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 2026-2

TURNO VESPERTINO

Integrantes de la academia: José Arturo González Zárate. **Fecha de Elaboración:** 27/04/2026

FORMATO DE LA GUÍA DE ESTUDIO

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

Instrucciones generales de la guía:

La guía tiene no tiene valor.

Para revisión del examen:

- El alumno deberá solicitar el formato de revisión de examen en el área Tecnológica.
- Lo anterior deberá realizarse en plazo no mayor a 48 horas a partir de que se le notifico la calificación correspondiente.

Presentación:

Esta guía de estudio tiene como propósito fundamental facilitar al estudiante la comprensión y el dominio de los conceptos, tipos, mecanismos de propagación, técnicas de análisis y mitigación relacionados con el Software Malicioso (Malware).

Al utilizar esta guía, el alumno será capaz de:

- Identificar las diferentes categorías de malware (virus, gusanos, troyanos, ransomware, etc.).
- Analizar el ciclo de vida y la operatoria de las amenazas informáticas.
- Aplicar los conocimientos teóricos para evaluar y proponer estrategias de seguridad y defensa contra el software malicioso.

Objetivos

- Identificar y diferenciar con precisión las familias de software malicioso (Malware), comprendiendo sus vectores de infección y métodos de persistencia en los sistemas.
- Adquirir la capacidad de analizar muestras de malware (estático y dinámico) para determinar su comportamiento, funcionalidad y los indicadores de compromiso (IoC).
- Aplicar los conocimientos para evaluar, proponer e implementar medidas efectivas de prevención, detección y mitigación contra las amenazas de software malicioso.

Justificación

Esta guía de estudio es una herramienta esencial para que el estudiante adquiera el conocimiento teórico-práctico necesario para comprender, analizar y contrarrestar estas amenazas sofisticadas. Su dominio es crítico y obligatorio para cualquier profesional del área de Tecnologías de la Información y Seguridad, garantizando la protección de activos digitales en cualquier organización.

Estructura y contenidos

1. **UNIDAD I:**
   INTRODUCCION A LA NATURALEZA DEL MALWARE

   1.1. Identifica el tipo y las características de un código malicioso que pueda ser una amenaza, así como los servicios de análisis estático y de comportamiento de un antivirus.

   1.2. Distingue los riesgos frecuentes a los que se enfrenta el usuario en el ciberespacio y evita poner en riesgo la seguridad de un equipo, a través de los servicios de análisis, detección y aplicación de un antivirus específico.

2. **UNIDAD II:**
   TENDENCIAS Y CONTRAMEDIDAS DEL MALWARE

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

   2.2. Analiza el entorno cibernético óptimo para llevar a cabo una navegación segura en cualquier dispositivo conectado a una red.

   2.3. Aplica el uso adecuado de herramientas antimalware para la seguridad de la información.

3. **UNIDAD III:**
   ESTRATEGIAS DE SEGURIDAD PARA MITIGAR EL MALWARE EN LAS ORGANIZACIONES

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

   3.2. Aplica métodos de prevención y control con base en el impacto de los diferentes tipos de malware, fomentando un comportamiento ético-social en una organización.

   3.3. Implementa medidas que protejan a las personas, a los procesos y a la tecnología para mantener la información segura en la navegación, preservando una conducta ética y responsable dentro de una organización.

Evaluación

Esta guía es solo de preparación para el examen a título de suficiencia por lo cual no tiene valor alguno.

Materiales para la elaboración de la guía

Para llevar a cabo la realización de los ejercicios de esta guía es necesario contar con los siguientes elementos:

- Computadora con Sistema Operativo Windows 10 o superior.
- Software de Maquina Virtual.
- Sistema Operativo Kali Linux o Kali Purple (montado en la máquina virtual).
- Acceso a Internet.

1. ELEMENTOS TEORICOS

1.1. INTRODUCCION

La seguridad de la información es un proceso integral que abarca todos los elementos técnicos, humanos y organizativos de nuestra compañía. No es simplemente una cuestión tecnológica, sino un pilar fundamental de nuestra estrategia corporativa y reputación.

Esta guía establece las políticas, normativas y procedimientos de cumplimiento obligatorio para todos los empleados, diseñados para proteger los activos de información críticos de la organización y garantizar la continuidad de nuestras operaciones.

