05 MAYO 2025

EMPRESA SOCIAL DEL ESTADO CARMEN EMILIA OSPINA
MUNICIPIO DE NEIVA

EQUIPO AISLADO POR CONEXIÓN MALICIOSA

LUIS FERNANDO CORREA CALDERON

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 mesaje 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 usario 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 **05/05/2025 03:03 a.m.** como se evidenciara en la imagen que a continuacion se adjunta.

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