

Seguridad informática

Seguridad informática, técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados. Estos daños incluyen el mal funcionamiento del *hardware*, la pérdida física de datos y el acceso a bases de datos por personas no autorizadas. Diversas técnicas sencillas pueden dificultar la delincuencia informática. Por ejemplo, el acceso a información confidencial puede evitarse destruyendo la información impresa, impidiendo que otras personas puedan observar la pantalla del ordenador, manteniendo la información y los ordenadores bajo llave o retirando de las mesas los documentos sensibles. Sin embargo, impedir los delitos informáticos exige también métodos más complejos.

En un sistema de los denominados "tolerante a fallos" dos o más ordenadores funcionan a la vez de manera redundante, por lo que si una parte del sistema falla el resto asume el control.

Los virus informáticos son programas, generalmente destructivos, que se introducen en el ordenador (al leer un disco o acceder a una red informática) y pueden provocar pérdida de la información (programas y datos) almacenada en el disco duro. Existen programas antivirus que los reconocen y son capaces de "inmunizar" o eliminar el virus del ordenador. Para evitar problemas en caso de apagón eléctrico existen las denominadas UPS (acrónimo de *Uninterrupted Power Supply*), baterías que permiten mantener el sistema informático en funcionamiento, por lo menos el tiempo necesario para apagarlo sin pérdida de datos. Sin embargo, la única forma de garantizar la integridad física de los datos es mediante copias de seguridad.

El mayor problema que tienen que resolver las técnicas de seguridad informática es el acceso no autorizado a datos. En un sistema seguro el usuario, antes de realizar cualquier operación, se tiene que identificar mediante una clave de acceso. Las claves de acceso son secuencias confidenciales de caracteres que permiten que los usuarios autorizados puedan acceder a un ordenador. Para ser eficaces, las claves de acceso deben resultar difíciles de adivinar. Las claves eficaces suelen contener una mezcla de caracteres y símbolos que no corresponden a una palabra real. Además, para aumentar la seguridad, los sistemas informáticos suelen limitar el número de intentos de introducir la clave.

Las tarjetas de contraseña son tarjetas de plástico que no pueden ser manipuladas, dotadas de un microprocesador que almacena una clave de acceso que cambia frecuentemente de forma automática. Cuando se entra en un ordenador mediante una tarjeta de acceso, el ordenador lee la clave de la tarjeta y otra clave introducida por el usuario, y las compara respectivamente con una clave idéntica a la de la tarjeta (que el ordenador genera automáticamente) y con la clave de acceso del usuario, que está almacenada en una lista confidencial. En el futuro, es posible que las claves y las tarjetas de acceso se vean reforzadas por mecanismos biométricos basados en características personales únicas como las huellas dactilares, los capilares de la retina, las secreciones de la piel, el ácido desoxirribonucleico (ADN), las variaciones de la voz o los ritmos

de teclado. Sistemas operativos como Mac OS, UNIX y Windows-NT permiten restringir el acceso a recursos del sistema (ficheros, periféricos...) de acuerdo con esa identificación.

Los *hackers* son usuarios muy avanzados que por su elevado nivel de conocimientos técnicos son capaces de superar determinadas medidas de protección. Internet, con sus grandes facilidades de conectividad, permite a un usuario experto intentar el acceso remoto a cualquier máquina conectada, de forma anónima. Las redes corporativas u ordenadores con datos confidenciales no suelen estar conectadas a Internet; en el caso de que sea imprescindible esta conexión se utilizan los llamados cortafuegos, un ordenador situado entre las computadoras de una red corporativa e Internet. El cortafuegos impide a los usuarios no autorizados acceder a los ordenadores de una red, y garantiza que la información recibida de una fuente externa no contenga virus.

Unos ordenadores especiales denominados servidores de seguridad proporcionan conexiones seguras entre las computadoras conectadas en red y los sistemas externos como instalaciones de almacenamiento de datos o de impresión. Estos ordenadores de seguridad emplean el cifrado en el proceso de diálogo inicial, el comienzo del intercambio electrónico, lo que evita una conexión entre dos ordenadores a no ser que cada uno de ellos reciba confirmación de la identidad del otro.

Una técnica para proteger la confidencialidad es el cifrado. La información puede cifrarse y descifrarse empleando ecuaciones matemáticas y un código secreto denominado clave. Generalmente se emplean dos claves, una para codificar la información y otra para descodificarla. La clave que codifica la información, llamada clave privada, sólo es conocida por el emisor. La clave que descodifica los datos, llamada clave pública, puede ser conocida por varios receptores. Ambas claves se modifican periódicamente, lo que complica todavía más el acceso no autorizado y hace muy difícil descodificar o falsificar la información cifrada. Estas técnicas son imprescindibles si se pretende transmitir información confidencial a través de un medio no seguro como puede ser Internet. Las técnicas de firma electrónica permiten autentificar los datos enviados de forma que se pueda garantizar la procedencia de los mismos (imprescindible, por ejemplo, a la hora de enviar una orden de pago).