El objetivo principal de esta guía es asegurar la confianza, integridad, disponibilidad y confidencialidad de los datos y sistemas que manejamos. Cada política aquí descrita contribuye a un entorno de trabajo seguro y resiliente, minimizando los riesgos hasta niveles aceptables.

El primer paso para defender nuestra organización es que cada empleado comprenda las amenazas a las que nos enfrentamos.

1.2. AMENAZAS CIBERNETICAS

El término malware, abreviatura de ***malicious software*** (software malicioso), se refiere a cualquier programa o código informático diseñado para dañar, obtener beneficios o hacer mal uso de un sistema sin el conocimiento o consentimiento del usuario. Comprender los diferentes tipos de malware y sus objetivos es el primer paso para construir una defensa proactiva y reconocer posibles ataques.

Los creadores de malware persiguen principalmente tres objetivos:

- **Robo de información:** Extraer datos confidenciales, credenciales de acceso, información financiera o secretos comerciales.
- **Secuestro de equipos y datos:** Bloquear el acceso a los sistemas o cifrar archivos para exigir un rescate a cambio de su liberación.
- **Reclutamiento para redes de bots (botnets):** Tomar el control de los equipos para utilizarlos en ataques coordinados a gran escala, enviar spam o realizar otras actividades ilícitas.

1.3. TECNICAS COMUNES DE ATAQUE

Los ciberdelincuentes emplean una variedad de técnicas para explotar la vulnerabilidad más común en cualquier sistema de seguridad: el factor humano. Se estima que el 95% de las incidencias de ciberseguridad se deben a errores humanos. A través de la ingeniería social y ataques directos a las conexiones, los atacantes buscan engañar a los empleados para que, sin saberlo, les abran las puertas de nuestra organización.

A continuación, se detallan las técnicas más frecuentes:

1.3.1. INGENIERÍA SOCIAL: Es un conjunto de técnicas de manipulación psicológica utilizadas para engañar a los usuarios y lograr que revelen información confidencial o realicen acciones que comprometan la seguridad. Sus variantes más comunes son:

- **Phishing, Vishing y Smishing:** El atacante suplanta la identidad de una entidad legítima (un banco, un proveedor, un servicio técnico) para solicitar información sensible. Utiliza el correo electrónico (Phishing), llamadas de voz (Vishing) o mensajes SMS (Smishing) para generar un sentido de urgencia o confianza y persuadir a la víctima.

- **Baiting (Cebo):** Esta técnica utiliza un "cebo" para atraer a la víctima. Puede ser un dispositivo físico, como una memoria USB infectada abandonada en un lugar público, o un cebo digital, como un anuncio de una descarga gratuita o un premio atractivo que oculta malware.

- **Spam:** Consiste en el envío masivo de correo electrónico no solicitado. Aunque a menudo tiene fines comerciales, es uno de los principales vehículos para distribuir malware, phishing y otros tipos de fraudes.

1.3.2. ATAQUES A LAS CONEXIONES: Estos ataques se centran en interceptar o manipular las comunicaciones entre el empleado y los servicios a los que accede.

- **Redes Wi-Fi Falsas (Redes Trampa):** Los atacantes crean puntos de acceso Wi-Fi con nombres similares a redes legítimas (por ejemplo, en aeropuertos o cafeterías). Cuando un usuario se conecta, el atacante puede monitorizar todo su tráfico de red, interceptando datos y credenciales.

- **Spoofing (Suplantación):** Consiste en falsear la identidad de un sistema para hacerse pasar por otro. Las variantes incluyen IP Spoofing (falsear la dirección IP), Web Spoofing (crear una copia de una página web legítima) y Email Spoofing (falsificar el remitente de un correo).

1.3.3. ATAQUES A CONTRASEÑAS: Técnicas orientadas a descubrir las credenciales de un usuario para acceder a sus cuentas.

- **Fuerza Bruta:** Consiste en probar sistemáticamente todas las combinaciones posibles de caracteres hasta dar con la contraseña correcta.

- **Ataque por Diccionario:** Utiliza un software que prueba automáticamente palabras y contraseñas comunes extraídas de listas (diccionarios) para intentar adivinar la clave.

El conocimiento de estas técnicas nos permite identificar los canales específicos a través de los cuales un empleado puede ser expuesto a un ataque en su día a día.

