Objetivos de la Seguridad Informática

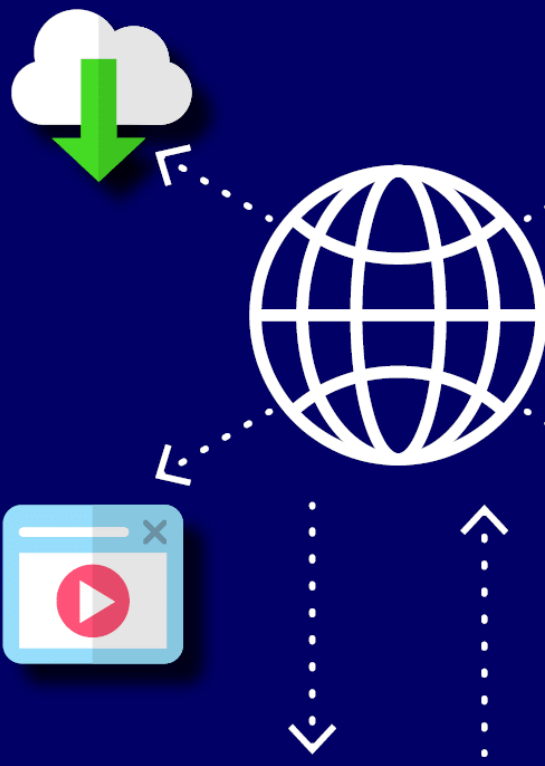
- ***Autenticación:*** Estar seguros de que la persona que envió el mensaje, es quien dice ser.
- ***Integridad:*** Asegurarse que la información no sea modificada por personas o procesos no autorizados.
- ***Confidencialidad:*** Garantizar que la información no sea accedida por terceros.
- ***Disponibilidad:*** Asegurarse que la información pueda ser accedida siempre que el usuario lo requiera.
- ***No Repudiación:*** Garantizar que el emisor no niegue que fue él quien envió la información.

¿Qué se quiere proteger?

- ***Datos:*** La información (conjunto de datos procesados) que viajan a través de la red.
- ***Equipos:*** Constituidos por *hardware* y software que consumen o proveen un servicio a usuarios específicos.
- ***Usuarios:*** Individuo que utiliza una PC, Sistema Operativo, Servicio o cualquier Sistema Informático.

Autor: Evelyn Terrones

Diseño: Dalesgry Tartaret



Seguridad Info

Es la encargada de diseñ
Procedimientos, Métodos y
prevención y reacción
proteger los activos inf

RMÁTICA

ıar Normas,
y Técnicas de
, a fin de
ormáticos

Algunos Ataques Informáticos

- ***Código malicioso:*** También llamado *malware*, es un tipo de *software* que tiene como objetivo infiltrarse o dañar un equipo informático o sistema de información, sin el consentimiento de su propietario.
- ***Denegación de servicio:*** Es un ataque que provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red o sobrecarga de los recursos computacionales del sistema, causando que un servicio o recurso sea inaccesible por los usuarios.
- ***Puerta trasera:*** También llamada *backdoor*, es una secuencia especial dentro del código de programación, mediante la cual se pueden evitar los sistemas de seguridad (autentificación) para acceder al sistema.
- ***Spoofing:*** Ocurre para fines maliciosos o de investigación y es cuando un atacante usa técnicas para hacerse pasar por una entidad distinta a través de la falsificación de los datos en una comunicación.
- ***Fuerza bruta:*** Es la forma de obtener una clave/contraseña probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso.
- ***Vulnerabilidades propias de los sistemas:*** Son debilidades a nivel de *hardware*, sistemas operativos, aplicaciones, protocolos de red, entre otros, que pueden ser aprovechadas por los atacantes.
- ***Escaneo de puertos:*** Es una técnica usada por *hackers* y administradores para auditar máquinas y redes con el fin de saber que puertos están abiertos/cerrados, qué servicios son ofrecidos, chequeo de existencia de un *firewall*, entre otros.
- ***Ingeniería social:*** Es la práctica de obtener información confidencial (ej. contraseñas) a través de la manipulación de usuarios.
- ***Spamming:*** Correo basura, son correos no deseados o anónimos, generalmente de forma masiva, que perjudican al receptor o al servicio.

Mecanismos de Protección más usados

- Control de Acceso/*Password*
- Antivirus
- *Firewall*
- Parches de Seguridad
- **IDS / IPS**
- **VPN**
- Políticas, Procedimientos, Normas, entre otros.