

Seguridad informática

La seguridad informática, también conocida como ciberseguridad o seguridad de tecnologías de la información, es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada.

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

Puesto simple, la seguridad en un ambiente de red es la habilidad de identificar y eliminar vulnerabilidades. Una definición general de seguridad debe también poner atención a la necesidad de salvaguardar la ventaja organizacional, incluyendo información y equipos físicos, tales como los mismos computadores. Nadie a cargo de seguridad debe determinar quién y cuándo puede tomar acciones apropiadas sobre un ítem en específico. Cuando se trata de la seguridad de una compañía, lo que es apropiado varía de organización en organización. Independientemente, cualquier compañía con una red debe tener una política de seguridad que se dirija a la conveniencia y la coordinación.

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, protocolos 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 está concebida para proteger los activos informáticos, entre los que se encuentran los siguientes:

- **La infraestructura computacional:** es una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la seguridad informática en esta área es 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. Debe protegerse el sistema en general para que el uso por parte de ellos no pueda poner en entredicho la seguridad de la información y tampoco que la información que manejan o almacenan sea vulnerable.

- **La información:** esta es el principal activo. Utiliza y reside 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 redundancias y la descentralización, por ejemplo, mediante determinadas estructuras de redes en el caso de las comunicaciones o servidores en clúster 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, no se les han restringido acciones innecesarias, etc.
- **Programas maliciosos:** programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado en el ordenador, 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 como *exploits* por los *crackers*, aunque se dan casos donde el mal desarrollo es, en sí mismo, una amenaza. La actualización de parches de los sistemas operativos y aplicaciones permite evitar este tipo de amenazas.
- **Intrusos:** personas que consiguen acceder a los datos o programas a los cuales no están autorizados (*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.**
- **Catástrofes naturales:** rayos, terremotos, inundaciones, rayos cósmicos, etc.

Referencias:

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