A continuación, se presenta un análisis de los tipos de malware más comunes:

Tipo de Malware	Análisis de su Funcionamiento y Objetivo
Virus	Programas que se adhieren a archivos ejecutables legítimos. Su objetivo es alterar el funcionamiento normal del equipo, dañar, modificar o eliminar archivos del sistema. Requieren la intervención del usuario para propagarse, como abrir un archivo infectado.
Gusanos (Worms)	A diferencia de los virus, los gusanos son autónomos y se replican a sí mismos para propagarse a través de las redes informáticas sin necesidad de acción humana. Su principal objetivo es expandirse al mayor número de equipos posible, consumiendo ancho de banda y pudiendo instalar malware adicional.
Troyanos	Software malicioso que se disfraza de una aplicación legítima para engañar al usuario e inducir su instalación. Una vez dentro, ejecuta acciones ocultas como robar información o abrir una "puerta trasera" (*backdoor*) para que el atacante acceda y controle el equipo de forma remota. Subtipos comunes incluyen *Keyloggers* (registran pulsaciones del teclado) y *Stealers* (roban información almacenada).
Spyware	Software espía diseñado para recopilar información sobre la actividad de un usuario, su historial de navegación o credenciales sin su conocimiento. Su objetivo es violar la privacidad para cometer fraude o robo de identidad.
Adware	Software que muestra o descarga publicidad no deseada de forma automática. Aunque a menudo se instala con consentimiento (oculto en los términos de software gratuito), puede recopilar datos personales para dirigir anuncios y afectar negativamente el rendimiento del equipo.
Ransomware	Es la forma de malware más hostil y directa. Su objetivo es cifrar los archivos del equipo o bloquear el acceso al sistema por completo para exigir el pago de un rescate a cambio de la clave de descifrado. Impacto: Paralización total de las operaciones si afecta a servidores compartidos, con posibles pérdidas financieras y de reputación irreparables.
Rootkits	Conjunto de herramientas diseñadas para obtener acceso no autorizado a un sistema y permanecer ocultas. Modifican el sistema operativo para esconder la presencia de otros malware, dificultando enormemente su detección y eliminación.
Botnets	No es un malware en sí, sino una red de dispositivos infectados ("bots" o "zombis") controlados de forma remota por un atacante. Estas redes se utilizan para lanzar ataques a gran escala, como ataques de denegación de servicio (DDoS), enviar spam masivo o robar datos.
Rogueware / Scareware	Software que simula ser un programa antivirus. Engaña al usuario mostrándole falsas alertas sobre infecciones para inducirlo a pagar por una solución inútil que, en realidad, puede ser el propio malware.

1.4. POLITICAS FUNDAMENTALES DE USO

Todos los equipos informáticos, sistemas y recursos de red son propiedad de la organización y se proporcionan como herramientas para el desempeño de las funciones laborales. Su uso debe ser siempre responsable, ético y estar alineado con los objetivos institucionales, de acuerdo con las siguientes normas:

- Los equipos informáticos y sistemas de la organización únicamente podrán emplearse para fines institucionales. Esto previene la introducción de software no verificado y asegura que los recursos de red estén disponibles para las operaciones críticas del negocio.
- Solo el personal de soporte técnico autorizado podrá distribuir, instalar o desinstalar software y hardware, o modificar la configuración de los equipos.
- Está estrictamente prohibido alterar cualquiera de los componentes físicos (hardware) o lógicos (software) de los equipos asignados.
- Los empleados no dispondrán de privilegios de administración sobre sus equipos, salvo autorización expresa y justificada, para evitar instalaciones no autorizadas que puedan comprometer la seguridad.
- Se debe facilitar en todo momento el acceso a los equipos al personal de soporte técnico para labores de mantenimiento.
- Es obligación de cada empleado comunicar inmediatamente al personal de soporte cualquier comportamiento anómalo detectado en los equipos.
- Cada usuario es responsable del cuidado y mantenimiento básico del equipo que le ha sido asignado.
- Se debe hacer un uso responsable de dispositivos extraíbles como memorias USB, DVDs o CDs.
- No está autorizado el uso de memorias USB personales, salvo autorización expresa. Esta medida es crucial para prevenir infecciones por malware a través de técnicas de *Baiting*.
- El uso de equipos grabadores de USB, DVDs o CDs no está autorizado, a menos que sea esencial para las funciones del puesto y esté previamente aprobado.
- No se podrán eliminar ni deshabilitar las aplicaciones informáticas instaladas por la organización, especialmente las herramientas de seguridad como el antivirus.
- Antes de abandonar las salas de reuniones o despachos, se deben limpiar adecuadamente las pizarras para no dejar expuesta información sensible.
- Se debe apagar el ordenador al finalizar la jornada laboral para asegurar la correcta aplicación de actualizaciones y políticas de seguridad.

