

 CARMEN EMILIA OSPINA Salud, bienestar y dignidad	FORMATO OFICIO			
PROCESO: GESTIÓN DEL DIRECCIONAMIENTO Y PLANEACIÓN ESTRATÉGICA	CODIGO: GE-S1-F12	VIGENCIA: 08/08/2023	V1	PÁGINA 1 de 4

9 MAYO 2025

**EMPRESA SOCIAL DEL ESTADO CARMEN EMILIA OSPINA
MUNICIPIO DE NEIVA**

EQUIPO AISLADO POR CONEXIÓN MALICIOSA

LUIS FERNANDO CORREA CALDERON

Buscamos la excelencia por su salud, bienestar y dignidad


LÍNEA AMIGA
863 2828


WHATSAPP
304 384 99 92


ESE Carmen Emilia Ospina

 CARMEN EMILIA OSPINA Salud, bienestar y dignidad	FORMATO OFICIO			
PROCESO: GESTIÓN DEL DIRECCIONAMIENTO Y PLANEACIÓN ESTRATEGICA	CODIGO: GE-S1-F12	VIGENCIA: 08/08/2023	V1	PÁGINA 2 de 4

1. REPORTE USUARIO FINAL

Desde centro de atencion Caimi reportan que el equipo activo No. 07309 no tiene acceso al internet, ni permite el acceso a indigo y aplicaciones de la institucion; el reporte se realizo por medio de mensaje de Whatapps al area Tics.

2. VERIFICACION Y REPORTE DEL AREA TIC

Desde el area Tic, se realiza la verificacion del entorno fisico, infraestructura y se valida con el el usuario final, es decir si la es debido a la conexión del equipo a la red, se determina que esta en forma adecuada; luego se procede a la validacion desde la consola del antivirus la cual nos reporta un aislado automatico del equipo por conexión maliciosa :

Endpoint Protection - 04182

Introducción / Panel de control de Endpoint Protection / Ordenadores / 04182



04182
Windows 10
IP: 192.168.6.39
Último usuario:
04182
Aislado automáticamente
Protección adaptativa contra
ataques

Actualizar ahora

Eliminar

RESUMEN | EVENTOS | ESTADO | POLÍTICAS

Eventos recientes

9 may. 2025 11:50	Dispositivo aislado automáticamente debido a estado de seguridad rojo
9 may. 2025 11:48	Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Windows\System32\svchost.exe' (Referencia de suport...
9 may. 2025 11:48	Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Program Files\Google\Chrome\Application\chrome.exe' (...)
9 may. 2025 11:48	Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Program Files\Google\Chrome\Application\chrome.exe' (...)
9 may. 2025 11:48	Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Program Files\Google\Chrome\Application\chrome.exe' (...)

Resumen del agente

Buscamos la excelencia por su salud, bienestar y dignidad

LÍNEA AMIGA
863 2828

WHATSAPP
304 384 99 92



ESE Carmen Emilia Ospina

 CARMEN EMILIA OSPINA Salud, bienestar y dignidad	FORMATO OFICIO			
PROCESO: GESTIÓN DEL DIRECCIONAMIENTO Y PLANEACIÓN ESTRATEGICA	CODIGO: GE-S1-F12	VIGENCIA: 08/08/2023	V1	PÁGINA 3 de 4

El equipo se pone en cuarentena automaticamente, con el fin de realizar la respectiva validacion del ataque al mismo; adicional se realiza una verificacion general de las ultimas 24 horas y se detecta que el evento inicio el **05/05/2025 03:03 a.m.** como se evidenciara en la imagen que a continuacion se adjunta.

ESE07309

Dispositivos / ESE07309



ESE07309
Windows 11
IP: 192.168.27.28
Último usuario:
07309
Aislado automáticamente
Protección adaptativa contra
ataques

RESUMEN EVENTOS ESTADO POLÍTICAS

Eventos recientes

5 may. 2025 3:05	Dispositivo aislado automáticamente debido a estado de seguridad rojo
5 may. 2025 3:03	Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Windows\System32\svchost.exe' (Referencia de soporte técnico: 0)
5 may. 2025 3:03	Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Program Files\Google\Chrome\Application\chrome.exe' (Referencia de soporte técnico: 0)
5 may. 2025 3:03	Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Program Files\Google\Chrome\Application\chrome.exe' (Referencia de soporte técnico: 0)
5 may. 2025 3:03	Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Program Files\Google\Chrome\Application\chrome.exe' (Referencia de soporte técnico: 0)

Como el incidente es repetitivo y por seguridad este equipo se debe formatear para una limpieza profunda de archivos del sistema.

Buscamos la excelencia por su salud, bienestar y dignidad

LÍNEA AMIGA
863 2828

WHATSAPP
304 384 99 92


 ESE Carmen Emilia Ospina

 CARMEN EMILIA OSPINA Salud, bienestar y dignidad	FORMATO OFICIO			
PROCESO: GESTIÓN DEL DIRECCIONAMIENTO Y PLANEACIÓN ESTRATEGICA	CODIGO: GE-S1-F12	VIGENCIA: 08/08/2023	V1	PÁGINA 4 de 4

Endpoint Protection - 04182

Introducción / Panel de control de Endpoint Protection / Ordenadores / 04182

ESE CARMEN



04182
Windows 10
IP: 192.168.6.39
Último usuario:
04182
Aislado automáticamente
Protección adaptativa contra ataques

Actualizar ahora
Eliminar

RESUMEN | EVENTOS | ESTADO | POLÍTICAS

Eventos recientes

9 may. 2025 11:50	Dispositivo aislado automáticamente debido a estado de seguridad rojo
9 may. 2025 11:48	Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Windows\System32\svchost.exe' (Referencia de suport...
9 may. 2025 11:48	Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Program Files\Google\Chrome\Application\chrome.exe' (...)
9 may. 2025 11:48	Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Program Files\Google\Chrome\Application\chrome.exe' (...)
9 may. 2025 11:48	Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Program Files\Google\Chrome\Application\chrome.exe' (...)

Resumen del agente

Endpoint Protection - 04182

Introducción / Panel de control de Endpoint Protection / Ordenadores / 04182

ESE CARMEN



04182
Windows 10
IP: 192.168.6.39
Último usuario:
04182
Aislado automáticamente
Protección adaptativa contra ataques

Actualizar ahora
Eliminar

RESUMEN | EVENTOS | ESTADO | POLÍTICAS

Eventos recientes

9 may. 2025 11:50	Dispositivo aislado automáticamente debido a estado de seguridad rojo
9 may. 2025 11:48	Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Windows\System32\svchost.exe' (Referencia de suport...
9 may. 2025 11:48	Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Program Files\Google\Chrome\Application\chrome.exe' (...)
9 may. 2025 11:48	Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Program Files\Google\Chrome\Application\chrome.exe' (...)
9 may. 2025 11:48	Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Program Files\Google\Chrome\Application\chrome.exe' (...)

Resumen del agente

Buscamos la excelencia por su salud, bienestar y dignidad

LÍNEA AMIGA
863 2828

WHATSAPP
304 384 99 92



ESE Carmen Emilia Ospina