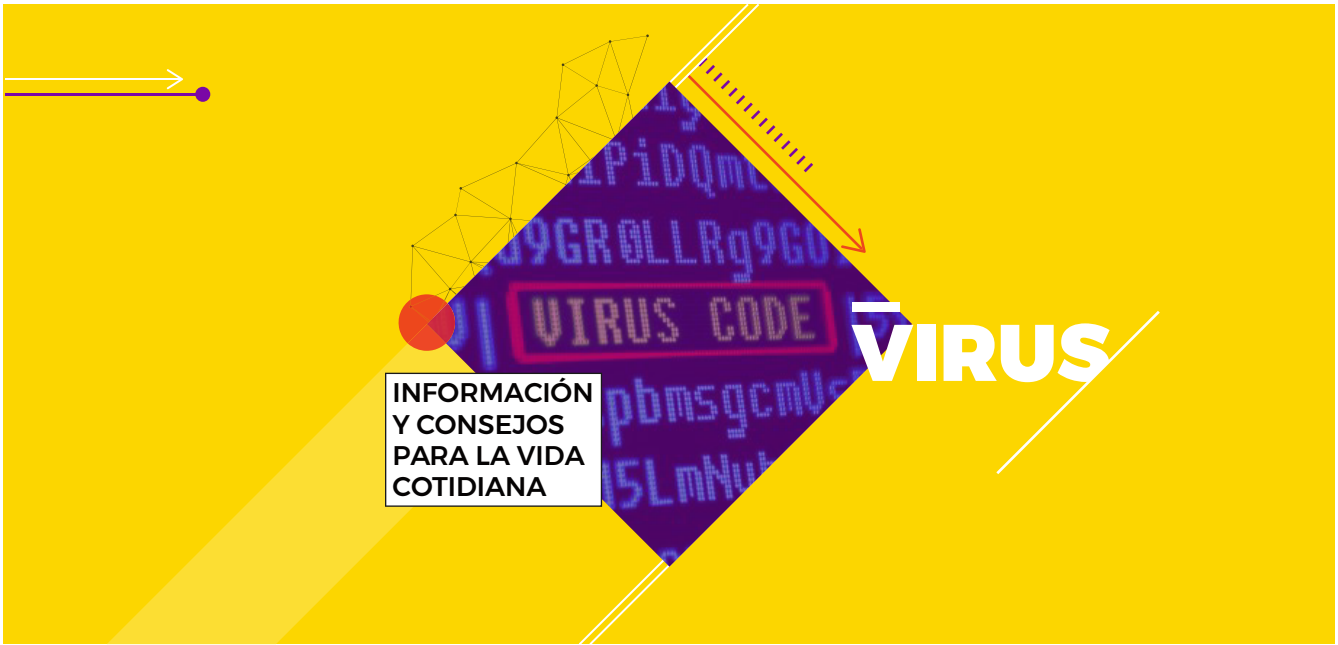
BACSIRT
Vamos Buenos Aires | Centro de Ciberseguridad
LA AGENCIA DE SISTEMAS

www.ba-csirt.gob.ar

BOLETÍN
N°07
FECHA DE PUBLICACIÓN
03 02 17



VIRUS INFORMÁTICOS: QUÉ SON Y COMO PREVENIRSE DE ELLOS

Muchas veces, a lo largo de nuestro tránsito por Internet, escuchamos, leemos, tememos e incluso somos víctimas de diferentes virus informáticos y, a pesar de ello, nos pasa que no tenemos del todo claro qué son ni cómo funcionan... y dado que ese mínimo conocimiento es esencial para poder prevenirnos y movernos con seguridad en el mundo de la informática, a continuación, describiremos las características básicas de los virus y algunos consejos para que puedas protegerte de ellos.

¿Qué son los virus informáticos?

