
 <p>CARMEN EMILIA OSPINA Salud, bienestar y dignidad</p>	FORMATO OFICIO			
PROCESO: GESTIÓN DEL DIRECCIONAMIENTO Y PLANEACIÓN ESTRATEGICA	CODIGO: GE-S1-F12	VIGENCIA: 08/08/2023	V1	PÁGINA 1 de 3

03 FEBRERO 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**

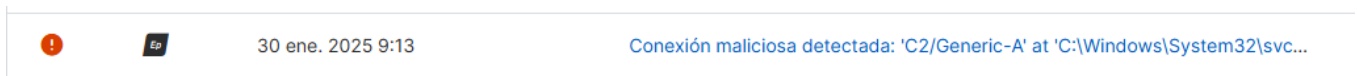
 <p>CARMEN EMILIA OSPINA Salud, bienestar y dignidad</p>	FORMATO OFICIO			
PROCESO: GESTIÓN DEL DIRECCIONAMIENTO Y PLANEACIÓN ESTRATEGICA	CODIGO: GE-S1-F12	VIGENCIA: 08/08/2023	V1	PÁGINA 2 de 3

1. REPORTE USUARIO FINAL



Desde el servicio de Odontología centro de salud Palmas reportan que el equipo activo No. 06328 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 :




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 **30/01/2025 9:13 a.m.** como se evidenciara en la imagen que a continuacion se adjunta.

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

ese6328
ESE CARMEN EMILIA OSPINA

Dispositivos / ese6328



ese6328
Windows 11
IP: 192.168.4.62
Último usuario:
06328
Aislado automáticamente
Protección adaptativa contra
ataques

Actualizar ahora

Eliminar

Más acciones

RESUMEN
EVENTOS
ESTADO
POLÍTICAS

De A
Especificar rango de fechas dentro de los últimos 90 días

[Ver informe de eventos](#)

Gravedad	Tipo	Fecha	Evento
i	Ea	30 ene. 2025 12:20	Escaneado "User Initiated Scan" completado
!	Ea	30 ene. 2025 9:14	Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Windows\System32\svc...
!	Ea	30 ene. 2025 9:13	Conexión maliciosa detectada: 'C2/Generic-A' at 'C:\Windows\System32\svc...
i	Ea	29 ene. 2025 13:48	Actualización realizada correctamente
i	Ea	28 ene. 2025 13:03	Actualización realizada correctamente

1 - 50 de 76 eventos
< >
Última actualización: 3 feb. 2025, 8:00

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

Nota: Equipo que 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