Seguridad Informática

UNACHI – FAC- DE ECONOMÍA – LIC. GESTIÓN DE T. I.

Prof. Andrés Miranda Cerceño

Septiembre de 2024

¿Qué es la Seguridad Informática?

La Seguridad Informática es una especialidad o disciplina con la disponibilidad de proteger la estructura de los computadores y todos los dispositivos electrónicos.

Dentro de la Protección de la Seguridad Informática, podemos destacar algunos conceptos, tales como:

- ✓ Salvaguardar la **confidencialidad** de los datos.
- ✓ Preservar la **integridad** de los datos.
- ✓ Generar la **disponibilidad** de datos para usuarios autorizados.
- ✓ Proteger la **autenticidad** de la información.

Objetivos de la Seguridad Informática

Confidencialidad:

Los ciberdelincuentes cada día utilizan métodos y herramientas que son una amenaza para la información de las empresas Privadas o Públicas.
Todo profesional del área de Tecnología, que tiene a su cargo la creación, implementación o de mantener la estructura de seguridad informática, debe tener claro lo importante que TODO es Confidencial.

Integridad:

Todo profesional en el área de Tecnología de ciberseguridad o Seguridad Informática es necesario asegurar que bajo ninguna circunstancia se pueden modificar los datos .
Es Importante tener claro que los datos tengan una seguridad, que estén protegidos de un borrado, además de otras prácticas como las copias de seguridad.

Disponibilidad:

Solo los usuarios o las personas que tengan la autorización, pueden acceder a los sistemas, los datos o informaciones, en el momento que se necesiten o se soliciten.

Organismos de Normalización Internacionales

Las siglas ISO/IEC se refieren a los organismos de normalización internacionales. ISO es la Organización Internacional de Normalización, y IEC es la Comisión Electrotécnica Internacional.

Estos organismos establecen estándares y certifican empresas que cumplen con altos estándares de calidad en sus procesos

ISO/IEC 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

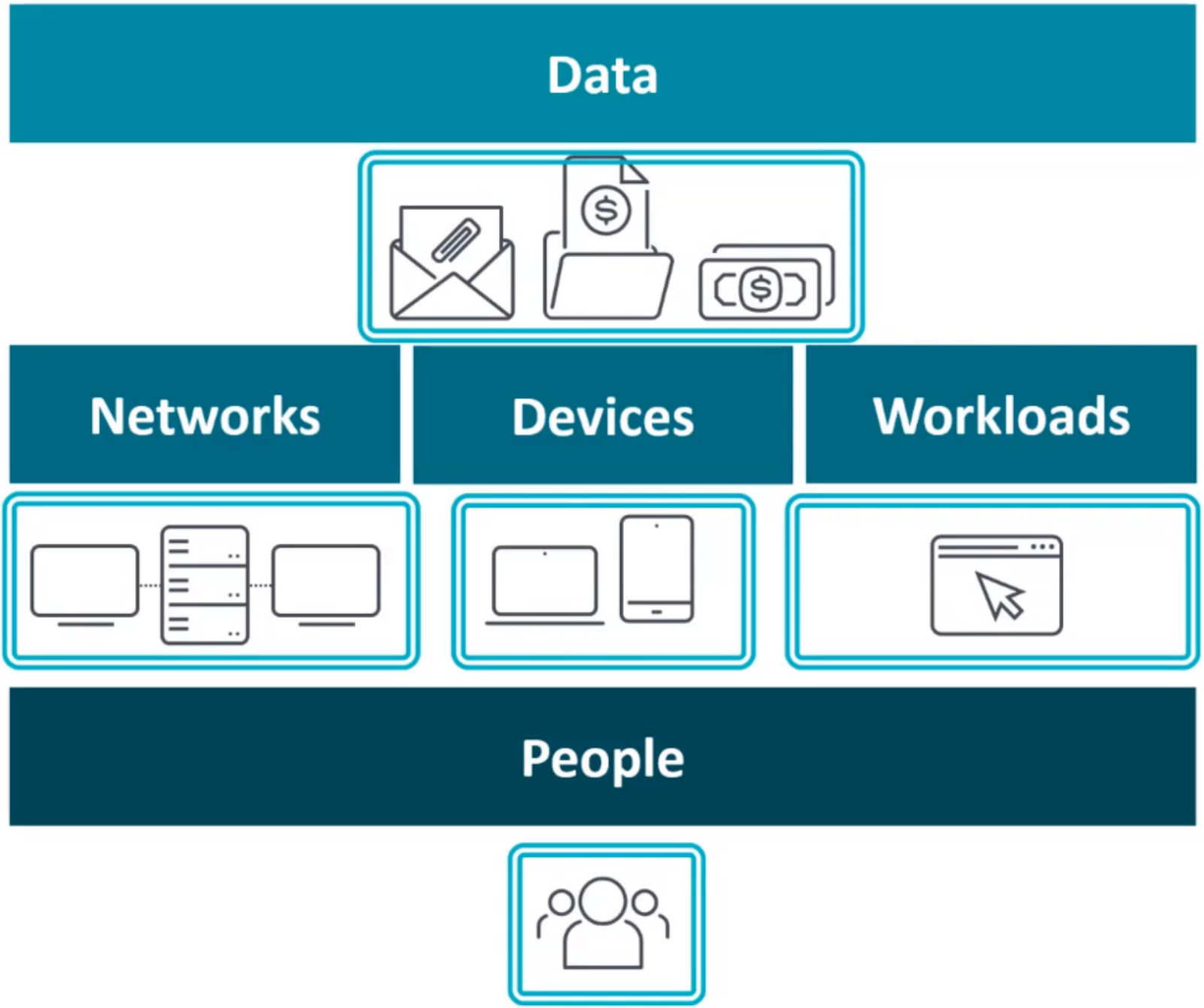
La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".

