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 DE LA INFORMACIÓN
Semestre 2026-2
TURNO MATUTINO

Integrantes de la academia: María de Lourdes Garcés Vanegas

Fecha de Elaboración: __20/abril/26

FORMATO DE LA GUÍA DE ESTUDIO

Área:	Nombre de la Unidad de Aprendizaje:	Nivel/semestre:
Tecnológica	**SOFTWARE MALICIOSO**	**Medio/SEXTO**

Instrucciones generales de la guía:

Esta guía tiene como objetivo prepararte para el examen ETS de la unidad de aprendizaje Software Malicioso.

Para aprovecharla al máximo:

- **Estudia los conceptos clave y asegúrate de comprenderlos, no solo memorizarlos.**
- **Resuelve los ejercicios de autoevaluación sin apoyo y verifica tus respuestas.**
- **Analiza los casos prácticos como si fueras un analista de ciberseguridad real.**
- **Relaciona los temas con situaciones reales (empresas, ataques, noticias).**
- **Organiza tu tiempo de estudio en sesiones cortas (30–40 min).**

Esta guía está enfocada en el desarrollo de habilidades prácticas para el examen.

Presentación:

Esta guía está diseñada para ayudar a los estudiantes a prepararse para el examen ETS de la Unidad de Aprendizaje Software Malicioso de la Información. Incluye conceptos clave, preguntas de opción múltiple, casos prácticos y recomendaciones para comprender mejor los temas centrales del programa de estudios.

Objetivos

Desarrollar en el estudiante la capacidad de identificar, analizar y mitigar amenazas de software malicioso, mediante el uso de modelos de seguridad, herramientas de protección y estrategias de defensa aplicadas a entornos reales.

Justificación

La presente guía de estudio está diseñada para proporcionar a los estudiantes un recurso completo y estructurado que les permita prepararse adecuadamente para el examen ETS de la Unidad de Aprendizaje Software Malicioso. Esta guía combina conceptos teóricos, ejercicios prácticos, enfocándose en las competencias clave establecidas en el programa oficial.

El objetivo principal es desarrollar los conocimientos para identificar los ciberataques que 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. La guía permite a los estudiantes reforzar sus conocimientos y desarrollar una visión integral para enfrentar con éxito el examen..

Estructura y contenidos

- **Conceptos Clave**
- **Casos Prácticos**
- **Recomendaciones de Estudio**

Evaluación

Sin valor.

Materiales para la elaboración de la guía

- Computadora o dispositivo móvil: Para acceder a recursos en línea y realizar investigaciones.
- Manuales y guías de seguridad informática: Incluyendo estándares como ISO 27001, COBIT e ITIL.
- Libros de texto recomendados: Relacionados con seguridad de la información.
- Acceso a Internet: Para investigaciones y consultas en bases de datos académicas.
- Cuaderno y bolígrafos: Para realizar anotaciones y esquemas.

Actividades de estudio

I. Conceptos Clave

Unidad 1: Seguridad de la Información

Aprendizaje Esperado 1: Naturaleza del Malware

1. ¿Qué es el Malware?

- Es cualquier código diseñado para infiltrarse en un dispositivo sin permiso.
- Dato Clave: El malware se clasifica por su Mecanismo de Propagación (cómo se mueve) y su Carga Útil/Payload (qué daño hace).

2. Los "Tres Grandes" (Clasificación Básica)

Tipo	¿Cómo se mueve?	Característica Principal
Virus	Necesita que un humano lo ejecute (dar clic a un archivo).	Se "pega" a programas sanos.
Gusano (Worm)	Se mueve solo a través de la red (WiFi o Ethernet).	No necesita ayuda humana para infectar toda la oficina.
Troyano	Engaña al usuario.	Parece algo bueno (un juego, un crack) pero esconde la amenaza.

Aprendizaje Esperado 2: Riesgos y Vulnerabilidades

1. La Triada de la Seguridad (C-I-D)

- Cuando un malware ataca una empresa, rompe una de estas tres cosas:
- Confidencialidad: El malware roba datos (ej. Spyware).
- Integridad: El malware cambia o borra archivos (ej. Virus).
- Disponibilidad: El malware bloquea el acceso (ej. Ransomware).

2. ¿Qué es una Vulnerabilidad?