1.5. VIAS DE INFECCION Y PUNTOS DE RIESGO PARA EL EMPLEADO

La mayoría de las infecciones de malware no ocurren por ataques técnicos sofisticados, sino cuando un usuario, sin saberlo, realiza una acción que permite la descarga e instalación del software malicioso. Comprender estas vías de entrada es crucial para que cada empleado pueda identificar y evitar los comportamientos de riesgo que ponen en peligro tanto su seguridad personal como la de toda la organización.

Las principales vías de infección y puntos de riesgo son:

1.5.1. **CORREOS ELECTRÓNICOS Y MENSAJERÍA:** Es la vía de infección más común. El riesgo reside en abrir archivos adjuntos o hacer clic en enlaces de correos electrónicos, SMS o mensajes de redes sociales no solicitados o de remitentes desconocidos, lo que puede iniciar la descarga de malware.

1.5.2. **DESCARGA DE SOFTWARE Y ARCHIVOS:** Instalar programas "gratuitos" (*freeware* o *shareware*) sin leer detenidamente las opciones de instalación puede incluir adware o spyware. Del mismo modo, el uso de redes de intercambio de archivos (P2P) o la descarga de actualizaciones de software desde fuentes no oficiales son prácticas de alto riesgo.

1.5.3. **NAVEGACIÓN WEB:** El simple hecho de visitar un sitio web fraudulento o un sitio legítimo que ha sido previamente infectado puede ser suficiente para que el malware se instale en el equipo sin ninguna acción adicional por parte del usuario (lo que se conoce como *drive-by-download*, donde el malware se instala automáticamente con solo visitar la página, sin necesidad de hacer clic en nada).

1.5.4. **REDES SOCIALES:** Hacer clic en enlaces acortados o publicaciones compartidas por contactos (cuyas cuentas pueden haber sido comprometidas) puede redirigir a sitios maliciosos diseñados para robar credenciales o distribuir malware.

1.5.5. **DISPOSITIVOS EXTRAÍBLES:** Insertar en el equipo una memoria USB, un CD, un DVD o un disco duro externo infectado es una forma clásica de propagación de malware.

1.5.6. **REDES INSEGURAS:** Conectarse a redes Wi-Fi públicas o poco seguras (como las de cafeterías, aeropuertos u hoteles) expone el dispositivo a posibles interceptaciones de datos y ataques.

Debido a la existencia de estos riesgos, la organización ha definido un conjunto de políticas de uso aceptable que son de cumplimiento obligatorio para todo el personal.

1.6. MEDIDAS DE PROTECCION BUENAS PRACTICAS Y

Más allá de las políticas corporativas, la seguridad depende de las decisiones y hábitos diarios de cada empleado. Dado que el 95% de los incidentes de seguridad se deben a errores humanos, esta sección proporciona las herramientas para que cada uno de nosotros pueda construir una defensa personal robusta, convirtiéndose en un eslabón fuerte en la cadena de seguridad de la organización.

1.6.1. GESTIÓN DE CONTRASEÑAS

Las contraseñas son la primera línea de defensa para proteger nuestras cuentas. Para ello, es mandatorio seguir estas Reglas de Oro para Contraseñas Seguras:

- **Complejidad y Longitud:** Las contraseñas deben tener una longitud mínima de 8 caracteres y combinar mayúsculas, minúsculas, números y símbolos.
- **Unicidad: Nunca** utilice la misma contraseña para diferentes servicios. Si una cuenta es comprometida, un atacante intentará usar esa misma contraseña en todas las demás.
- **Doble Factor de Autenticación (2FA):** Habilite siempre la verificación en dos pasos cuando el servicio lo ofrezca. Esta capa extra de seguridad protege su cuenta incluso si su contraseña es robada.
- **Gestores de Contraseñas:** Considere el uso de un gestor de contraseñas aprobado por la compañía para almacenar sus credenciales de forma segura y cifrada.
- **Confidencialidad:** Su contraseña es personal e intransferible. Nunca la comparta con nadie, ni siquiera con compañeros de trabajo o personal de soporte técnico.

