

 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 3

27 ENERO 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 ESTRATÉGICA	CODIGO: GE-S1-F12	VIGENCIA: 08/08/2023	V1	PÁGINA 2 de 3

1. REPORTE USUARIO FINAL

Desde el servicio de urgencias del centro de salud Caimi, la jefe de turno de la mañana reporta que el equipo del consultorio No.3 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 :

Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Program Files\Google\Chrome\Application\chrome.exe' (Referenci...

Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Program Files\Google\Chrome\Application\chrome.exe'

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 **26/01/2025 0:07 a.m.** como se evidenciara en la imagen que a continuacion se adjunta.

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 3

SOPHOS Paneles de control Mis productos Centro de análisis de amenazas Alertas Informes Personas Dispositivos

ESE07314
Dispositivos / ESE07314



ESE07314
Windows 11
IP: 192.168.27.27
Último usuario:
07314
Aislado automáticamente
Protección adaptativa contra
ataques

Actualizar ahora
Eliminar
Más acciones

RESUMEN EVENTOS ESTADO POLÍTICAS

De Oct 29, 2024 A Jan 27, 2025
Especificar rango de fechas dentro de los últimos 90 días

Gravedad	Tipo	Fecha	Evento
1	Info	26 ene. 2025 0:08	Dispositivo aislado automáticamente debido a estado de seguridad rojo
3	Malware	26 ene. 2025 0:08	Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Windows\System32\svchost.exe' (Referencia de soporte técnico: ...)
3	Malware	26 ene. 2025 0:07	Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Windows\System32\svchost.exe' (Referencia de soporte técnico: ...)
3	Malware	26 ene. 2025 0:07	Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Windows\System32\svchost.exe' (Referencia de soporte técnico: ...)
3	Malware	26 ene. 2025 0:07	Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Windows\System32\svchost.exe' (Referencia de soporte técnico: ...)
3	Malware	26 ene. 2025 0:07	Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Program Files\Google\Chrome\Application\chrome.exe' (Referenci...
3	Malware	26 ene. 2025 0:07	Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Program Files\Google\Chrome\Application\chrome.exe' (Referenci...
3	Malware	26 ene. 2025 0:07	Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Program Files\Google\Chrome\Application\chrome.exe' (Referenci...
3	Malware	26 ene. 2025 0:07	Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Windows\System32\svchost.exe' (Referencia de soporte técnico: ...)
3	Malware	26 ene. 2025 0:07	Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Program Files\Google\Chrome\Application\chrome.exe' (Referenci...
3	Malware	26 ene. 2025 0:07	Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Program Files\Google\Chrome\Application\chrome.exe' (Referenci...
3	Malware	26 ene. 2025 0:07	Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Program Files\Google\Chrome\Application\chrome.exe' (Referenci...

Finalmente se realiza el escaneo total del equipo y se validara una vez su funcionalidad una vez terminado el tiempo de cuarentena.