www.eysglobal.com

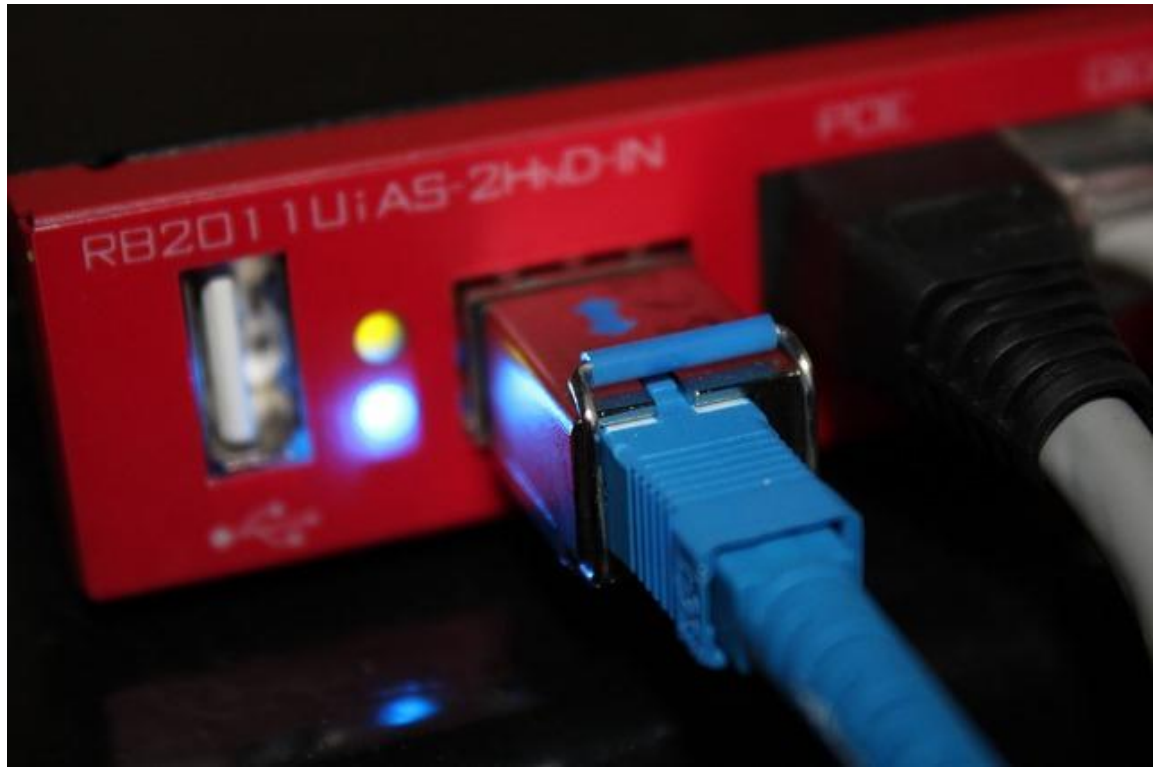
CURSO DE INFORMÁTICA FORENSE

MÓDULO 3
Protección de terminales

Protección antimalware

Amenazas a terminales

Protección de malware basada en hosts



Protección de malware basada en la red

- Los dispositivos de prevención de malware basados en la red son capaces de compartir información entre ellos para permitir que se tomen mejores decisiones.
- La protección de terminales en una red sin fronteras puede lograrse usando técnicas basadas en la red y basadas en los hosts

Protección contra intrusiones basada en hosts

INFORMÁTICA FORENSE

Productos HIDS

Seguridad de las aplicaciones

Evaluación de vulnerabilidades de terminales

Perfiles de redes y servidores

Sistema de puntuación de vulnerabilidades comunes (CVSS)