- Es la "puerta abierta" que usa el malware. Las más comunes para el examen son:
- Software desactualizado (falta de parches).
- Uso de memorias USB sin escanear.
- Contraseñas débiles (ej. 123456).

Práctica

1. Identificación Visual:

   Si ves un archivo llamado tarea.pdf.exe, el alumno debe identificar que es sospechoso por la doble extensión.

2. Uso de la Consola (CMD):

   Comando vital: dir /ah. Sirve para ver archivos que el malware puso como "Ocultos" o de "Sistema".

3. Identificación de Procesos:

   Si en el Administrador de Tareas ves algo llamado svch0st.exe (con un cero), es un impostor de un proceso real del sistema.

Ejercicios de Autoevaluación:

Caso: Un empleado de una empresa particular recibe un correo con una factura. Al abrirla, todos sus archivos se bloquean y le piden dinero.

Pregunta: ¿Qué tipo de malware es?

Respuesta: Ransomware

Pregunta: ¿Qué pilar de la seguridad se rompió?

Respuesta: Disponibilidad

Herramientas: Si sospechas que hay un virus escondido en una USB, ¿qué comando escribes en la terminal para verlo?

Respuesta: dir /ah.

Unidad 2: Tendencias Modernas y Defensa de la Infraestructura

Aprendizaje Esperado 1: Tendencias Modernas

1. Malware Fileless (Sin archivos)

Es la tendencia más importante. A diferencia de los virus viejos, este no se guarda en el disco duro.

• Cómo funciona: Vive solo en la memoria RAM y usa programas que ya están en la computadora (como PowerShell) para atacar.

• Por qué es peligroso: Si el alumno solo busca archivos con dir /ah, no encontrará nada.

• Concepto clave: "El enemigo invisible".

2. APT (Amenaza Persistente Avanzada)

No es un virus rápido, es un ataque planeado.

Objetivo: Robar información de empresas o gobierno (como la DGETIC) durante mucho tiempo sin que nadie se dé cuenta.

Característica: Es paciente y silencioso.

3. MaaS (Malware como Servicio)

Ahora los criminales no necesitan saber programar; "rentan" el malware en internet, como si fuera una suscripción de streaming.

Aprendizaje Esperado 2: Contramedidas y Mitigación

1. De Antivirus a EDR (La evolución)

Antivirus Tradicional: Busca "fotos" de virus conocidos (Firmas). Si el virus es nuevo, no lo ve.

EDR (Endpoint Detection and Response): Es un detective. No le importa cómo se llame el programa, sino qué está haciendo. Si un programa intenta cifrar archivos, el EDR lo detiene de inmediato.

2. El Sandbox (Caja de Arena)

Es un entorno virtual aislado.

Para qué sirve: Para ejecutar un archivo sospechoso y ver qué hace sin que infecte la red real de la empresa.

Metáfora: Es como probar una granada dentro de un búnker de acero.

3. Honeypot (Tarro de Miel)

• Es un servidor falso que parece tener información valiosa (como nóminas o presupuestos).

Objetivo: Engañar al atacante para que entre ahí, así el auditor puede estudiar sus técnicas sin que toque los datos reales.

Unidad 3: Diseño y Análisis de los Modelos de Seguridad

- Gestión de la Seguridad: Incluye estrategias, procesos y métricas. Procesos de Implementación: Planificación y aplicación de modelos según normas vigentes.

II. Preguntas de Opción Múltiple

1. ¿Qué representa la integridad en la seguridad de la información?

A) Protección frente a usuarios externos

B) Evitar la modificación no autorizada de los datos (Correcta)

C) Garantizar el acceso a los datos las 24 horas

D) Proteger el equipo físico

2. ¿Qué modelo se centra en el control de acceso basado en niveles de confidencialidad?

A) Modelo TG (Take GranT)

B) Modelo BLP (Bell-Lapadula) (Correcta)

C) ISO 27001

D) COBIT

3. ¿Cuál es un ejemplo de malware?

A) Contraseña segura

B) Firewalls

C) Virus informático (Correcta)

D) Políticas de acceso

4. ¿Qué principio se ve comprometido en un ataque de denegación de servicio (DoS)?

A) Confidencialidad

B) Integridad

C) Disponibilidad (Correcta)

D) Privacidad

5. ¿Qué estándar se utiliza para la gestión de la seguridad de la información?

