**MEDIANTE UN MAPA CONCEPTUAL REPRESENTE ESTA INFORMACION**

**Virus informáticos**

**¿Qué son los virus informáticos? :** Un virus informático es un programa que puede infectar a otros programas, modificándolos de tal manera que causen daño en el acto (borrar o dañar archivos) o afectar su rendimiento o seguridad. Este software constituye una amenaza muy seria; se propaga más rápido de lo que se tarda en solucionarlo. Por lo tanto es necesario que los usuarios se mantengan informados acerca de los virus, huyendo de la ignorancia que les han permitido crecer hasta llegar a ser un grave problema.
**¿Qué es un caballo de Troya? :**Un caballo de Troya es un programa que hace algo oculto y que el usuario no ha aprobado, como abrir una conexión para que alguien externo tenga acceso a nuestra información. Finalmente, mucha gente usa el término "Troyano" para referirse solamente a un programa malicioso que no se copia a si mismo, a diferencia de los llamados "gusanos" que estos si se copian y propagan rápidamente. **¿Cuáles son los principales tipos de virus para PC? :**La primera clase incluye los que infectan archivos, adjuntos a programas ordinarios, aunque algunos pueden infectar cualquier archivo. Un virus de acción directa selecciona uno o varios programas para infectar cada vez que el programa es ejecutado. Uno 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 de los que infectan archivos de sistema o sector de arranque. Estos virus, infectan el área de sistema en un disco. Hay algunos que se ejecutan al iniciarse Windows, y virus que infectan directamente al sector de arranque de discos duros, pudiendo incluso dañarlos permanentemente. Hay otros virus que modifican las entradas a la tabla de archivos para que el virus se ejecute. Hay que tener en cuenta que estos pueden causar perdida de información (archivos).

**¿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. También usted puede encontrarse con un virus simplemente visitando ciertos tipos de páginas web que utilizan un componente llamado ActiveX o Java Applet. Además, usted puede ser infectado por un virus simplemente leyendo un e-mail dentro de ciertos tipos de programas de e-mail como Outlook.
**¿Qué hacen los virus?:**Cuando un virus lleva a cabo la acción para la que había sido creado, se dice que se ejecuta la carga, pueden ser bastante maliciosos e intentan producir un daño irreparable al ordenador personal destrozando archivos, desplazando/sobrescribiendo el sector de arranque principal, borrando los contenidos del disco duro o incluso escribiendo sobre la BIOS, dejando inutilizable el equipo. La mayoría de los virus no borran todos los archivos del disco duro. La razón de esto es que una vez que el disco duro se borra, se eliminará el virus, terminando así el problema.

**¿Por qué la gente crea virus?:** Algunos virus se crean por el desafío que implica crear una amenaza que sea única, no detectable, o simplemente devastadora para su víctima. El creador espera que el virus se propague de tal manera que le haga famoso. La notoriedad aumenta cuando el virus es considerado tal amenaza que los fabricantes de antivirus tienen que diseñar una solución. **¿Cómo sé si tengo un virus?:**Muchos virus se anuncian ellos mismos produciendo un sonido o mostrando un mensaje, pero también 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, un antivirus actualizado es el único que puede indicarnos si tenemos una infección.

**¿Cómo puedo evitar ser infectado por un virus?:** La mejor herramienta para combatir virus es saber como actúan, infectan y se propagan. No obstante, le recomendamos lo siguiente: El correo electrónico es el medio de transmisión preferido por los virus, por lo que hay que tener especial cuidado en su utilización. Cualquier correo recibido puede contener virus aunque no le acompañe el símbolo de datos adjuntos (el habitual "clip"). Además, no es necesario ejecutar el archivo adjunto de un mensaje de correo para ser infectado. Por ejemplo, en versiones antiguas y no actualizadas del MS Internet Explorer basta únicamente con abrir el mensaje, o visualizarlo mediante la 'vista previa'. Para prevenir esto, lo mejor es verificar los mensajes no esperados a ver si son reales antes de abrirlos. Un indicativo de posible virus es la existencia en el asunto del mensaje de palabras en un idioma diferente (generalmente inglés).

1. Muchas páginas de Internet permiten la descarga de programas y archivos a los ordenadores de los usuarios. Cabe la posibilidad de que estos archivos estén infectados con virus.
2. Como no existen indicadores claros que garanticen su fiabilidad, debemos evitar la descarga de programas gratis. Por lo general, son sitios seguros aquellos que muestran una información clara acerca de su actividad y los productos o servicios que ofrecen; también los avalados por organizaciones tales como editoriales, organismos oficiales, etc.
3. Gracias a Internet es posible intercambiar información y conversar en tiempo real sobre temas muy diversos mediante los chats. Un amplio número de virus utiliza precisamente estos chats para propagarse. Lo hacen enviando ficheros adjuntos (generalmente con nombres muy sugerentes). En general, si desconocemos el usuario que nos envía el archivo, debemos de rechazarlo.
4. Una muy buena forma de minimizar el impacto de un virus, tanto a nivel corporativo como particular, es respaldar correctamente con copias de seguridad de nuestra información.
5. Realizar copias periódicas y frecuentes de nuestra información más importante es una magnífica política de seguridad. De esta manera, una pérdida de datos, causada por ejemplo por un virus, puede ser superada mediante la restauración de la última copia.

**¿Qué hacer si he sido infectado?:** Su acción principal debería será contener el virus para que no se propague por cualquier sitio y así poder erradicarlo. Si trabaja en un entorno de red y tiene un administrador de sistema, dígale lo que ha sucedido. Es posible que la máquina haya infectado a más de una máquina de su grupo de trabajo u organización. Si usted trabaja en una red local, desconecte el cable de la red inmediatamente. Una vez que usted ha contenido el virus, necesitará desinfectar su sistema, y después trabajar cuidadosamente buscar cualquier propagación del mismo en su red local o a sus contactos. De esta forma puede asegurarse de que no volverá a infectar su ordenador accidentalmente. Finalmente pregúntese quien ha usado el ordenador durante las últimas semanas. Si hay otros que lo hayan podido utilizar, pueden haber transportado, sin darse cuenta, la infección a su ordenador y necesitarán ayuda. Pregúntese si ha enviado algún fichero, como e-mails con ficheros adjuntos, o si ha copiado algún fichero de su máquina a un servidor, página web o sitio FTP recientemente. Si ha sido así, revíselos para ver si han sido infectados, y si lo han sido, informe a otras personas que puedan tener actualmente una copia del fichero infectado en su máquina.

**¿Qué es un bulo?:** Un bulo es una noticia o una información falsa. Normalmente llega por correo electrónico y tiene un mensaje con contenido falso: por ejemplo que debemos borrar tal o cual fichero de nuestro sistema porque se trata de un virus. Los bulos se sirven de la propia mentira para propagarse a sí mismos: recomiendan que ese mensaje sea enviado a tantas personas como sea posible. Solo el administrador de sistema puede borrar archivos de Windows o del sistema.

**¿Cómo funciona un antivirus?:** La clave de los antivirus reside en unos ficheros de configuración donde se almacenan una serie de patrones que sirven para identificar los virus. El antivirus analiza cada uno de los correos entrantes en el sistema, ficheros, disquetes, etc y busca dentro ellos esos patrones. Si el fichero o correo bajo análisis tiene alguno de los patrones, entonces se ha detectado el virus. Dependiendo de la configuración del antivirus, éste informará al usuario o simplemente lo borrará. Por esta razón es muy importante que los ficheros de datos del antivirus estén permanentemente actualizados. En general, los antivirus modernos se actualizan automáticamente (conectándose al proveedor) cada vez que se inicia una conexión con Internet.