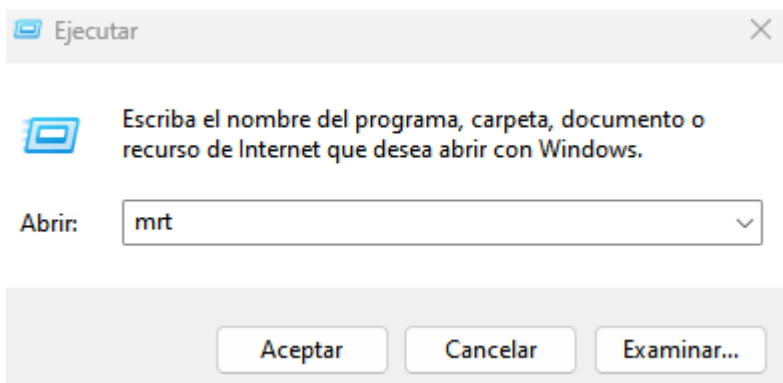


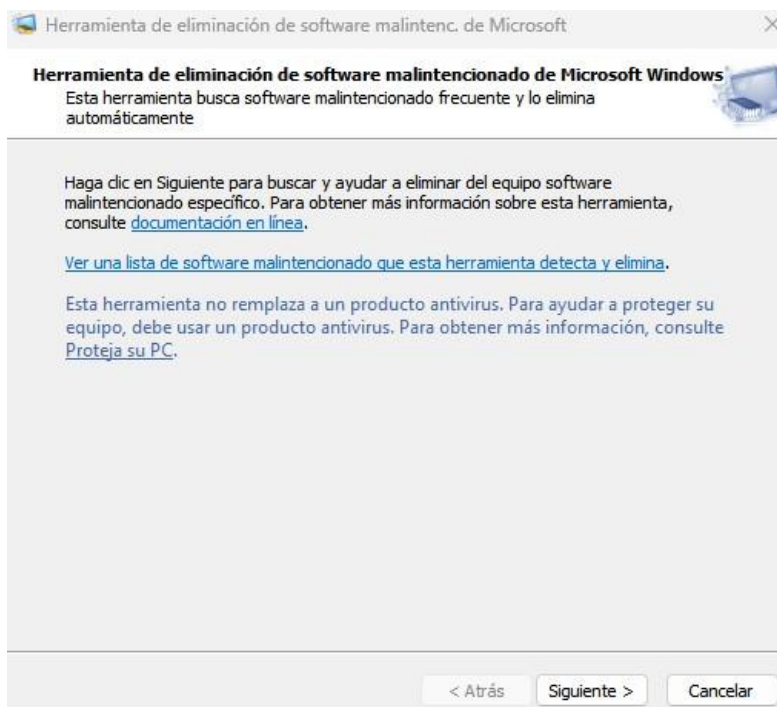
LABORATORIO # 1

HERRAMIENTAS DE ELIMINACION Y DETECCION DE MALWARE DE WINDOWS

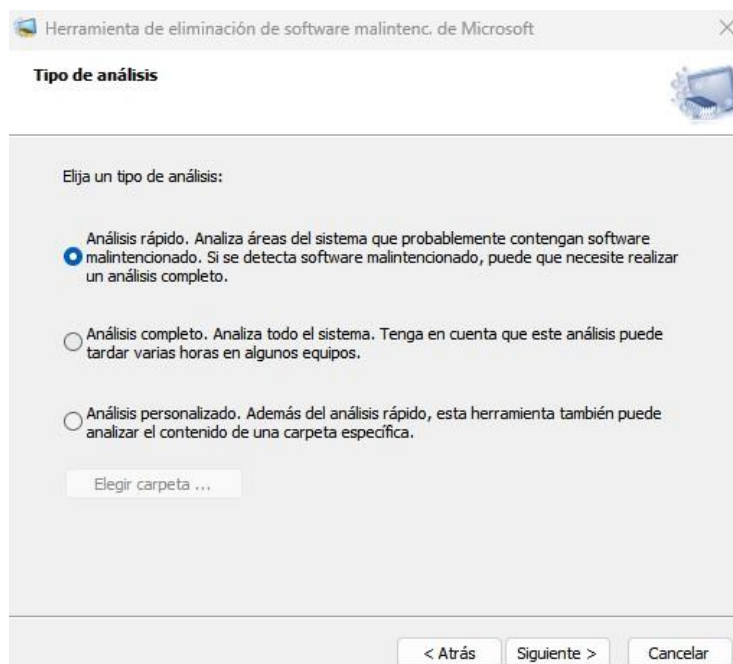
EJECUTAR MRT



