# Seguridad informática

En los últimos años, la seguridad informática se ha convertido en un tema de interés público. Tanto expertos en la materia como usuarios generales utilizan términos como "clave de usuario", "contraseña (o *password*)", "fraude informático", "*hacker*", etcétera. Hoy por hoy no solo es deseable, sino indispensable, tener conocimientos firmes relacionados con este tema, pues sin ellos el usuario de computadoras podría caer en un estado de indefensión que ponga en peligro no solo su información o equipo, sino su propia integridad.

Gómez (2006) define la seguridad informática como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática cuyos efectos puedan conllevar daños sobre la información, equipo o *software*. Por su parte, Kissel (2012) la define como la protección de información y sistemas de información de acceso no autorizado. En efecto, con base en estos conceptos, la seguridad informática se vincula con tres elementos básicos: la información que, como activo intangible, representa quizá el elemento más sensible y vulnerable; el *software*, cuya pérdida o modificación mal intencionada puede representar severos quebrantos económicos u operativos no solo hacia el usuario sino a toda una institución; y el *hardware*, que al fallar provoca retrasos en la operación diaria y la consecuente pérdida de tiempo y costos elevados.

Existe un sinnúmero de medidas preventivas que permiten proteger estos tres elementos, como respaldos de información (*backups*), controles de acceso de *hardware* y *software*, programas antivirus, antis*pyware* y *antispam*, uso de *firewalls*, actualizaciones continuas al sistema operativo, mantenimiento al equipo de cómputo y protección física en las áreas de operaciones de red (extintores, detectores de humo y calor, sistemas de anclaje, ventilación, controles de temperatura y humedad, reguladores de voltaje, sistemas de suministro continuo de energía, entre otros).

Sin embargo, para un usuario, la protección de su información es generalmente más importante que la protección misma del *software* o su equipo, razón por la cual, para garantizar la seguridad de los datos, es preciso cumplir con tres componentes fundamentales: integridad, que significa que la información debe ser modificada solo por entidades autorizadas; disponibilidad, es decir, tener acceso a la información cuando se lo requiera; y confidencialidad, donde solo instancias facultadas para ello podrán visualizar los datos.

Debido a la importancia que ha ido adquiriendo la seguridad en cómputo, en las siguientes ediciones de cápsulas TI se abordarán en detalle recomendaciones diversas que permitan evitar posibles pérdidas de datos, robos de información, accesos no autorizados, suplantación de identidad, presencia de *malware*, entre otros.

## REFERENCIAS


- Gómez, Álvaro (2006). *Enciclopedia de la seguridad informática,* RA-MA, España.
- Kissel, Richard (2012). *Glossary of Key Information Security Terms*, National Institute of Standards and Technology. doi.org/10.6028/NIST.IR.7298.