1. ¿Qué es un antivirus?
   Consiste en un programa que detecta y elimina programas de software malicioso

2. Explica en qué consisten los siguientes tipos de antivirus:
   Vacuna: actúan como filtro en los programas ejecutados.
   Detector: detectan cualquier alteración en los archivos, aunque no sea por un virus.
   Eliminador: detectan y eliminan cualquier archivo contaminado, dejando el programa en estado original.

3. ¿Qué es Reeper y Creeper?
   Creeper fue el primer virus creado con la intención de saber si existía la posibilidad de que un programa se moviera entre ordenadores, mientras que el **Reaper** fue el primer antivirus creado para buscar y eliminar el virus Creeper.

4. ¿Qué es virus boot?
   Este tipo de virus no infecta ficheros, sino los discos que los contienen. Actúan infectando en primer lugar el sector de arranque de los dispositivos de almacenamiento.
   Cuando un ordenador se pone en marcha con un dispositivo de almacenamiento, el virus de boot infectará el disco duro.

5. ¿Qué es un virus hijackers?
   Son programas que secuestran navegadores de internet (en especial el explorer). Alteran las páginas iniciales del navegador e impide que el usuario pueda cambiarla, muestra publicidad en "pops ups", instala nuevas herramientas en la barra del navegador y, a veces impiden al usuario acceder a ciertas páginas web.

6. ¿Qué es el virus keylogger?
   Este virus se encarga de registrar cada tecla que sea pulsada. Son virus que quedan escondidos en el sistema operativo. Se utilizan para robar contraseñas.

7. ¿Qué es el virus zombie?
   Son programas que secuestran ordenadores de forma que es controlada por terceros. Se utiliza para diseminar virus, keyloggers y procedimientos invasivos en general.

8. ¿Cuál es la característica principal del antivirus AVAST?
   La característica que más destaca es el hecho de ser gratuito.

9. ¿Por qué se denominan virus a los virus informáticos?
   Tienen la misma función que un virus (enfermedad), ya que los dos contagian a sistemas y alteran partes de estes.

10. Investiga que es Elk Cloner y quien es Rich Skrenta.
    Elk Cloner fue un virus informatico creado por Rich Skrenta, que se propagaba mediante disquetes del sistema informativo Apple II. Se diseñó con el objectivo de ser molesto, mostrándose en el arranque nº50 un poema.

11. ¿Por qué crees que se hacen los virus?
Para obtener información importante para el creador.

12. ¿cuál es la necesidad de actualizar un antivirus?
Para que los nuevos virus no puedan infiltrarse dentro del sistema.

13. ¿Qué diferencias existen entre la protección de un antivirus gratuito y uno pago?
Los antivirus gratuitos contienen una seguridad básica, mientras que uno de pago está más completo, y puedes comprar el que se te adapte mejor a tus necesidades.

14. ¿Qué es un antivirus online? Pon algún ejemplo
Este antivirus nos permite escanear el sistema en búsqueda de algún programa malicioso, para luego desinfectarlo.
Ej.: BirDefender

15. Indica en que consiste cada uno de los siguientes tipos de virus.
Adware: muestra publicidad no deseada o engañosa en ventanas flotantes, carteles…
Spyware: consiste en recolectar información de las actividades realizadas en el ordenador.
Malware: realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario.
Ransomware: restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción.
Gusanos: códigos que reenvían a sí mismos para propagarse por las redes del ordenador, para saturar programas y bloquearlos.
Troyano: modifica el sistema dejándolo desprotegido para que entren otros programas.
Denegación de servicio: causa que un servicio o recurso sea inaccesible a los usuarios.
Puerta trasera: secuencia especial trasero dentro del código de programación, mediante la cual se pueden evitar los sistemas de seguridad del algoritmo para acceder al sistema.
Phishing: consiste en engañar al usuario, haciéndose pasar por una persona o empresa, ganándose su confianza para que de su información.
Darknets o deep web, comercio de vulnerabilidades: sirve para compartir información y contenidos digitales de manera anónima.
Bombas lógicas o de tiempo: programa que se activa cuando se da un cierto acontecimiento, como una fecha concreta o una combinación de teclas. Mientras no se ejecute, permanece oculto.
Hoax: consisten en mensajes de contenido falso que incitan al usuario a hacer copias y enviarla a sus contactos

16. Compara los siguientes tipos de antivirus e indica las ventajas de cada uno de ellos.
Kaspersky: fácil de manipular, no hace perder rendimiento
Nod 32:
Mcafee: es el que usa menos recursos, instalación en varios dispositivos

17. Investiga en que consistían los siguientes virus.

Morris (1988): malware que se autorreplicaba mediante internet. Este virus buscaba las contraseñas de los ordenadores. Al obtener la contraseña, el virus pasaba a otras máquinas.

CIH/Chernóbil (1998): atacaba a los sistemas de Windows x9. Fue considerado uno de los virus más peligrosos y destructivos, capaz de eliminar información importante y sobrescribir el sistema BIOS. Se propagaba a través de ficheros ejecutables, con la ayuda de los correos electrónicos.

Melissa (1999): virus que infectaba documentos de Microsoft Office. Se replicaba mediante los correos electrónicos, ya que al abrirlo este se ejecutaba y cambiaba el registro de Windows.

I love you (2000): este gusano borraba documentos de video, fotos, audio, etc. Algunos los reescribía y les daba otra extensión. Se multiplicaba en el disco duro con la extensión .vbs . Este virus se propagaba mediante los correos electrónicos.

Mydoom (2004): es un gusano que afectaba a Microsoft Windows. Se transmitía principalmente por correo electrónico con el asunto "Error". Al abrir el documento, este se ejecutaba y se reenviaba a demás usuarios.

Conficker (2008): gusano que afectaba a Microsoft Windows. El virus se propagaba mediante un desbordamiento del búfer del server de Windows. Una vez instalado, este inutilizaba varios servicios (como Windows Security). Se encargaba de varias cosas, como de recolectar información como descargar otros malware.

WannaCry (2017): ransomware que afecto a la gran mayoría de países en el mundo. Se aprovechó de la vulnerabilidad de EternalBlue, para atacar a sistemas Windows desactualizados. Los archivos quedaban cifrados y mostraban un mensaje en la pantalla exigiendo 300 $ en Bitcoins para poder descifrarlos.