El proceso de CVSS

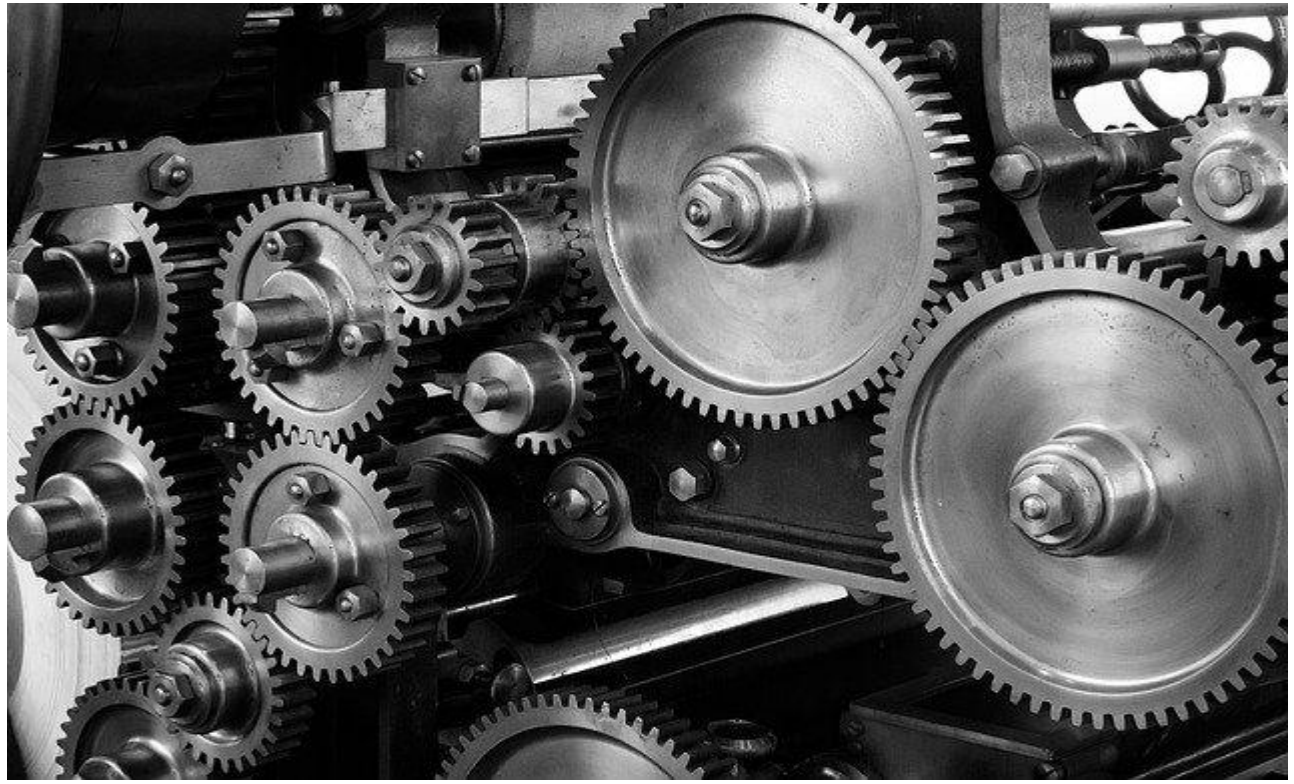
- Después, los valores de las métricas temporales y del entorno modificarán los resultados de las métricas básicas para proporcionar una puntuación general.

Administrador de dispositivos de seguridad

Gestión de riesgos

- La gestión de riesgos implica seleccionar y especificar controles de seguridad para una organización.

Administración de configuraciones



Técnicas de administración de parches

Sistemas de administración de seguridad de la información

Marco de ciberseguridad de NIST

- **NIST Cybersecurity Framework** – Conjunto de normas diseñadas para integrar estándares, pautas y prácticas existentes con el fin de mejorar la administración y reducción del riesgo de ciberseguridad.
- La siguiente tabla describe las funciones principales de NIST Cybersecurity Framework