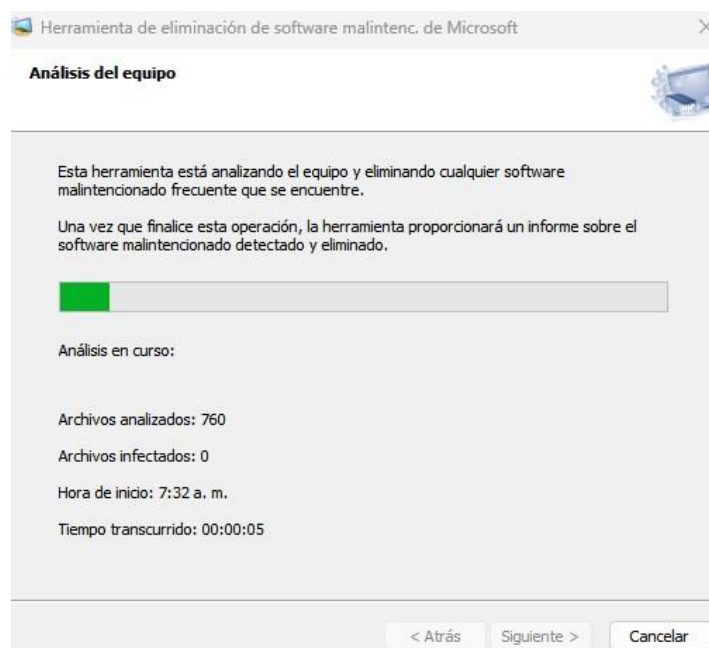
MRT EJCUTADO



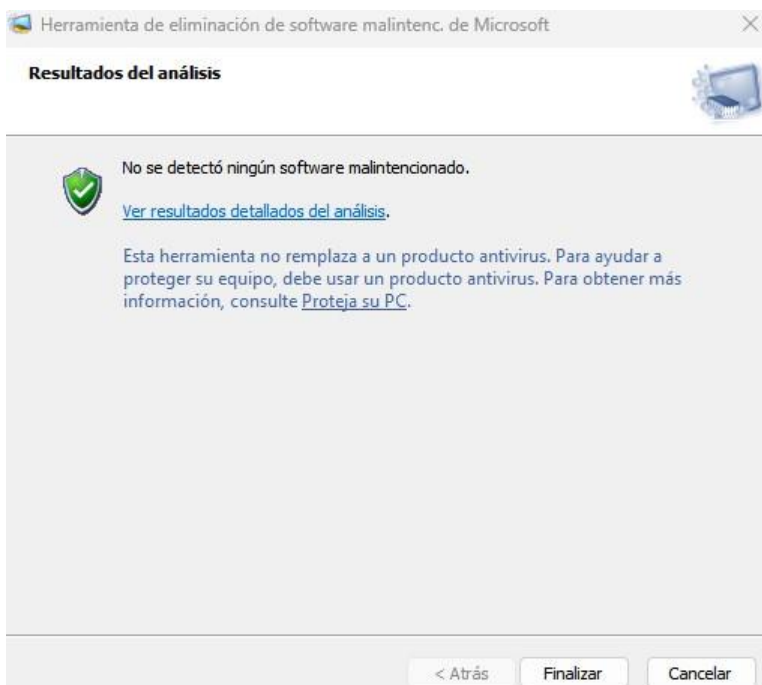
SELECCIÓN DEL TIPO DE ANÁLISIS



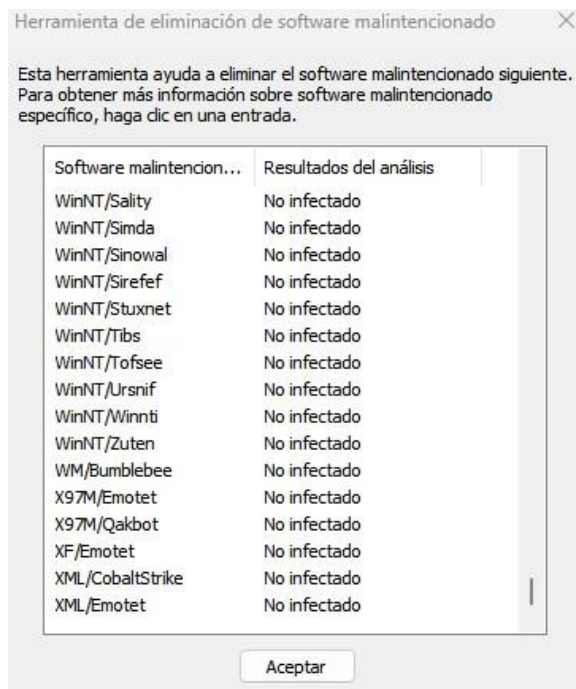
INICIO DEL ANÁLISIS



ANÁLISIS FINALIZADO



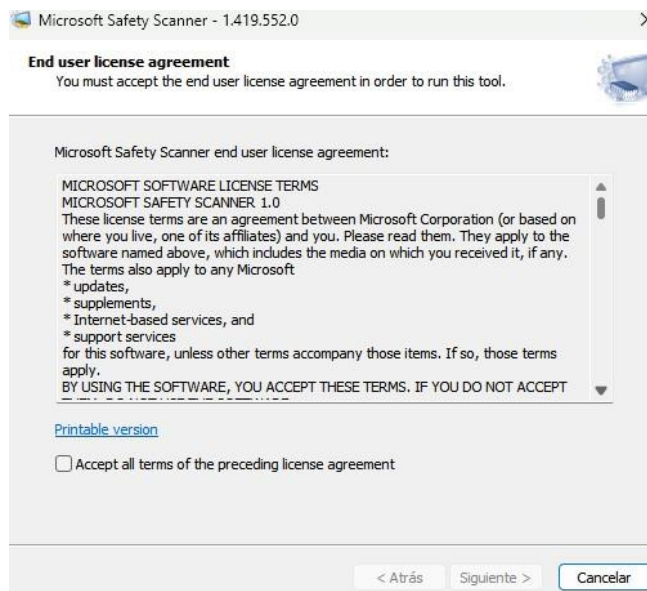
