VIRUS INFORMÁTICOS Y COMO EVITARLOS

La Dirección Nacional de Comunicaciones, a través del Departamento de Seguridad de la Información, ha elaborado un boletín de seguridad sobre los tipos de virus informáticos y como protegernos de estas amenazas.

La mayoría de las amenazas a las cuales están expuestos los computadores pueden ser clasificadas como virus, códigos maliciosos o ataques remotos.

Además de los programas instalados en su equipo, este puede ser atacado por programas maliciosos (malware) o, a través de una red, por parte de alguien que opera un equipo desde una ubicación remota.

Los programas maliciosos y los ataques remotos pueden causar pérdida de tiempo y dinero.

Virus informáticos

Un virus es un programa informático creado para producir algún daño en el equipo y que posee dos características particulares: Pretende actuar de forma transparente al usuario y tiene la capacidad de reproducirse a sí mismo. Los virus pueden ingresar en su equipo desde otras computadoras infectadas, a través de medios extraíbles (PenDrive (USB), DVD, etc.) o por medio de una red (local o internet).

¿Cómo se transmiten los virus?

La forma más común en que se transmiten los virus es por transferencia de archivos, descarga o ejecución de archivos adjuntos a correos.

¿Qué hacen los virus?

Cuando los virus se ejecutan producen daño irreparable al ordenador personal destrozando archivos, borrando los contenidos del disco duro, encriptando la información y hasta dejando inutilizable el equipo.

¿Cuáles son los principales tipos de virus para PC?

La primera clase incluye los que infectan archivos, adjuntos a programas ordinarios. Un virus de acción directa selecciona uno o varios programas para infectar cada vez que el programa es ejecutado. Un virus residente se esconde en alguna parte de la memoria la primera vez que un programa infectado se ejecuta, y después infecta a otros programas cuando son ejecutados.

La segunda categoría es la que infectan archivos de los sistemas operativos o sectores de arranque de los discos duros, pudiendo incluso dañarlos permanentemente.

Existen numerosos tipos de virus, los más comunes se describen a continuación:

- **Gusano:** Es un programa independiente que se replica a través de una red, el gusano se propaga activamente enviando copias de sí mismo a través de la red local o Internet, la comunicación por correo electrónico o aprovechando errores de seguridad del sistema operativo.

- **Troyano:** Es un código malicioso que, a diferencia de los gusanos, no puede reproducirse por sí mismo e infectar archivos. Usualmente se encuentra en forma de archivo ejecutable (.exe, .com) y no contiene ningún elemento más, a excepción del propio código del troyano. Posee varias funciones desde actuar como keyloggers, eliminar archivos y hasta formatear discos.

- **Adware:** Es una abreviatura (en inglés) de programas relacionados a la propagación de mensajes publicitarios. Trabajan mostrando ventanas emergentes durante la navegación en Internet, definiendo varios sitios web como página de inicio o abriendo una ventana especial de interfaz del programa. El adware frecuentemente es instalado por medio de programas de descarga gratuita.

- **Rogue:** Es un programa que, simulando ser una aplicación anti-malware (o de seguridad), ocasiona los efectos contrarios a esta: instala códigos maliciosos. Por lo general, se trata de ataques que muestran en la pantalla del usuario advertencias llamativas respecto a la existencia de infecciones en su equipo. La persona es invitada a descargar este tipo de "soluciones" con el objetivo de instalar códigos maliciosos en el equipo para obtener información confidencial o dinero a través del ataque.

- **Spyware:** Es un programa que se vale de Internet para recolectar piezas de información sensible del usuario sin su conocimiento. Algunos de estos programas buscan información tal como la referente a aplicaciones instaladas y al historial de sitios web visitados. Otros programas del tipo spyware son creados con un objetivo mucho más peligroso: la recolección de información financiera o personal para el robo de identidad.

- **Ransomware:** Es un software malicioso que al infectar nuestro equipo le da al ciberdelincuente la capacidad de bloquear el PC desde una ubicación remota y encriptar nuestros archivos quitándonos el control de toda la información y datos almacenados. Para desbloquearlo el virus lanza una ventana emergente en la que nos pide el pago de un rescate, el ejemplo más claro es el virus Cryptolocker.

¿Cómo sé si tengo un virus?

Es común que un virus no muestre señales de su presencia en absoluto. Los virus se comportan de diferentes formas y no existe un signo indicador absoluto que le avise de su presencia, sin embargo deberá mantenerse alerta ante acciones sospechosas de posibles virus como: aumento del tamaño de los archivos, la computadora funciona más lenta de lo normal, la computadora se reinicia por sí sola, la computadora se congela, se cuelga o no responde etc. Un antivirus actualizado es el único que puede indicarnos si tenemos una infección.

¿Cómo puedo evitar ser infectado por un virus?

Aunque existe una relativa concientización, generalmente no se toman todas las precauciones necesarias para anular el peligro. Si bien no es posible para ningún antivirus eliminar por completo el riesgo causado

por infiltraciones y ataques, es posible minimizar significativamente el riesgo de infección cumpliendo determinadas y simples estrategias.

- **Mantenga su base de datos de firma de virus actualizada:** Instalar un antivirus para la detección y eliminación de nuevos virus informáticos, además es necesario actualizarlo diariamente, la efectividad de un programa antivirus reside, en gran medida, en su capacidad de actualización.

- **Mantenga la protección en tiempo real del sistema de archivos activada:** Asegurarse que el antivirus esté siempre activo vigilando constantemente todas las operaciones realizadas en el sistema. Los archivos son analizados inmediatamente después de cada actualización de la base de datos de firma de virus.

- **Utilice un Firewall:** Tener siempre activo el Firewall de la computadora, para proteger las conexiones entrantes y salientes.

- **Realice análisis regulares en su computador:** Periódicamente se debe ejecutar un análisis completo del equipo con el software antivirus, lo que servirá para detectar las amenazas de virus existentes en el computador.

- **Tenga precaución con los archivos adjuntos y descargas:** No abra correos con archivos adjuntos de usuarios desconocidos, o de usuarios conocidos si no esperaba correos de ellos. Asegúrese de analizar todos los archivos adjuntos antes de descargarlos.

- **Evitar la descarga de programas de lugares no seguros o pocos fiables de Internet:** Muchas páginas web permiten la descarga de programas y archivos con la posibilidad que estos archivos estén infectados. Rechazar archivos que no se hayan solicitado cuando se

esté en chats o grupos de noticias. Hay que tener especial cuidado y aceptar sólo lo que llegue de un remitente conocido y de confianza.

- **Analizar siempre con el antivirus**: Los dispositivos extraíbles que entran y salen de la computadora antes de ser usados deberán ser examinados para detectar la presencia de virus.

- **Descargue los parches de seguridad.** Mantener el sistema operativo actualizado para evitar fallos de seguridad, por lo que es importante tener configurado los computadores para que las actualizaciones se realicen automáticamente.