

Otro punto por demás importante es la protección de los datos, como archivos cuentas, proyectos, contraseñas y hardware. Por ello es de suma relevancia contestar lo siguiente parafraseando e incluyendo el link de donde sustrajo la información.

1. Define el concepto de seguridad informática y de la web

R.-

SEGURIDAD INFORMATICA: La **seguridad informática** o **seguridad de tecnologías de la información** es el área de la [informática](#) que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante.

Web: es un vocablo inglés que significa “red”, “telaraña” o “malla”. El concepto se utiliza en el ámbito tecnológico para nombrar a una red informática y, en general, a [Internet](#) (en este caso, suele escribirse como **Web**, con la W mayúscula).

2. Tipos de protección que hay actualmente (utiliza puntos).

R.-

- No dejar la dirección de correo electrónico en cualquier formulario o foro de internet en el que no nos interese participar.
- No responder a los correos no solicitados.
- No enviar respuesta a la dirección que figura, para evitar envíos posteriores.
- Configurar filtros o reglas de mensaje en el programa de correo para filtrar mensajes de determinadas direcciones.
- No configurar respuesta automática para los pedidos de acuse de recibo.
- No responder a los pedidos de acuse de recibo de orígenes dudosos.

3. Menciona 5 antivirus incluyendo sus versiones con su descripción breve.

a) Kaspersky:

Excelentes características; Muy efectivo; a mi parecer el mejor de todos; Excelente soporte; Excelente análisis Eurístico; En muchos de los casos cuando un virus lo intenta modificar para no ser reconocido; este protege su código y restaura una copia del correcto automáticamente; En su versión Internet Security la protección mas completa y segura.

Eset (Nod32): Muy liviano y noble con los recursos del computador; Muy buena protección y análisis eurístico de los archivos. Rapida respuesta en caso de virus. En su versión internet security: Bloqueo efectivo de páginas web con virus o de archivos infectados.

Avast:

Muy liviano; En su versión de paga buen análisis de archivos y eurístico; Actualización de sus definiciones en su base de datos bastante rápida.

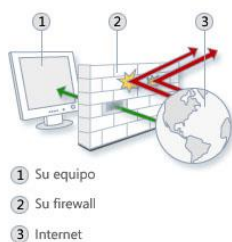
McAfee:

Bastante liviano; Muchas veces me he topado que algunos virus solo este **antivirus** los reconoce ya que su equipo trabaja muy rápido en el reconocimiento eurístico y de nuevos tipos de virus; Fácil de instalar y configurar.

Avira: Muy liviano y generoso con nuestros recursos del computador; Económico; Buena actualización de definiciones de virus.

4. *Qué herramientas adicionales al antivirus podemos usar para la protección de mi equipo (5 ej.) y su descripción e imagen.*

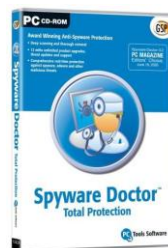
Firewall. Un firewall puede ayudarle a proteger el equipo al impedir que los hackers o el software malintencionado obtengan acceso a él.



Protección antivirus. Software antivirus que puede ayudarle a proteger un equipo frente a virus, gusanos y otras amenazas de seguridad.



Protección contra spyware y otros tipos de malware. El software anti spyware



puede ayudarle a proteger el equipo contra spyware.

Windows Update. Windows puede comprobar habitualmente las actualizaciones para el equipo e instalarlas de forma automática.



5. *Qué es una amenaza informática*

amenazas que surgen de la programación y el funcionamiento de un dispositivo de almacenamiento, transmisión o proceso deben ser consideradas, también hay otras circunstancias que deben ser tenidas en cuenta, incluso «no informáticas». Muchas son a menudo imprevisibles o inevitables, de modo que las únicas protecciones posibles son las redundancias y la descentralización, por ejemplo mediante determinadas estructuras de redes en el caso de las comunicaciones o servidores en [clúster](#) para la disponibilidad.

6. *Da 5 tipos de virus más comunes*

- **El phishing.** El primer puesto lo ocupan el [phishing](#), es decir, los intentos de robarnos las [contraseñas](#) tanto de acceso a los juegos online más conocidos como a nuestras cuentas de correo, banacarias.
- **Los troyanos.** Sin que lo sepamos, podemos tener [troyanos](#) instalados en nuestro ordenador que pudieran estar capturando toda la información que intercambiamos por la red. Dicha información se envía, de forma periódica, a su autor, que, al igual que en el caso anterior, sacará un beneficio económico
- **Los cracks o parches ilegales.** Con el fin de ahorrarse unos euros, que en época de crisis no viene mal, algunos usuarios descargan copias ilegales de juegos sin tener en cuenta que, la mayoría de las veces, el *crack* necesario para activar el juego está infectado y contiene *malware*.

- **Las conexiones gratuitas.** Mucho cuidado con las conexiones que utilizamos para conectarnos a la red.
- **Los mods.** Es decir, la extensión que modifica un juego original proporcionando nuevas posibilidades, ambientaciones, personajes, diálogos, objetos, etc. puede, además de contar con el beneplácito de los creadores del juego, también contienen *malware*.

7. *Cómo puedo quedar infectado por un virus*

Estas personas pueden atacar directamente, mediante la irrupción en su equipo a través de Internet y el robo información personal, o indirectamente mediante la creación de software malintencionado diseñado para dañar el equipo.

8. *Qué recomendaciones puedes tomar para evitar el robo de datos*

Cuidar de no ser observados al escribir nuestra clave.

- No observar a otros mientras lo hacen.
- No escribir la clave en papeles, ni en archivos sin cifrar.
- No compartir claves con otros.
- No pedir las claves de otros.
- No habilitar la opción de recordar claves en los programas que utilicen en equipos compartidos.
- No enviar claves por correo electrónico.
- No mantener una contraseña indefinidamente (se recomienda cambiarla con cierta regularidad).
- No abrir archivos adjuntos de origen desconocido.
- No abrir archivos adjuntos que no esperan recibir, aunque les parezca que su origen es conocido.

12. *Inserta una imagen al final que explique todo lo que es seguridad.*