SUMARIO DE RESULTADOS



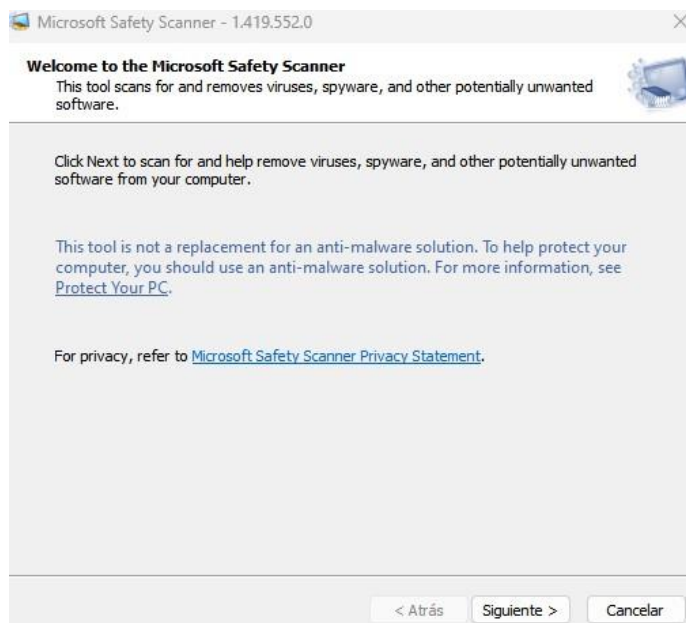
Una vez realizado y terminado el análisis muestra los resultados del mismo para el caso de mi computadora no se encontró software mal intencionado.