1.6.2. PROTECCION ACTIVA Y MANTENIMIENTO DEL SISTEMA

El software de seguridad y las actualizaciones son nuestros aliados fundamentales contra el malware. Es responsabilidad de cada empleado asegurarse de que estas protecciones estén siempre operativas.

- **Antivirus y Antimalware:** Debe mantenerse siempre en funcionamiento y con las bases de datos actualizadas. Notifique inmediatamente a TI si detecta alguna advertencia de mal funcionamiento.
- **Cortafuegos (Firewall):** El cortafuegos del sistema operativo debe estar siempre activo. Actúa como una barrera que controla el tráfico de red y bloquea accesos no autorizados.
- **Actualizaciones del Sistema Operativo:** Instale todos los parches y actualizaciones de seguridad que el sistema operativo notifique.
- **Actualizaciones de Aplicaciones:** Mantenga actualizados todos los programas instalados, especialmente los navegadores web y librerías como Java y Adobe.

1.6.3. COPIAS DE SEGURIDAD

Las copias de seguridad son nuestra red de seguridad más importante. Su propósito es garantizar la continuidad del negocio y la recuperación de la información ante un incidente grave, como un fallo de hardware o un ataque de ransomware.

Es fundamental realizar copias de seguridad periódicas de toda la información importante. De acuerdo con los procedimientos de la empresa, estas copias deben realizarse en soportes externos o en la nube, según lo dicte el procedimiento de la empresa. Además, deben ser probadas periódicamente para garantizar que la restauración de los datos se puede llevar a cabo con éxito en caso de emergencia.

A pesar de todas las precauciones, es posible que en algún momento sospechemos de un incidente de seguridad. Saber cómo actuar en ese momento es crucial.

SÍNTOMA O SEÑAL DE ALERTA	POSIBLE CAUSA
Funcionamiento Lento	El equipo o Internet funcionan mucho más lento de lo normal, posiblemente porque un malware está consumiendo recursos o generando un alto tráfico de datos.
Ventanas Emergentes y Programas No Deseados	Aparecen constantemente ventanas emergentes (*pop-ups*) o se instalan nuevos programas que usted no ha autorizado.
Comportamiento Anómalo del Equipo	El ordenador se apaga o se reinicia solo, el sistema se bloquea con frecuencia o no le permite apagarlo.
Redirecciones del Navegador	El navegador le redirige automáticamente a sitios no solicitados o la página de inicio ha cambiado sin su permiso.
Desactivación de la Seguridad	El software antivirus o el cortafuegos se desactivan solos y no puede volver a activarlos, ya que algunos malware están diseñados para deshabilitar las defensas.
Reducción Súbita del Almacenamiento	Nota una disminución inexplicable del espacio libre en el disco duro, lo que podría indicar que un malware está replicando archivos.

2. CUESTIONARIO DE REPASO

2.1. ¿Cuál es la definición de malware y cuáles son sus objetivos principales?

El malware, abreviatura de "malicious software" (software malicioso), es un programa informático que se ejecuta sin el conocimiento ni la autorización del usuario para realizar funciones perjudiciales. Sus principales objetivos son el robo de información, el secuestro del equipo o los datos del sistema (ransomware) y el "reclutamiento" de dispositivos para crear redes de bots.

2.2. Describa el ransomware. ¿Qué lo distingue de otros tipos de malware?

El ransomware es un tipo de malware que bloquea o deniega el acceso a un dispositivo y sus archivos, a menudo mediante cifrado, y exige el pago de un rescate para restaurar el acceso. Se considera la forma más hostil y directa de malware porque, a diferencia de otros que operan de forma invisible, el ransomware anuncia su presencia de inmediato y demanda un pago.

2.3. ¿Qué es un troyano y cómo se diferencia de un virus en términos de propagación?

Un troyano es un programa malicioso que se disfraza de software legítimo para engañar al usuario y lograr que lo instale. A diferencia de los virus, que tienen la capacidad de replicarse y autopropagarse al infectar otros archivos, los troyanos no pueden expandirse por sí solos y requieren un proceso de instalación por parte del usuario.

2.4. Explique el funcionamiento del spyware y los riesgos que representa para un usuario.

El spyware es un software malicioso que recopila información sobre la actividad de un usuario en un dispositivo o red y la envía a un atacante. Puede registrar pulsaciones de teclas, capturas de pantalla e historial de navegación para robar datos personales como credenciales de inicio de sesión, números de tarjeta de crédito o información financiera, con el propósito de cometer fraude o robo de identidad.

