Seguridad Informatica

Las amenazas pueden proceder desde programas dañinos que se instalan en la **computadora** del usuario (como un **virus**) o llegar por vía remota (los delincuentes que se conectan a **Internet** e ingresan a distintos sistemas).

Tipos de virus

En el caso de los virus hay que subrayar que en la actualidad es amplísima la lista de ellos que existen y que pueden vulnerar de manera palpable cualquier equipo o sistema informático. Así, por ejemplo, nos encontramos con los llamados virus residentes que son aquellos que se caracterizan por el hecho de que se hallan ocultos en lo que es la memoria RAM y eso les da la oportunidad de interceptar y de controlar las distintas operaciones que se realizan en el ordenador en cuestión llevando a cabo la infección de programas o carpetas que formen parte fundamental de aquellas.

De la misma forma también están los conocidos virus de acción directa que son aquellos que lo que hacen es ejecutarse rápidamente y extenderse por todo el equipo trayendo consigo el contagio de todo lo que encuentren a su paso.

Los virus cifrados, los de arranque, los del fichero o los sobreescritura son igualmente otros de los peligros contagiosos más importantes que pueden afectar a nuestro ordenador.

Software de seguridad informática

Entre las herramientas más usuales de la seguridad informática, se encuentran los **programas antivirus**, los cortafuegos o firewalls, la encriptación de la información y el uso de contraseñas (passwords). Herramientas todas ellas de gran utilidad como también lo son los conocidos sistemas de detección de intrusos, también conocidos como anti-spyware. Se trata de programas o aplicaciones gracias a los cuales se puede detectar de manera inmediata lo que son esos programas espías que se encuentran en nuestro sistema informático y que lo que realizan es una recopilación de información del mismo para luego ofrecérsela a un dispositivo externo sin contar con nuestra autorización en ningún momento. Entre este tipo de espías destaca, por ejemplo, Gator.

Claves para un uso seguro de los sistemas

Un sistema seguro debe ser **íntegro** (con información modificable sólo por las personas autorizadas), **confidencial** (los datos tienen que ser legibles únicamente para los usuarios autorizados), **irrefutable** (el usuario no debe poder negar las acciones que realizó) y tener **buena disponibilidad** (debe ser estable).

De todas formas, como en la mayoría de los ámbitos de la **seguridad**, lo esencial sigue siendo la capacitación de los usuarios. Una persona que conoce cómo protegerse de las amenazas sabrá utilizar sus recursos de la mejor manera posible para evitar ataques o accidentes.

En otras palabras, puede decirse que la seguridad informática busca garantizar que los recursos de un sistema de información sean utilizados tal como una organización o un usuario lo ha decidido, sin intromisiones.

Las cuatro áreas principales que cubre la seguridad informática

1. **Confidencialidad**: Sólo los usuarios autorizados pueden acceder a nuestros recursos, datos e información.
2. **Integridad**: Sólo los usuarios autorizados deben ser capaces de modificar los datos cuando sea necesario.
3. **Disponibilidad**: Los datos deben estar disponibles para los usuarios cuando sea necesario.
4. **Autenticación**: Estás realmente comunicándote con los que piensas que te estás comunicando.

Medidas para el mantenimiento de la seguridad informática y la prevención de intrusiones

Los ataques más utilizados en contra de un sistema informático son los troyanos, los gusanos y la suplantación y espionaje a través de redes sociales. También son populares los ataques DoS/DDoS, que pueden ser usados para interrumpir los servicios. A menudo algunos usuarios autorizados pueden también estar directamente involucrados en el robo de datos o en su mal uso. Pero si se toman las medidas adecuadas, la gran mayoría de este tipo de ataques pueden prevenirse, por ejemplo a través de la creación de diferentes niveles de acceso, o incluso limitando el acceso físico. Las medidas de **seguridad informática** que puedes tomar incluyen:

- **Asegurar la instalación de software legalmente adquirido**: por lo general el software legal está libre de troyanos o virus.
- **Suites antivirus**: con las reglas de configuración y del sistema adecuadamente definidos.
- **Hardware y software cortafuegos**: los firewalls ayudan con el bloqueo de usuarios no autorizados que intentan acceder a tu computadora o tu red.
- **Uso de contraseñas complejas y grandes**: las contraseñas deben constar de varios caracteres especiales, números y letras. Esto ayuda en gran medida a que un hacker pueda romperla fácilmente.
- **Cuidado con la ingeniería social**: a través de las redes sociales los ciberdelincuentes pueden intentar obtener datos e información que pueden utilizar para realizar ataques.
- **Criptografía, especialmente la encriptación**: juega un papel importante en mantener nuestra información sensible, segura y secreta.