¿Qué es Zero Trust?

Forrester creó este concepto en 2010 en contraste con el modelo de seguridad tradicional que se basa en la premisa de **"confiar pero verificar".**

Zero Trust, en cambio, establece que las organizaciones nunca deben confiar en una entidad ya sea interna o externa. En otras palabras, **"nunca confíes, verifica siempre".**

El modelo Zero Trust crea seguridad en torno a cada uno de los recursos y entidades clave de una organización: datos, redes, dispositivos, cargas de trabajo y personas.



- ✓ VISIBILITY
- ✓ POLICIES
- ✓ AUTOMATION

¿Qué debe hacer una organización para implementar el modelo de confianza cero?

Hay tres áreas centrales de capacidad que una organización debe desarrollar a medida que implementas el **modelo Zero Trust:**

1. Visibilidad: identifique los dispositivos y recursos que se deben supervisar y proteger. No es posible proteger un recurso que no conoce. Tener visibilidad de todos sus recursos y puntos de acceso es indispensable.

2. Políticas: Establezca controles que solo permitan que personas específicas tengan acceso a recursos específicos en condiciones específicas. En otras palabras, se requiere un nivel granular de controles de directiva.

3. Automatización: Automatice los procesos para garantizar la correcta aplicación de las políticas y permitir que la organización se adapte rápidamente a cualquier desviación de los procedimientos estándar.

Basándose en las capacidades fundamentales descritas aquí, podemos definir Zero Trust como un modelo de seguridad que construye defensas alrededor de cada una de las siguientes entidades**: datos, redes, dispositivos, cargas de trabajo y personas.**

¿Cómo funciona una arquitectura de confianza cero o seguridad Zero Trust?

La **Implementación de Confianza Cero** implica requerir una verificación de identidad estricta para cada persona o dispositivo que intente acceder a la red o aplicación. Esta verificación se aplica independientemente de si el dispositivo o usuario ya está dentro del perímetro de la red.

La Superficie de Protección

La protección comienza identificando su superficie de protección, que se basa en datos, aplicaciones, activos o servicios, comúnmente referidos por el acrónimo **DAAS:**

- ✓ **Datos**: ¿Qué datos tiene que proteger?
- ✓ **Aplicaciones**: ¿Qué aplicaciones tienen información confidencial?
- ✓ **Activos**: ¿Cuáles son sus activos más sensibles?
- ✓ **Servicios**: ¿Qué servicios puede vulnerar un actor malicioso en un intento de interrumpir el funcionamiento normal de TI?

Establecer esta superficie de protección, le ayuda a perfeccionar exactamente lo que debe protegerse.

Una política de confianza cero o modelo Zero Trust, implica regular el tráfico relacionado con los datos y componentes críticos mediante la formación de microperímetros.

En el borde de un microperímetro, una red de confianza cero emplea una **Puerta de Enlace de Segmentación**, que monitorea la entrada de personas y datos. Aplica medidas de seguridad diseñadas para examinar exhaustivamente a los usuarios y datos antes de otorgar acceso utilizando un firewall de Capa 7 y el método Kipling.

Una regla de **Capa 7** implica inspeccionar la carga útil de paquetes para ver si coinciden con los tipos de tráfico conocidos.

Si un paquete contiene datos que no cumplen con los parámetros de la regla de **Capa 7**, el acceso se bloquea.