2.5. ¿Qué es una red de robots (botnet) y para qué fines maliciosos puede ser utilizada por un atacante?

Una botnet no es un tipo de malware en sí, sino una red de equipos infectados con software malicioso conocido como "robots" o "bots". Esta red es controlada remotamente por un atacante y puede ser utilizada para coordinar ataques de denegación de servicio (DDoS), enviar spam, robar datos, crear anuncios falsos y propagar otros tipos de malware.

2.6. ¿Cuáles son dos de las consecuencias más comunes que un usuario puede experimentar cuando su dispositivo está infectado con malware?

Un usuario con un dispositivo infectado puede notar que el equipo o la velocidad de Internet funcionan más lento de lo normal debido a un aumento en la carga del procesador o un elevado tráfico de datos. Otra consecuencia común es la aparición de ventanas emergentes, anuncios y programas no deseados en el dispositivo sin que el usuario los haya instalado conscientemente.

2.7. Mencione tres medidas preventivas basadas en software que son cruciales para proteger un sistema informático.

Tres medidas preventivas fundamentales son: mantener un programa antivirus eficaz y permanentemente actualizado para proteger contra amenazas; tener un firewall activo para proteger el ordenador de accesos no autorizados; y mantener actualizados tanto el sistema operativo como los programas instalados para eliminar vacíos de seguridad.

2.8. ¿Qué es una vulnerabilidad y qué significa el término "vulnerabilidad de día cero" (0-day)?

Una vulnerabilidad es una debilidad o fallo en un sistema de información que permite a un atacante violar la confidencialidad, integridad o disponibilidad de la información. Una "vulnerabilidad de día cero" (0-day) se refiere a una vulnerabilidad para la cual no existe una solución o parche conocido por parte del fabricante, pero sí se conoce una forma de explotarla, haciéndola especialmente peligrosa.

2.9. Defina el phishing y describa su método de funcionamiento más común.

El phishing es un tipo de ataque de ingeniería social en el que un ciberdelincuente suplanta la identidad de una entidad legítima (como un banco o una red social) para engañar al usuario. Comúnmente, envía un mensaje de carácter urgente o atractivo por correo electrónico, SMS (smishing) o llamada (vishing) para inducir a la víctima a revelar información personal o bancaria, o a descargar malware a través de un enlace o archivo adjunto.

2.10. ¿Qué son los PUP (Programas Potencialmente no Deseados) y por qué no se clasifican técnicamente como malware?

Los PUP son programas que, aunque pueden realizar acciones no deseadas como mostrar publicidad o modificar la configuración del navegador, no se clasifican como malware porque el usuario otorga su consentimiento para descargarlos, aunque sea de forma involuntaria. Este consentimiento a menudo se obtiene a través de cláusulas ocultas o confusas en el proceso de instalación de otro software, lo que dificulta que un antivirus los catalogue como maliciosos por riesgo a una demanda legal.

3. GLOSARIO

TÉRMINO	DEFINICIÓN
Adware	Software malicioso que somete a la víctima a publicidad no deseada, a menudo instalándose junto a programas gratuitos. Recopila datos personales del usuario para personalizar los anuncios que muestra y puede dirigirlo a páginas maliciosas.
Baiting (Cebo)	Técnica de ingeniería social que utiliza un medio físico (como una memoria USB infectada) o un señuelo atractivo (como un concurso) para incitar a la víctima a infectar su equipo o compartir información personal.
BHO (Browser Helper Objects)	Pequeños programas asociados al navegador Internet Explorer que extienden sus funcionalidades. Aunque no siempre son maliciosos, a menudo son utilizados por spyware y secuestradores de navegador para redirigir al usuario a sitios no solicitados.
Botnet (Red de Robots)	Una red de equipos infectados con software malicioso llamado "bots", controlados de forma remota por un atacante. Se utiliza para coordinar ataques, enviar spam, robar datos o realizar otras actividades ilícitas.
Criptojacking	Práctica maliciosa que utiliza los recursos de un dispositivo sin el consentimiento del usuario para "minar" o extraer criptomonedas, lo que provoca una reducción del rendimiento del equipo y un aumento en el consumo de energía.
Esquema Nacional de Seguridad (ENS)	Política de seguridad en el uso de medios electrónicos en las Administraciones Públicas de España, regulada por el Real Decreto 311/2022. Su finalidad es asegurar la confianza y proteger la información, aplicando principios como la gestión de riesgos y la existencia de líneas de defensa.
Firewall (Cortafuegos)	Programa o dispositivo diseñado para filtrar el tráfico de red y proteger un ordenador o una red de accesos no autorizados. Actúa como primera línea de defensa ante ataques desde Internet.
Fleeceware	Práctica deshonesta de desarrolladores de aplicaciones que busca cobrar al usuario una cantidad económica abusiva por una aplicación, a menudo mediante suscripciones con pruebas gratuitas engañosas que continúan realizando cargos incluso después de desinstalar la app.
Gusano (Worm)	Programa malicioso diseñado para replicarse y expandirse automáticamente a través de una red informática, sin necesidad de la intervención del usuario o de adherirse a un archivo existente. Puede colapsar redes al consumir ancho de banda y servir como vehículo para instalar otro malware.
Keylogger	Tipo de troyano o spyware que registra en secreto cada pulsación de tecla que un usuario realiza en su dispositivo. Su objetivo es robar información sensible como nombres de usuario, contraseñas y datos de tarjetas de crédito.

