Seguridad informática

¿Podemos pensar en una cuarta revolución industrial? Aunque en la historia de la humanidad podemos definir claramente tres revoluciones industriales, lo cierto es que existe una cuarta y, es precisamente, la que estamos viviendo en la actualidad, gracias a la aparición de las tecnologías de información y las comunicaciones (TIC), junto con Internet.

En las últimas dos décadas, las TIC han adquirido un valor en dimensiones que nunca antes había ocurrido en la historia, generando profundas transformaciones en todos los ámbitos socioeconómicos y, por supuesto, de la mano aparecieron conductas ilícitas cometidas sobre los datos, la información, los programas y todo aquel recurso tecnológico susceptible de ser manipulado ilícitamente.

La seguridad informática, o ciberseguridad, es una disciplina que se encarga de proteger la integridad y la privacidad de los datos y toda la información que se encuentre alojada en un sistema informático. La idea principal es que se pueda evaluar la seguridad de los sistemas de cómputo y redes para, posteriormente, protegerlos de los ataque informáticos que se pueden llevar a cabo a los sistemas.

Ciberseguridad

La seguridad informática se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, especialmente, en la información que se transmite a través de las redes de computadoras. Para minimizar todos los riesgos a la infraestructura y a la información se han creado a lo largo de la historia múltiples métodos, como estándares, protocolos, reglas, herramientas y obviamente leyes informáticas.

Debemos tener en cuenta que la seguridad informática únicamente se va a centrar en el medio de comunicación por el cual va a viajar la información. No debemos confundir este término con el de seguridad de la información, ya que esta última puede estar en diferentes medios y no solo en los medios informáticos.

TIPOS DE AMENAZAS PRESENTES EN LA ACTIVIDAD INFORMÁTICA

Troyano:
Son programas malwares capaces de introducirse en los ordenadores permitiendo el acceso a usuarios externos, a través de una red local o de internét, con el fín de controlar el ordenador o saquearle información sin afectar el funcionamiento de este.

Gusano:
Es un programa muy parecido a un virus diferenciándose de la forma en que se infecta. Los gusanos realizan copias de los ordenadores mismos, infectando a otros y propagándose automáticamente en una red independientemente de la acción humana.

Virus informático:
Programa creado para copiarse y propagarse a sí mismo, normalmente adjuntándose en aplicaciones. Cuando se ejecuta una aplicación infectada, puede infectar otros archivos. Se necesita acción humana

para que un virus se propague entre máquinas y sistemas. Esto puede hacerse descargando archivos, intercambiando disquetes y discos USB, copiando archivos a y desde servidores de archivos o enviando adjuntos de e-mail infectados.

Espía:
es aquel que, sin permiso o conciencia de sus actos por parte de un afectado, adquiere información privada para beneficio propio o de terceros.

Pharming:
Redirecciona con mala intención al usuario a un sitio web falso mediante la explotación del sistema DNS, denominándose secuestro o envenenamiento del DNS.

Phising:
Los ataques de phishing roban a los usuarios información personal sin el permiso de estos (principalmente de acceso a servicios financieros).Utilizan el correo basura (spam) para difundirse. Una vez que llega el correo al destinatario, intentan engañar a los usuarios para que faciliten datos de carácter personal para que estos introduzca datos personales de su cuenta bancaria, como su número de cuenta, contraseña, número de seguridad social, etc.

Spam:
Todo correo no deseado recibido por el destinatario, el cual viene de un envío automático y masivo por parte de aquel que lo emite. El ’spam’ generalmente se asocia al correo electrónico personal, pero no sólo afecta a los correos electrónicos personales, sino también a foros, blogs y grupos de noticias.

Protección de la información

La protección de la información se basa en garantizar el completo y total funcionamiento de las 3 dimensiones, para ello, debemos implementar medidas preventivas y reactivas.
Medidas preventivas se refiere a todas las acciones que pueden tomarse para evitar problemas no deseados. Por otro lado, las medidas reactivas son aquellas donde ya se ocasionó un problema de seguridad y hay que solventarlo.

Protección de la confidencialidad:
La confidencialidad puede romperse de varias maneras, tanto directas (hackeando la seguridad) como indirectas a través de errores humanos.

Protección de la integridad:
La integridad puede romperse de varias maneras similares a la de la confiabilidad, por lo cual, varias de sus acciones de seguridad son reutilizadas.

Protección de la disponibilidad:
La disponibilidad debe tenerse en cuenta para cuando ocurra un problema de seguridad como de forma preventiva al mismo.