



CONCEPTOS BÁSICOS

SEGURIDAD Y REDES

Un sistema informático se compone de 5 elementos: hardware, software, datos, memoria y usuarios.

De estos componentes cualquiera puede convertirse en un objetivo para el delincuente informático. Con estas opciones para poder atacar algún sistema, se dificulta el análisis de riesgos y ofrece la ventaja de aplicar al delincuente la filosofía del punto más débil, lo que significa, atacar al sistema por su punto más vulnerable. Por lo tanto, de cara a la protección del sistema, será necesario considerar por igual a los elementos antes citados como vulnerables de un ataque


Principios de la Seguridad Informática

- Principio del Acceso más fácil.
- Principio de la Caducidad de la Información.
- Principio de la Eficiencia.

Principio del Acceso más fácil: “El intruso al sistema utilizará cualquier artilugio o mecanismo que haga más fácil su acceso al sistema y posterior ataque.”

Las debilidades de todo sistema informático se pueden agrupar en función de los problemas que ocasionan debido a la exposición, vulnerabilidades, ataques y amenazas.

La exposición se refiere a la posible pérdida o daño en el sistema debido a modificación, extravío de datos o acceso no autorizado al sistema. La vulnerabilidad es el punto débil del sistema que, si se traspasa, produce los efectos nocivos indicados. Un ataque es el hecho de la intromisión con daño manifiesto al sistema y, por último, las amenazas consisten en desastres naturales, errores humanos, fallos de hardware y software, sean fortuitos o voluntarios.





Clasificar las amenazas dado que los objetivos principales de ataque son el hardware, el software y los datos, se clasifican las amenazas en cuatro tipos:

Amenazas de interrupción, interceptación, modificación


Generación de la información en general. Los objetivos amenazados (hardware, software, datos) pueden caracterizarse como un flujo (información, servicio, programas, datos, etc.).


Interrupción: Se produce cuando un punto del sistema se daña, pierde o deja de funcionar. La detección de este problema es inmediata, tanto por el sistema como por el usuario. Como ejemplos de interrupción son la destrucción maliciosa del hardware, borrado de programas y/o datos, fallos del sistema operativo, etc.

Intercepción: Es el acceso a la información por parte de personas no autorizadas. Su detección resulta difícil dado que no deja huellas. Como ejemplos de interceptación son las copias ilícitas de programas y la escucha de una línea de datos

Modificación: Se produce una amenaza de modificación cuando alguien no autorizado accede al sistema y cambia el entorno para su beneficio. Dependiendo de las circunstancias puede resultar difícil de detectar, siendo ejemplos típicos los de modificación de una base de datos y los de hardware, aunque éste último es más sofisticado y menos frecuentes.

Generación: Contempla la creación de nuevos objetivos dentro del sistema informático, tales como añadir transacciones específicas de red o registros a una base de datos. Su detección resulta difícil y en muchos casos se trata de un delito de falsificación, para defenderse frente a estas amenazas se deben crear métodos de control que preserven el supuesto secreto asociado a la información, el acceso a esos datos solamente a las personas autorizadas y, por último, que tales datos estén disponibles a dicho usuario cuando éste lo desee. Estos tres aspectos darán lugar a los tres elementos básicos de la seguridad informática conocidos como confidencialidad, integridad y disponibilidad de la información.





En cuanto a los sistemas de control, éstos pueden ser mediante hardware, a través del uso de dispositivos que limiten físicamente el acceso a un programa, aplicación o datos; mediante software directo, los relacionados con el desarrollo de los sistemas operativos y programas que contemplan la protección de archivos, directorios, definición de niveles de usuarios, etc., y por último, el software de aplicación para el cifrado de la información.

Principio de la eficiencia. “Las medidas de control se implementan para ser utilizadas de forma efectiva. Deben ser eficientes, fáciles de usar y apropiadas al medio.” El decir que sean efectivas significa que cuando sean invocadas por un programa o por el usuario, funcionen perfectamente, lo que se puede asociar al hecho de estar en el lugar y momento oportunos. En cuanto a la eficiencia, se refiere a indicar que debe funcionar sin producir trastornos ni fallos al sistema informático, en términos de consumo de tiempo, ocupación de espacio de memoria o deficiente interfaz hombre/máquina. En resumen, que funcione y lo haga bien, optimizando el uso de recursos

Todo esto lleva a la afirmación de que un buen sistema de seguridad es aquel que contempla controles eficaces y no obstante, pasa desapercibido por el sistema informático y por sus usuarios.

