INSTITUTO POLITÉCNICO NACIONAL
SECRETARIA ACADÉMICA
DIRECCIÓN DE EDUCACION MEDIA SUPERIOR
CENTRO DE ESTUDIOS CIENTÍFICOS Y TECNOLÓGICOS No. 13
"RICARDO FLORES MAGÓN"

G U Í A

d e e s t u d i o p a r a
presentar ETS de la
UNIDAD DE APRENDIZAJE
SOFTWARE MALICIOSO

Semestre 2023-2
TURNO VESPERTINO

Integrantes de la academia: **Alfredo Campos Guerrero**

Fecha de Elaboración: **12/06 /2023**

FORMATO DE LA GUÍA DE ESTUDIO

Área:	Nombre de la Unidad de Aprendizaje:	Nivel/semestre:
Tecnológica	**Software Malicioso**	**Sexto**

Instrucciones generales de la guía:

Anotar aspectos que el alumno debe considerar antes de presentar el examen:

- Esta guía no tiene ningún valor sobre la calificación final

Presentación:

Los ciberataques en la actualidad son una amenaza para las distintas organizaciones (públicas o privadas) ya que afecta directamente a la información que es fundamental para su funcionamiento; esta unidad de aprendizaje contribuye a entender la importancia, el impacto y las consecuencias que tiene un software malicioso en la actualidad; así como crear políticas y protocolos que ayuden a prevenir y mitigar estos ataques. Reconocer que, con la misma rapidez y agilidad, que las empresas han buscado adaptarse a un nuevo entorno, los ciberataques también se han sofisticado, de manera que la única forma que tendrán las empresas para consolidar sus planes de crecimiento de mediano y largo plazo, dependerán del enfoque y medidas de ciberseguridad para garantizar el día a día de la operación. Introduce al campo conceptual y procedimental que posibilite al estudiante contar con una visión crítica del marco regulatorio permitiendo frenar el crecimiento exponencial de cualquier código malicioso que se infiltre en un equipo.

Objetivos

Los principales objetos del conocimiento que se adquirirán y serán cuerpo de las acciones o desempeños a realizar son:

- Analizar un caso práctico de un ataque provocado a un equipo derivado de un código malicioso
- Mencionar la actividad preventiva y correctiva a realizar en dicho ataque.
- Formulación de un plan de mejora continua para prevenir ataques por software malicioso
- Implementar un plan de trabajo de actividades preventivas y correctivas por software malicioso

Justificación

Las competencias profesionales (generales y particulares) implican como principales objetos de conocimiento la auditoría informática por medio de las bases metodológicas, que podrá vincular con su entorno socioeconómico y laboral. Asimismo, en la particularidad del estudiante:

- Diseña un plan o programa de trabajo para llevar a cabo actividades preventivas y correctivas provocadas por software malicioso
- Hacer uso de herramientas informáticas que permiten llevar a cabo una limpieza del sistema operativo, paquetería o archivos que pudiera infectarse y dañar el equipo o información

Materiales para la elaboración de la guía

No Aplica

Estructura y contenidos

I. Distingue tipos, características y fases de un malware, así como riesgos más comunes, a través de los servicios de análisis y detección de seguridad en el software.

- Tipos de malware y su ámbito de operación.
  - Entornos objetivo.
  - Objetos portadores.
  - Mecanismos de transporte.
- Importancia y tipos de Antivirus.
- Información de servicios de análisis diario.
- Tipos de análisis estático y de comportamiento de un antivirus.
- Riesgos frecuentes (impacto, naturaleza y normativas)
- Vulnerabilidades de un activo ante un malware.
- Medidas preventivas y correctivas en la aplicación de un antivirus

II. Aplica buenas técnicas de navegación para preservar la seguridad de la información

- Dispositivos de seguridad en redes públicas y privadas.
- Filtrado de información segura a través de las telecomunicaciones.
- Alcance y consecuencias del malware.
- Aplica contramedidas del malware:
  - Análisis de marcas de antimalware.
  - Instalación y mantenimiento de antimalware
  - Antimalware para dispositivos de escritorio y móviles.
  - Antimalware basado en la nube.
  - Seguridad de Puertos dentro de redes públicas y privadas.
  - Configuración de seguridad de dispositivos en red.
  - Normas de seguridad del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE).
  - Troubleshooting.

III. Gestiona el fortalecimiento de una navegación segura con el fin de mitigar malware, dentro una organización de acuerdo a la normatividad vigente.

- Códigos de ética y tipos de navegantes para la seguridad en la información.
- Estándar de la IEEE para ciberseguridad.
- Conoce usos y costumbres en la navegación.
- Aplica políticas para las buenas prácticas.
- Aplica protocolos de navegación segura.
- Distingue el Sistema de Gestión de Seguridad de la Información (SGSI).
- Distingue estándares internacionales que permiten el aseguramiento, confidencialidad e integridad de datos e información (ISO 27000).

Actividades de estudio

- Repaso de conceptos teóricos en esta guía detallados
- Se recomienda estudiar los siguientes temas:
  - ✓ Tipos de malware y su ámbito de operación.
  - ✓ Importancia y tipos de Antivirus.
  - ✓ Información de servicios de análisis diario.
  - ✓ Tipos de análisis estático y del comportamiento de un antivirus.
  - ✓ Riesgos frecuentes (impacto, naturaleza y normativas)
  - ✓ Vulnerabilidades de un activo ante un malware.
  - ✓ Medidas preventivas y correctivas en la aplicación de un antivirus.
  - ✓ Dispositivos de seguridad en redes públicas y privadas.

- ✓ Filtrado de información segura a través de las telecomunicaciones.
- ✓ Alcance y consecuencias del malware.
- ✓ Análisis de marcas de antimalware.
- ✓ Instalación y mantenimiento de antimalware
- ✓ Antimalware para dispositivos de escritorio y móviles.
- ✓ Antimalware basado en la nube.
- ✓ Seguridad de puertos dentro de redes públicas y privadas.
- ✓ Configuración de seguridad de dispositivos en red.
- ✓ Normas de seguridad del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE).
- ✓ Troubleshooting.

Información Adicional

- Ninguna

Bibliografía Básica

- Malware Analysis Techniques: Tricks for the triage of adversarial software. Packt Publishing. Barker, D. (2021, June 18).
- https://scholar.google.com.mx/scholar?q=(autores,+2021)+malware&hl=en&as_sdt=0&as_vis=1&oi=scholart. (n.d.). Retrieved September 8, 2022, from
- Sikorski, M., & Honig, A. (2012, February 1). Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software (1st ed.). No Starch Press.