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.

Pero, ¿esto fue siempre así? A lo largo de la historia, esta seguridad se ha ido transformando, gracias a los controles y auditorías sobre los sistemas, explotando las vulnerabilidades que se puedan encontrar en los mismos. Se han implementado medidas de seguridad física y lógicas en conjunto con la seguridad en Internet.

Por otro lado, sería fantástico poder analizar de forma particular cuál es el impacto que ha causado en la sociedad, en sus normas jurídicas y éticas. Además, reconocer e identificar los delitos informáticos y las consecuencias legales que implican el no acatarlas.

Bien, ha llegado el momento de adentrarnos en el estudio de este maravilloso mundo de seguridad.

Objetivos del módulo

En términos generales esperamos que a lo largo de este módulo podamos:

- Identificar todo tipo de amenazas informáticas, la importancia de los fallos, vulnerabilidades y las contingencias que se pueden tener.
- Conocer los aspectos generales de la seguridad de los sistemas informáticos, criterios generales de medidas de seguridad y protección a tener en cuenta.
- Brindar al futuro profesional conocimientos acerca de la importancia de la informática en la sociedad, los códigos de ética, moral y práctica profesional.

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.

Bajo este último concepto, la seguridad informática va a identificar, eliminar vulnerabilidades y proteger de ataques maliciosos a los equipos de cómputo, servidores, redes informáticas y todo aquel medio informático por el cual se transmita información.

Tipos de amenazas informáticas PARTE 1

Si bien todas están causadas por un ser humano, el atacante usa un tipo de software maligno llamado MALWARE para que realice todo el proceso de piratería.

MALWARE quiere decir malicius software y es un termino que se utiliza para definir a todos los software maliciosos que tienen como objetivo infiltrarse o dañar un sistema de informacion sin el consentimiento del usiario.

Es necesario que este infiltrado para el usuario.

Malware pueden ser virus, troyanos,gusanos o varios otros.

Algunas de las amenazas teconolías mas comunas que conocemos.

Virus: es el más antiguo de todos. Este tipo de malware es un componente de software cuyo objetivo es permanecer en un sistema copiandose a sí mismo en

varios lugares desde el momento que se ejecuta en el sistema. Así cuando lo borramos, sigue en memoria porque se guardó en otras partes del sistema.

Objetivo: destruir o inhabilitar archivos o programas.

No pueden afectar por sí mismos a otros dispositivos a menos que los pasemos por medio de un Hardware como es el caso de un usb

GUSANO: cuando la pc se empieza a conectar a la red. no solo se copia a sí mismo en el sistema, sino que usa la red para conectarse a otras por la vulnerabilidad.

El objetivo de los gusanos es replicarse a sí mismo hasta SATURAR el funcionamiento del sistema.

TROYANO: estructura utilizada para cargar cosas ocultas, ejemplo gusanos virus etc. Los troyanos general//son esos programas que descargamos sin licencia o crack.

Necesita la activación del usuario ya que no puede replicarse a él mismo.

Puede crear Backdoors. Servidor proxy o spam.

Tipos de amenazas informáticas PARTE 2

Existen algunos malware especialmente peligrosos porque son mas silenciosos

SPYWARE o software espías. No daña los dispositivos pero sí roba toda la información del sistema. Objetivo: estar oculto para robar todo tipo de datos. Puede acceder por la cámara o micrófono sin que el usuario lo utilice.
Malwares más complejos como los ROOTKITs que son un conjunto de softwares.

BOTNETS: mezcla entre bot y NETS red de robot puesto por un atacante para ser utilizadas todos al mismo tiempo.

RANSOMWARE: o software de secuestro suelen ser usados contra empresas para pedir dinero.

Protección de la información - HTML

Protección de la información

Protección de la información - PPT

Protección de la información - PPT

Protección de la confidencialidad

La confidencialidad puede romperse de varias maneras, tanto directas (hackeando la seguridad) como indirectas a través de errores humanos. Algunas técnicas para asegurar la confiabilidad pueden ser:

Nombre	Descripción
Encriptación	Significa cambiar el formato de los datos con la razón de que si estos son interceptados solo las personas autorizadas sepan cómo leerlos (medida preventiva).
Controles de acceso	Asegurar que solo las personas autorizadas puedan acceder a la información (medida preventiva).
Borrado remoto	Se refiere al esfuerzo de mantener los datos siempre privados, en el caso de que se perdiera el acceso, la capacidad de bloquear el dispositivo o borrar la información (medida reactiva).
Capacitación al personal	Existe un concepto llamado **ingeniería social**, el cual es la denominación que se le da a cómo los usuarios son engañados para otorgar sus accesos, la capacitación en estos problemas es una acción preventiva para evitarlos.