Derechos de autor y seguridad informática

Seguridad informática

Podemos definir **qué es la seguridad informática** como el proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica el proceso de proteger contra intrusos el uso de nuestros recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente.

La seguridad informática es en realidad una rama de un término más genérico que es la seguridad de la información, aunque en la práctica se suelen utilizar de forma indistinta ambos términos cuando en realidad no son lo mismo. La definición de seguridad de la información no debe ser confundida con la de «seguridad informática», ya que esta última solo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

La seguridad informática abarca una serie de medidas de seguridad, tales como programas de software de antivirus, firewalls, y otras medidas que dependen del usuario, tales como la activación de la desactivación de ciertas funciones de software, cuidar del uso adecuado de la computadora, los recursos de red o de Internet.

La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

Objetivos

La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los trabajadores y de la organización en general y como principal contribuyente al uso de programas realizados por programadores. La seguridad informática debe proteger los activos informáticos, entre los que se encuentran los siguientes:

- **La infraestructura computacional**: velar por que los equipos funcionen adecuadamente y anticiparse en caso de fallas, robos, incendios, sabotajes, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.

- **Los usuarios**: son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información.

- **La información**: esta es el principal activo, que se utiliza en la infraestructura computacional y es utilizada por los usuarios.

Amenazas

No sólo las amenazas que surgen de la programación y el funcionamiento de un dispositivo de almacenamiento, transmisión o proceso deben ser consideradas, también hay otras circunstancias no informáticas que deben ser tomadas en cuenta. Muchas son a menudo imprevisibles o inevitables, de modo que las únicas protecciones posibles son las copias de seguridad y la descentralización, por ejemplo, mediante determinadas estructuras de redes en el caso de las comunicaciones o servidores en alternos para la disponibilidad.

Las *amenazas* pueden ser causadas por:

- **Usuarios**: causa del mayor problema ligado a la seguridad de un sistema informático. En algunos casos sus acciones causan problemas de seguridad, si bien en la mayoría de los casos es porque tienen permisos sobredimensionados y no se les han restringido acciones innecesarias.

- **Programas maliciosos**: programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado en la computadora, abriendo una puerta a intrusos o bien modificando los datos. Estos programas pueden ser un virus informático, un gusano informático, un troyano, una bomba lógica,

un programa espía o *spyware*, en general conocidos como *malware*.

- **Errores de programación**: la mayoría de los errores de programación que se pueden considerar como una amenaza informática es por su condición de poder ser usados por personas ajenas a la institución.
- **Intrusos**: personas que consiguen acceder a los datos o programas a los cuales no están autorizados, clasificados en crackers, defacers, hackers, script kiddie o script boy, viruxers, etc.

- **Un siniestro** (robo, incendio, inundación): una mala manipulación o mala intención derivan en la pérdida del material o de los archivos.
- **Personal técnico interno**: técnicos de sistemas, administradores de bases de datos, técnicos de desarrollo, etc. Los motivos que se encuentran entre los habituales son: disputas internas, problemas laborales, despidos, fines lucrativos, espionaje, etc.
- **Fallos electrónicos o lógicos de los sistemas informáticos en general**.

Autor:

EDUFUTURO

Referencias:

http://www.viu.es/la-seguridad-informatica-puede-ayudarme/

https://www.ecured.cu/Seguridad_Inform%C3%A1tica

https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica