¿Qué es la seguridad informática?

La seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. Aunque ya hay métodos muy capaces de preservar esta información a salvo, no hay ninguna técnica que permita asegurar la inviolabilidad de un sistema.

La protección puede hacerse desde dos puntos de vista distintos

Punto de vista lógico:

Es por medio del desarrollo de un software antivirus o firewall integrados en el sistema operativo. Desde este punto, la amenaza puede convivir en la red, pero el software de la máquina final, puede detenerla.

Punto de vista físico:

Vinculado con el mantenimiento. Es un sistema perimetral físico que protege de forma proactiva las amenazas de toda la red antes de que éstas puedan llegar a su destino final, independientemente de si la máquina final tiene protección.

¿De dónde provienen las amenazas a nuestro sistema?

Provienen de programas dañinos que se instalan en la computadora del usuario por distintas vías, email, software ilegal creackeado y recompilado, parches para programas sin licencia, páginas web con código malicioso, etc, en definitiva, los temidos virus. O de forma remota, provocados por delincuentes que se conectan a internet e ingresan a distintos sistemas por contener una apertura de puertos en los router de las empresas y domicilios sin securizar.

Seguridad informática contra los virus

Hay que ser conscientes de la amplísima lista de virus que hay en la actualidad. Y una vez sea así, atacarles para que nuestros sistema o nuestros equipos no sean infectados. Por eso, hay que mantener una seguridad continuada o actuar directamente desde el foco y deshacerse de la amenaza lo antes posible. Los virus más comunes a los que nos enfrentamos cada día son:

Aquellos virus que están ocultos en la memoria RAM. Les da la oportunidad de interceptar y controlar las distintas operaciones que se realizan en el ordenador, infectando programas y carpetas.

Los virus de acción directa. Aquellos que hacen que se ejecute rápidamente y se extienda por todo el equipo, llevándose por delante el contagio de toda carpeta o archivo por el que pasan.

Los virus cifrados. Son los de arranque, los de fichero o los de sobre escritura. Pueden afectar a todo el ordenador en un abrir y cerrar de ojos.

Medidas de Seguridad informática

Los más comunes son los programas antivirus, los cortafuegos o firewalls por software o perimetrales, la encriptación de la información y el uso de contraseñas fuertes. Creación de entornos de trabajo con directivas de seguridad, políticas de ejecución de software, filtrado de correo electrónico, filtrado de urls o direcciones web por categorías o dominios no permitidos, filtrado de aplicaciones que no se desean ejecutar, (youtube,

Facebook, Dropbox, google drive, etc.) Conexiones remotas de empleados de la empresa mediante aplicaciones seguras y cifradas. Creación de listas blancas y negras para distintos softwares, monitorización de todo el tráfico de la red, analíticas por franjas de horarios y aplicaciones que se realizan en internet desde cualquier máquina de la empresa, copias de seguridad en diferentes ubicaciones de la red y en la nube y monitorización del estado de las actualizaciones de los parches de seguridad o críticos de los sistemas operativos de la empresa.

Los sistemas deben de ser integrales y confidenciales, es decir, con información modificable sólo por personas autorizadas, y para ser leídos solamente por usuarios autorizados.

En la mayoría de los ámbitos de la seguridad, lo esencial es la capacitación de los usuarios, para ellos mismos, protegerse de las amenazas básicas que pueda haber. Después, habrá que detectar cuáles son las más frecuentes para luchar contra ellas.