El método de Kipling cuestiona la validez del intento de participación haciendo seis preguntas sobre la participación y quién está tratando de ingresar: **¿Quién? ¿Qué? ¿Cuándo? ¿Dónde? ¿Por qué? ¿Cómo?** Si la respuesta a cualquiera de las

¿Qué es un escritorio como servicio (DaaS)?

Desktop-as-a-Service (DaaS) es una forma de ofrecer entornos completos de escritorios virtuales a los usuarios, incluidos sistemas operativos, aplicaciones, archivos y preferencias de usuario desde la nube. Los escritorios se ejecutan en **Virtual Machines** alojadas en una infraestructura de computación, almacenamiento y red administrada por el proveedor de la nube.

Los usuarios pueden acceder a su entorno de escritorio desde una amplia variedad de dispositivos, incluidos PC, computadoras portátiles, tabletas y algunos smartphones.

Muchas organizaciones buscan una alternativa al modelo tradicional de despliegue de escritorio, en el que los administradores de TI instalan un sistema operativo y aplicaciones en cada dispositivo de los empleados.

Con ese modelo, los administradores suelen gastar demasiado tiempo y dinero instalando software, administrando actualizaciones e intentando proteger los dispositivos.

DaaS versus infraestructura de escritorio virtual

Al igual que las ofertas de DaaS, las soluciones de infraestructura de escritorio virtual (VDI) ofrecen escritorios a dispositivos desde un centro de datos centralizado.

Con el modelo DaaS, la infraestructura de **cómputo, almacenamiento y red** son gestionadas por un proveedor de la nube.

La organización que proporciona escritorios a sus empleados puede administrar el **sistema operativo de escritorio, las aplicaciones, el software antivirus** y cualquier otra tarea relacionada con el escritorio, o trabajar con un proveedor de servicios de escritorio administrado por terceros.

UNIVERSIDAD AUTÓNOMA DE CHIRIQUÍ

FACULTAD DE ECONOMÍA

LICENCIATURA EN GESTIÓN DE TECNOLOGÍA DE INFORMACIÓN

Asignatura: *Seguridad Informática*

Código de Asignatura: 23674 Código: PROG 431

Profesor: *Andrés Miranda C.* **Fecha:** 1-oct.-2024

Parcial No. 1 – IIa. Parte - Investigación de Consecuencias, Herramientas y Protocolos en la Seguridad Informática

Ia. Parte. Mural de Vulnerabilidades Valor 50 Pts. **IIa. Parte. Investigación de Temas Valor 50 pts.**

Fecha de Entrega y Sustentación: 03-oct.-2024 **Valor Total: 100 pts.**

Nombre del Estudiante	Tema de Investigación
Amairanis S. / Rosemery G.	Fraudes Informáticos y Robos de Información / Protocolo: SSH
Agbert P. / Alain C.	El Cifrado de la Información y Protocolos Seguros / Ataques ARP Spooling
Ezequiel P. / Óscar P.	Criptografía Digital, Firma Digital, Cifrado, Autenticación / Bucanero / Lammer
Kevin A. / Yomar P.	Claves Simétricas y Asimétricas, Seguridad en Redes Inalámbricas / Insider / Grey Hat
Zaideth P. / Ameth S.	Criptografía Mixta: DES, AES / Protocolo: IP Security (IPSec)
Jesús D. / Brandon S.	Sistemas de Identificadores en las Comunicaciones / Ataques: CSRF / Listas: ABAC, RBAC
Juan G. / Onésimo A.	Conceptos RADIUS / VPN y Túnel DNS
Jonathan Sánchez	Beneficios e Importancia de SGSI, Técnicas en SHA / ScriptKiddie / Phreaker

Presentar su Sustentación estos puntos y otros.

Conceptos, Características, Importancias, Amenazas, Prevención, Ventajas, Desventajas, Vídeo Instruccional, Conclusiones, Recomendaciones.

¡Seguimos Avanzando…con la Ayuda de Dios!