HERRAMIENTA MSERT

Uso de MSERT

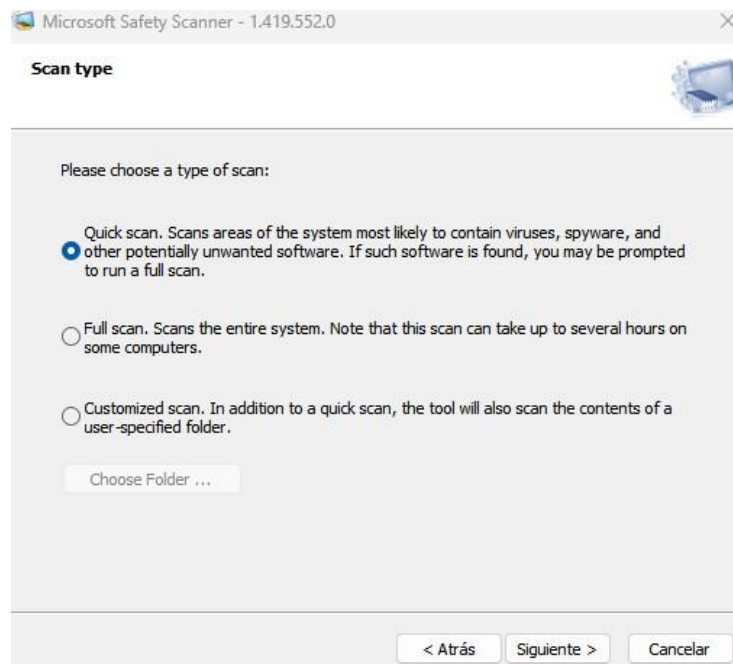


SE ACEPTAN LOS TERMINOS Y CONDICIONES

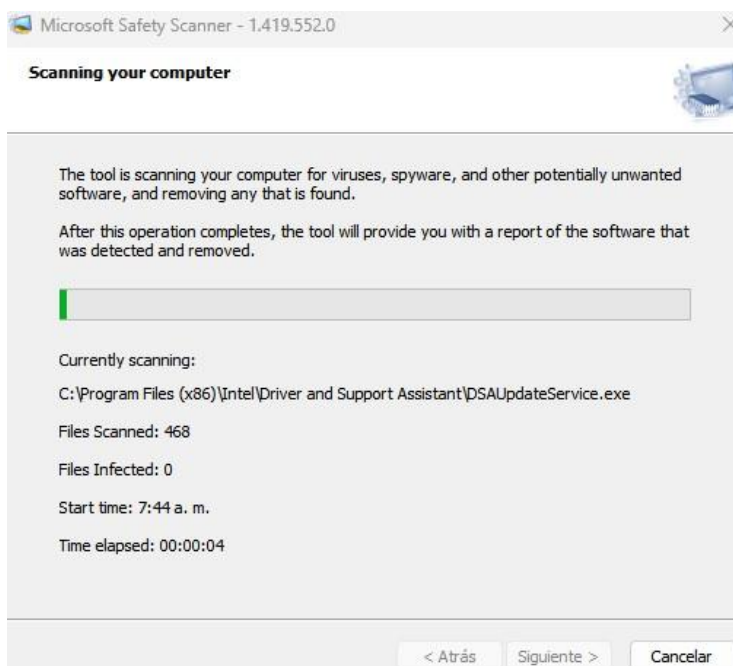


UNA VEZ ACEPTADO LOS TERMINOS Y CONDICIONES DAMOS CLICK EN SIGUIENTE

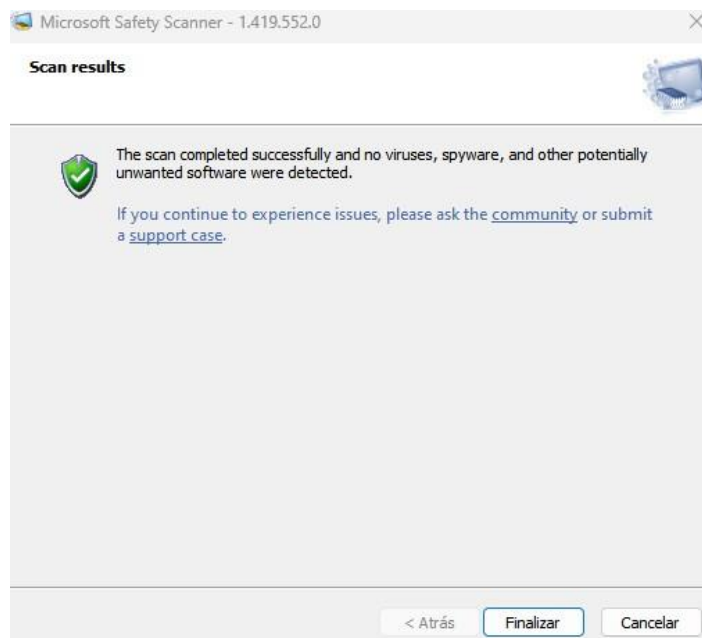
SELECCIÓN DEL TIPO DE ANÁLISIS



EJECUCIÓN DEL ANÁLISIS



RESULTADOS



CONCLUSIONES

MSERT No es una herramienta propia que se pueda obtener mediante el Windows update, la misma hay que descargarla de forma manual y se recomienda descargarla cada 10 días que es su tiempo de actualización a diferencia de MRT que si viene integrada con Windows y de actualización mensual.

MRT se utiliza para **eliminar software malicioso tipo malware residente** en la computadora en cambio MSERT se utiliza para la **detección de software malicioso activo** y el mismo se recomienda usarlo junto con Windows defender y **no ofrece un sumario de resultados** ambas herramientas son de uso manual y no representan una protección en tiempo real.