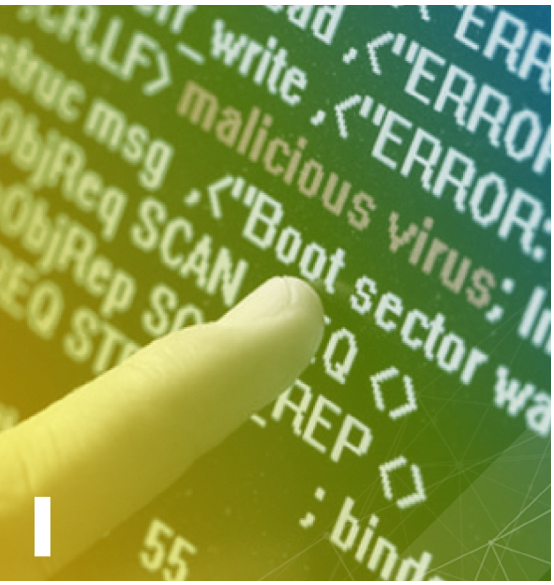
Un virus es un tipo específico de malware -del inglés *malicious software*, es decir, "programa malicioso"- **cuyo objetivo es alterar el funcionamiento normal de computadoras, celulares, Tablets y demás dispositivos electrónicos, de forma oculta**, es decir, sin que el usuario de los mismos tenga conocimiento de dicha alteración. Y, **paradójicamente, tienen la particularidad de que necesitan de la intervención del usuario para lograr su objetivo**.

Es importante tener en cuenta que todo dispositivo que se conecte a Internet es potencialmente vulnerable a sufrir una infección por malware.

En general, lo que los virus hacen es reemplazar los programas del dispositivo en cuestión por programas "impostores" que están infectados. Estos pueden, desde causar molestias inocuas hasta destruir, intencionalmente, los datos almacenados en un dispositivo, o, incluso, utilizar tu computadora (o cualquier otro equipo) para llevar a cabo otro tipo de ataque como, por ejemplo, el famoso ataque DDoS de octubre de 2016.

El funcionamiento de un virus informático es conceptualmente simple:

Tomando en consideración la alta exposición que tenemos a los virus informáticos, es imprescindible hacer uso de programas antivirus en todos los dispositivos que utilicemos conectados a Internet.



Los códigos maliciosos requieren de la intervención de los usuarios para lograr su objetivo de infectar a los dispositivos.

una vez que se ejecuta (inicia/pone en funcionamiento) un programa que está infectado -en general, por desconocimiento del usuario-, la información de programación del virus queda alojada en la memoria de la computadora y, de ese modo, éste toma el control de los servicios básicos de todo el sistema, infectando, a su vez, todos aquellos programas que se utilicen posteriormente.

Existen diversos tipos de virus, los cuales varían según su función o la manera en que se ponen en marcha en los dispositivos, algunos de los más comunes son:

- **Virus residentes:** la característica principal de estos virus es que se ocultan en la memoria RAM (memoria principal) de forma permanente o "residente". De este modo, pueden controlar e interceptar todas las operaciones llevadas a cabo por el sistema, infectando todas aquellas carpetas y/o programas que sean abiertos, cerrados, renombrados o copiados.
- **Virus de acción directa:** al contrario que los residentes, estos virus no permanecen en la memoria. Por tanto, su objetivo prioritario es reproducirse y actuar en el mismo momento de ser ejecutados; entonces, al cumplirse una determinada condición (que depende del virus del que se trate), se activan y buscan nuevas carpetas para contagiarlas.

¿Cómo podemos protegernos de los virus y demás tipos de malware?

Bien, además de utilizar un antivirus -programas que analizan permanentemente a los sistemas operativos para detectar, eliminar y/o controlar todo software sospechoso-, hay varias pautas muy sencillas y fáciles de aplicar que nos ayudarán a prevenir y evitar las infecciones por virus. Atención:

- No instalar programas de dudosa procedencia. Descargarlos solo de sitios conocidos y confiables y, al hacerlo, prestar atención a los requerimientos y permisos que van siendo solicitados a lo largo de todo el proceso de instalación. Si hay algo extraño o que presenta dudas, es preferible cancelarlo.
- No abrir correos electrónicos de desconocidos ni adjuntos inesperados. Tener especial precaución al respecto si utilizás programas para descargar correo como Outlook, por ejemplo; verificar que en la configuración no esté habilitada la apertura automática de los correos.
- Usar un bloqueador de elementos emergentes en el navegador.
- Usar la configuración de privacidad del navegador, fundamentalmente si vas a ingresar a sitios que manejan información sensible como home-banking y similares. ▪