu	▼ Filters	06:43:29	▼ ➡ Diana failed to connect to 10.12.0.1 [8080]

Observaciones:

- Por favor revisar si el dispositivo está permitido para realizar esta actividad.
- Agradecemos una retroalimentación sobre la infracción.
- De manera preventiva se activa el bloqueo de esta actividad por una hora, teniendo en cuenta que previamente se ha alertado en varias ocasiones el mismo modelo hacia esta IP de destino.
- El modelo Antigena **Network Scan** protege contra gusanos de red que intentan moverse lateralmente a través de una red, de manera preventiva se activa la confirmación de este bloqueo en la herramienta.

Cordialmente,



SOC

Security Operation Center

email: soc.minminas@rotorr.co

Corporación Rotorr – Motor de Innovación

Hemeroteca Universidad Nacional

Av. El Dorado No. 44^a – 40, Bogotá, Colombia, 111321

Teléfono:

TLP:RED



**MINISTERIO DE MINAS Y
ENERGÍA**