UNIVERSIDAD AUTÓNOMA DE CHIRIQUÍ

FACULTAD DE ECONOMÍA

LICENCIATURA EN GESTIÓN DE TECNOLOGÍA DE INFORMACIÓN

Asignatura: *Seguridad Informática*

Código de Asignatura: 23674 Código: PROG 431

Profesor: *Andrés Miranda C.* **Fecha:** 12-sept.-2024

Proyecto No. 1 – Investigación de Consecuencias en las Vulnerabilidades Informáticas

I **19-sept.-2024** **Valor Total: 100 pts.**

Nombre del Estudiante	Tema de Investigación
Amairanis Saldaña	Ingeniería Social
Agbert Pitty	Inyección SQL
Ezequiel Pérez	Contraseñas Débiles
Alain Caballero C.	Bugs
Oscar Pérez	Vulnerabilidad – Cross Site Scripting(XSS)
Kevin Araúz	Botnet
Yomar Pineda	RansomWare
Zaideth Pinzón	RootKit
Ameth Saldaña	Robo de Identidad
Jesús Del Cid	Cibercrimen
Brandon Sanjur	Ataque DDoS
Juan García	Vulnerabilidad IDOR
Rosmery Guerrero	Academia AWS
Onésimo Arcia	IAM – Administración de identidad y Acceso
Jonathan Sánchez	Hacking Ético

Importante: **Los temas de Investigación está centrado a Vulnerabilidades.**

Presentar su Sustentación estos puntos y otros.

Conceptos, Consecuencias, Amenazas, Prevención, Ventajas, Desventajas, Vídeo Instruccional, Conclusiones, Recomendaciones.

¡Seguimos Avanzando…con la Ayuda de Dios!

UNIVERSIDAD AUTÓNOMA DE CHIRIQUÍ

FACULTAD DE ECONOMÍA

LICENCIATURA EN GESTIÓN DE TECNOLOGÍA DE INFORMACIÓN

Asignatura: *Seguridad Informática*

Código de Asignatura: 23674 Código: PROG 431

Profesor: *Andrés Miranda C.* **Fecha:** 11-Nov.-2024

Proyecto No. 2 –

Herramientas de Seguridad y su Implementación de Uso

Sustentación: 21-Nov. 2024 **Valor Total:** 100 pts.

Nombre del Estudiante	Tema de Investigación
Amairanis S., A. Pitty, A. Caballero	Bloquear y Desbloquear: App Lock
E. Pérez, O. Pérez, K. Araúz	Contraseñas Seguras: Bitwarden
Z. Pinzón, A. Saldaña, Y. Pineda	Escáner de Vulnerabilidades: Nikto
J. Del Cid, B. Sanjur, J. García	Antirrobo y Protección de Datos: Prey
R. Guerrero, O. Arcia, J. Sánchez	Escaneo - Network Mapper - Nmap

Importante: Los temas de Investigación Herramientas de Seguridad

Presentar su Sustentación estos puntos y otros.

Conceptos, Importancia, Uso y Aplicación, Ventajas, Desventajas, Vídeo Instruccional, Conclusiones, Recomendaciones.

¡Seguimos Avanzando…con la Ayuda de Dios!

Universidad Autónoma de Chiriquí
Facultad de Economía – Lic. en Gestión de Tecnología de Información
Departamento de Ciencias Computacionales

Asignatura: *Seguridad Informática*
Profesor: Andrés Miranda C. **Fecha: 17-octubre-2024**

Taller – Resumen del Congreso CESI 2024

F. Entrega y Sustentación: 7-Nov.-2024 **Valor: 100 pts.**

El estudiante redactará un documento identificando los diferentes temas en las conferencias que asistió durante la semana que se mantuvo el Congreso Economía, Sociedad e Innovación 2024, realizado del 21 al 25 de octubre de 2024. Mínimo cinco (5) conferencias y un (1) taller sobre las conferencias presentadas.

El formato para trabajar el documento constará de los siguientes puntos:

- ✓ **Fecha**
- ✓ **Hora**
- ✓ **Tema y Desarrollo**
- ✓ **Conclusiones**
- ✓ **Expositor**
- ✓ **Empresa o Entidad a la cual pertenece o representa**
- ✓ **Comentarios**

¡SEGUIMOS AVANZANDO…CON LA AYUDA DE DIOS!

UNIVERSIDAD AUTÓNOMA DE CHIRIQUÍ

FACULTAD DE ECONOMÍA

LICENCIATURA EN GESTIÓN DE TECNOLOGÍA DE INFORMACIÓN

Asignatura: *Seguridad Informática*

Código de Asignatura: 23674 Código: PROG 431

Profesor: *Andrés Miranda C.* Fecha: 22-agosto-2024

Investigación No. 2

Fecha de Entrega y Sustentación: 29-agosto-2024 Valor Total: 100 pts.