A) ISO 27001 (Correcta)

B) GDPR

C) ITIL

D) COBIT

6. ¿Qué acción corresponde a la gestión de la seguridad?

A) Monitorear redes sociales

B) Definir estrategias y métricas de seguridad (Correcta)

C) Eliminar antivirus

D) Compartir datos sin control

7. ¿Qué modelo gestiona permisos y privilegios de acceso?

A) BLP (Bell-Lapadula)

B) TG (Take GranT) (Correcta)

C) Clark-Wilson

D) Matriz de accesos

8. ¿Qué principio de seguridad asegura que solo usuarios autorizados accedan a la información?

A) Disponibilidad

B) Confidencialidad (Correcta)

C) Integridad

D) Autenticación

9. ¿Qué estándar define buenas prácticas de gestión de servicios de TI?

A) COBIT

B) ITIL (Correcta)

C) ISO 9001

D) GDPR

10. ¿Qué tipo de ataque implica el robo de datos mediante engaño a usuarios?

A) Phishing (Correcta)

B) Ransomware

C) DoS

D) Keylogger

11. ¿Qué técnica garantiza la disponibilidad de datos en caso de fallo del sistema?

A) Cifrado de datos

B) Realización de copias de seguridad (Correcta)

C) Control de acceso

D) Uso de firewalls

12. ¿Qué significa implementar una política de seguridad en una empresa?

A) Eliminar datos confidenciales

B) Definir reglas y procedimientos de protección (Correcta)

C) Dar acceso a todos los empleados

D) Desactivar sistemas de seguridad

13. ¿Qué tipo de malware bloquea el acceso a los datos hasta recibir un pago?

A) Spyware

B) Ransomware (Correcta)

C) Adware

D) Keylogger

14. ¿Qué técnica permite verificar si los datos han sido alterados?

A) Uso de firewalls

B) Control de accesos

C) Cifrado de datos

D) Hashing (Correcta)

15. ¿Cuál es el objetivo principal de la gestión de seguridad en una organización?

A) Desarrollar software

B) Proteger los activos informáticos (Correcta)

C) Aumentar el número de usuarios

D) Compartir información con terceros

III. Casos Prácticos

Caso 1: Implementación de un Modelo de Seguridad

Una empresa de desarrollo de software necesita proteger sus datos confidenciales. Deben seleccionar un modelo de seguridad adecuado y justificar su elección.

- Tareas:
  - Identificar amenazas principales.
  - Seleccionar un modelo (BLP o TG).

- Justificar su elección y describir la implementación.

Caso 2: Análisis de un Ataque Informático

Una universidad detectó un ataque de malware que afectó la disponibilidad de sus servicios de TI.

- Tareas:
  - Identificar el tipo de malware.
  - Explicar el principio afectado (CID).
  - Proponer soluciones para prevenir futuros ataques.

Caso 3: Diseño de una Política de Seguridad

- Una empresa quiere crear una política de seguridad para proteger su red interna.
- Tareas:
  - Establecer los objetivos de la política.
  - Incluir normas de acceso y control de datos.
  - Proponer medidas de seguridad técnicas y administrativas.

Información Adicional

- Revisar Conceptos Clave: Asegúrate de comprender los términos técnicos.
- Practicar Preguntas: Resuelve preguntas de opción múltiple.
- Estudiar Casos Prácticos: Desarrolla respuestas detalladas y justificadas.
- Usar Recursos Digitales: Consulta materiales en línea y manuales de seguridad.

Bibliografía Básica

- Arturo Cuellar Feradez, 2015, Seguridad Integral dela Empresa, México, Trillas
- Alvaro Gómez Vieites, 2014. Enciclopedia de la Seguridad Informática, Espala RA MA
- Becerra., L. C.(2019). Diseño de un modelo de seguridad informática a una empresa en sus sitemas de monitoreo del área de tencnología. Colobia: Tesis

Normativas y Estándares

- Norma ISO/IEC 27001 - Sistema de gestión de la seguridad de la información.
- COBIT 2019 - Marco para la gestión de TI.
- ITIL 4 - Gestión de servicios de TI.

Recursos Digitales

- Sitio Web de la ISO - https://www.iso.org
- NIST Cybersecurity Framework - https://www.nist.gov
- Artículos y Publicaciones Académicas - Google Scholar, IEEE Xplore.