Malware	Abreviatura de "malicious software". Es cualquier programa informático diseñado para ejecutarse sin autorización del usuario, con el fin de dañar un sistema, robar información, eludir controles de acceso o causar cualquier otro perjuicio.
Phishing	Ataque de ingeniería social donde un atacante suplanta la identidad de una entidad legítima para engañar a la víctima y hacer que revele información confidencial (como contraseñas o datos bancarios) a través de correos, mensajes o sitios web fraudulentos.
PUP (Programa Potencialmente no Deseado)	Software que, aunque el usuario consiente su instalación (a menudo sin saberlo), realiza acciones no deseadas como mostrar publicidad o modificar la configuración del navegador. No se clasifica como malware porque técnicamente existe un consentimiento.
Ransomware	Malware que bloquea o cifra los archivos de un dispositivo y exige el pago de un rescate para devolver el acceso al usuario. Es considerado el tipo de malware más hostil y directo.
Rootkit	Conjunto de programas maliciosos diseñados para obtener acceso no autorizado a un sistema y permanecer oculto, modificando el sistema operativo para que ni el usuario ni el software de seguridad puedan detectar su presencia.
Scareware (o Rogueware)	Software malicioso que utiliza alertas de seguridad falsas para engañar al usuario, haciéndole creer que su ordenador está infectado. Su objetivo es inducir al usuario a pagar por un software fraudulento o a instalar más malware.
Spam	Envío masivo de mensajes no solicitados, generalmente de carácter publicitario, a través de medios electrónicos como el correo. A menudo se utiliza como vehículo para ataques de phishing o para distribuir malware.
Spoofing	Técnica que consiste en suplantar la identidad de un usuario, una página web, una dirección de correo electrónico o una dirección IP para engañar a la víctima y obtener acceso a sus datos o sistemas.
Spyware (Software espía)	Malware que recopila información sobre un usuario o una organización sin su conocimiento, supervisando su actividad en Internet para robar credenciales, datos financieros u otra información personal.
Troyano	Malware que se disfraza de software legítimo para engañar a la víctima y lograr su instalación. Una vez activado, puede robar datos, controlar el equipo de forma remota o descargar malware adicional, pero no puede replicarse por sí mismo.
Virus	Tipo de malware que infecta otros archivos o programas del sistema con la intención de modificarlos o dañarlos. Necesita la intervención del usuario para ejecutarse y tiene la capacidad de copiarse a sí mismo y propagarse a otros dispositivos.
Vulnerabilidad	Debilidad o fallo en el diseño, implementación o configuración de un sistema de información que puede ser explotado por un atacante para comprometer su seguridad. Si no existe una solución conocida, se denomina "vulnerabilidad de día cero".

Información Adicional

- Ninguna

Bibliografía Básica

- Sikorski, M., & Honig, A. (2012). *Practical malware analysis: The hands-on guide to dissecting malicious software*. No Starch Press.
- Stallings, W., & Brown, L. (2023). *Computer security: Principles and practice* (5.a ed.). Pearson.
- Bancal, D., & Ebel, F. (2022). *Seguridad informática y malwares: Ataques, amenazas y contramedidas* (3.a ed.). Ediciones ENI.