Nombre del Documento: INV2SINFysunombre

I. **De acuerdo con el listado de Herramientas sugeridas, busque los siguientes conceptos:**
   1. **Características**
   2. **Ventajas y Desventajas**
   3. **Costos de Implementación y asesoría**
   4. **Adiestramientos y certificaciones**
   5. **Otros**

Herramientas:

a. **Certificados SSL (A. Saldaña, A. Pitty, O. Arcia)**
b. **Escáneres de Vulnerabilidades (E. Pérez, A. Concepción)**
c. **Encriptadores (O. Pérez, K. Araúz, Y. Pineda)**
d. **Servidores Proxy (Z. Pinzón, A. Saldaña)**
e. **Antispyware (J. Del Cid, R. Guerrero)**
f. **Firewall (B. Sanjur, J. García)**

II. **Presentación**
   a. **Deberá crear una presentación de la Investigación y la implementación de la Herramienta.**

Emita sus consideraciones de la Herramienta y sus conclusiones.

¡Seguimos Avanzando…con la Ayuda de Dios!

UNIVERSIDAD AUTÓNOMA DE CHIRIQUÍ
FACULTAD DE ECONOMÍA
LICENCIATURA EN GESTIÓN DE TECNOLOGÍA DE INFORMACIÓN

Asignatura: ***Seguridad Informática***
Código de Asignatura: 23674 Código: PROG 431
Profesor: ***Andrés Miranda C.*** Fecha: 17-octubre-2024

Laboratorio No. 1

Fecha de Entrega y Sustentación: 17-octubre-2024 Valor Total: 100 pts.

Herramientas:

1. **MRT - (Malicious Software Removal Tool – MSRT) - Herramienta de Eliminación de Software Malintencionado**: es una herramienta gratuita de Microsoft que elimina el software malintencionado que pueda estar presente en el sistema operativo Windows.
   MRT encuentra y elimina las amenazas e invierte los cambios que estas han llevado a cabo.
   Para ejecutar MRT, se puede usar el comando MRT en el cuadro de búsqueda de Windows.
   Para hacer: Ejecutar y sacar sus conclusiones de los resultados encontrados.

2. **MSERT: Microsoft Support Emergency Response Tool (MSERT - Herramienta de respuesta a emergencias de soporte técnico de Microsoft**) es una herramienta antimalware portátil e independiente que incluye firmas de Microsoft Defender para buscar y eliminar el malware detectado.

   MSERT es un escáner a demanda que no proporcionará ninguna protección a tiempo real. Por lo tanto, solo debes usarlo para análisis puntuales y no debes confiarte de él, como si de un programa antivirus se tratase.
   Para hacer: Ejecutar y sacar sus conclusiones de los resultados encontrados.

Importante: Elabore un documento del Informe, con los resultados encontrados y sus conclusiones con respecto a las herramientas de escaneo presentadas.

Nota: Este trabajo debe ser presentado y sustentado en la fecha especificada, de lo contrario NO tiene derecho al valor asignado.

Consideraciones especiales de las herramientas:

Ventajas de MRT:

Gratuito: No se requiere ningún pago adicional para acceder a esta herramient
Actualizaciones regulares: Microsoft lanza actualizaciones mensuales para mantener el softwar actualizado y efectiv
Desarrollado por Microsoft: Al ser creado por el mismo fabricante del sistema operativo, se espera qu MRT funcione sin problemas y sea compatible con Windows, lo que brinda una sensación de confianza

Desventajas de MRT:

Limitaciones de funcionalidad: MRT se centra principalmente en la eliminación de malware y puede carecer de funciones avanzadas que ofrecen las soluciones antivirus completas
No es un reemplazo completo para un antivirus: Aunque MRT proporciona cierta protección, no garantiza una defensa completa contra todas las amenazas de seguridad.
Dependencia de las actualizaciones de Microsoft: La eficacia de MRT depende de las actualizaciones periódicas de Microsoft, lo que puede generar una brecha de protección hasta que se lancen las actualizaciones.

Cómo usar MRT;

La utilización de MRT es bastante sencilla. Si estás utilizando una versión reciente de Windows, probablemente ya esté preinstalada en tu sistema. Sin embargo, también puedes descargarla desde la página oficial de Microsoft. Para acceder a ella, simplemente busca la herramienta «MRT» en el sistema y ejecútala. También puedes ejecutarla a través de la PowerShell, CMD o la ventana de ejecutar.

Hay 3 tipos de escaneo disponibles:

- ✓ **Análisis rápido**: Un análisis rápido de la memoria y los archivos del sistema que pueden estar infectados con mayor frecuencia. Si se detecta un virus o un troyano, la herramienta ofrecerá realizar un análisis completo;
- ✓ **Análisis completo:** Un análisis completo del dispositivo (puede llevar varias horas dependiendo de la cantidad de archivos en un disco);
- ✓ **Escaneo personalizado:** En este modo puede especificar una carpeta para escanear.

¡SEGUIMOS AVANZANDO...CON LA AYUDA DE DIOS!