Milpa Digital

Manteniendo nuestro sistema operativo libre de virus

Seguro hemos oído hablar de los virus informáticos, esos bichos electrónicos que se propagan por todos nuestros dispositivos. Son programas maliciosos y su nombre es **malware** (Milpa 9). En esta Milpa revisaremos como cuidarnos de ellos.

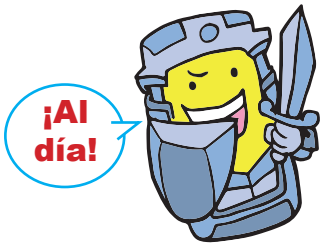
El malware funciona aprovechándose de alguna **debilidad de un sistema operativo**, y todos los sistemas operativos tienen alguna debilidad, ya sean de software libre o privativos, ya sea el que usamos en la computadora, en el teléfono, en la impresora, etc. Windows es el sistema operativo más usado en el mundo, por eso las personas que crean estos programas maliciosos los desarrollan principalmente para este sistema operativo para llegar al mayor número de dispositivos posibles. En el mundo Windows por tanto se han desarrollado varios programas para lidiar con los virus: los antivirus.

Algunos antivirus que recomendamos revisar

- **Avast:** Existen versiones de software libre y privativo. Disponible para Windows, MacOS, Android y iOS. **https://www.avast.com**
- **Avira:** Disponible para Windows, MacOs, Android y iOS (la versión para Linux ya no está soportada) **https://www.avira.com/es**
- **Clamav:** Antivirus de código abierto, disponible para Windows, Linux y MacOS **https://www.clamav.net/**

Consejos para usar antivirus

- No ejecutar dos herramientas contra el malware al mismo tiempo.
- Asegurarnos de que nuestro antivirus se puede actualizar por sí mismo y con frecuencia.
- Usar la opción de dejar el antivirus “siempre encendido” si es que la tiene.
- Hacer escaneos de todos nuestros archivos de cuando en cuando.
- Existen muy pocos antivirus de software libre, pero esto no significa que un antivirus sea mejor o peor que otro. En la industria se suele priorizar que el programa sea gratuito antes que abierto.

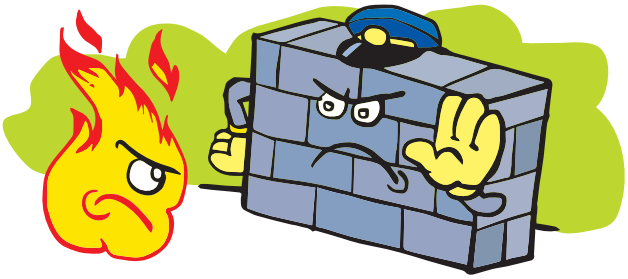


Consejos para proteger los teléfonos y tablets

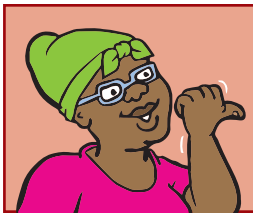
- Mantener actualizado el sistema operativo y las aplicaciones.
- Instalar programas solamente de fuentes oficiales o confiables como F-Droid.
- Desinstalar aplicaciones que no estamos usando.
- Negar permisos que nos pide una aplicación si nos parecen excesivos.
- Instalar una herramienta confiable contra el malware.

Firewall o cortafuegos

El cortafuegos es un programa en nuestra computadora que es el primero en examinar cada mensaje entrante y saliente en una red, y permitir, limitar, bloquear, cifrar o descifrar el tráfico de aquellos paquetes de información que no cumplen los criterios de seguridad especificados. Un cortafuegos correctamente configurado añade una protección necesaria a nuestra red, pero que en ningún caso es suficiente por sí mismo, mejor combinarlo con un antivirus.



Suscríbete a ResistenciaDigital en Telegram @CanalResistenciaDigital



Recomendamos
revisar esta tabla comparativa de antivirus en la wikipedia: https://w.wiki/6tj

Actualizaciones

No todo depende de los antivirus. Las debilidades (o vulnerabilidades) de las que se aprovechan los virus suelen ser arregladas (o parcheadas) y por eso se lanzan **nuevas versiones** de los sistemas operativos cada cierto tiempo. Si usamos un sistema operativo libre como **Ubuntu** (Milpa 16) o **Debian** (Milpa 17), podemos actualizarlo de las fuentes oficiales de forma gratuita cuando queramos. En cambio, si usamos un Windows pirateado no podemos acceder a las actualizaciones oficiales del sistema (podemos encontrar modos para actualizarlo usando software no oficial como kmspico, pero es bastante menos seguro) y esto nos hace cada vez más vulnerables a nuevos virus.

¡No olvides que puedes imprimir tu propia MilpaDigital y compartirla!

CódigoSur EDICIONES