SEGURIDAD INFORMÁTICA

Introducción

UNTDF – IDEI | Profesor Lic. Leonardo de - Matteis | 2019/1c

Fundamentos y objetivos

La seguridad en sistemas es de suma relevancia en nuestra profesión principalmente debido a los cambios que ha producido la incorporación de Internet en nuestros trabajos y vida diaria.

El objetivo es alcanzar una visión global sobre lo que implica la seguridad en los sistemas informáticos y lo que los rodea.

Trataremos temas relativos a la seguridad en sistemas, abordando diferentes aspectos en forma general y relacionándolos con problemáticas y noticias actuales.

Temas a tartar dudrante el seminario

- ❑ Introducción a la seguridad
- ❑ Seguridad física
- ❑ Introducción a la criptografía y autenticación
- ❑ Seguridad en sistemas operativos
- ❑ Seguridad en bases de datos
- ❑ Seguridad en redes

Bibliografía

- Charles Pfleeger & Shari Lawrence Pfleeger. *Security in Computing* (5th edition)
- William Stallings. *Cryptography and Network Security: Principles and Practice* (7th edition)
- Matt Bishop. *Computer Security* (2nd edition)
- Ross J. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*
- Edward Amoroso. *Fundamentals of Computer Security Technology*
- Dieter Gollmann. *Computer Security*
- Bruce Schneier. *Applied Cryptography* (2nd edition)
- William Stallings. *Network Security Essentials: Applications and Standards*

Temario

- ❖ Hitos que influyen en la seguridad actual los sistemas.
- ❖ Definición de seguridad informática y terminología básica.
- ❖ Triada CIA.
- ❖ Terminología básica sobre control de acceso.
- ❖ Amenazas, vulnerabilidades y ataques.
- ❖ Controles y contramedidas.

¿Qué es la seguridad?

Según Diccionario de la Lengua Española (DLE):

Seguridad
Cualidad de seguro

de ~
Dicho de un mecanismo: Que asegura algún buen funcionamiento, precaviendo que este falle, se frustre o se violente.

Según New Oxford American Dictionary:

Security
Is the state of being free from danger or threat.

¿Qué es la seguridad?

"La seguridad es una necesidad básica. Es de interés en la prevención de la vida y las poesiones. La seguridad es tan antigua como la vida misma."

¿Qué es la seguridad informática?

La seguridad en sistemas se enfoca en proteger objetos de valor dentro de un sistema informático que posee datos y brinda servicios.

El objetivo es tratar de proveer distintos grados y tipos de seguridad.

Protección de los activos de un sistema de computación:

- ✓ Hardware
- ✓ Software
- ✓ Datos

Línea de tiempo

1950: Primeros ataques provenientes de personas cercanas a los sistemas.

1960: HW de protección de memoria.

1962: Mecanismos de control de acceso a los archivos.

1967: Funciones *one-way* (contraseñas).

1968: Seguridad en sistemas *operativos/kernels* (Multics).

1969/89: Comienza el desarrollo de ARPANET por parte de DARPA (Defense Advanced Research Projects Agency).

Línea de tiempo

1975: UNIX-UNIX *copy protocol* (UUCP) y *trapdoors* en emails.

1976: Criptografía de clave pública y firma digital.

1974/77: Trabajos de especificación y desarrollo de TCP/IP.

1978: Definición de RSA (sistema de clave pública).

1982: Declaración de TCP/IP como standard para la red militar de computadoras.

1983: DNS distribuido (vulnerable al *spoofing*).

Línea de tiempo

1980s: Sobre la base de ARPANET se interconectan redes militares y académicas. Luego interconexión mediante la National Science Foundation Network.

1984: Virus: comienzo de investigaciones.

1988: Internet Worm con 6000 computadoras afectadas (10% de Internet)

1988: Autenticación distribuida (Kerberos).

1989: Pretty Good Privacy (PGP) y Privacy Enhanced Mail (PEM).

1990s: Interconexión de redes comerciales y de organizaciones surgimiento de: Internet (red de aspecto libre y comercial).

Línea de tiempo

1990: *Remailers* anónimos.

1993: *Spoofing*, *sniffing*, *firewalls*.

1994: SSL v1.0 (navegador *Netscape*).

1996: *Exploits* Java (*web hacking*).

1997: DNSSec.

1998: *Netscanning*. IPSec.

1999: Primer ataque DDoS.

2000s: Infecciones de virus con propagaciones globales: *I LoveYou* (VBscript), *Red code*, *Nimbda*. Proliferación de *worms.*

Seguridad en una organización

En el pasado:

- Física
- Administrativa

En la actualidad:

- Computadoras: incorporan la necesidad de contar con elementos que protejan la información.

  Ejemplos: *time-sharing*, interconexiones *LAN* y *WAN*, *Internet*, sistemas distribuidos, etc.

La colección de herramientas diseñadas para dificultar la vida de los atacantes conforman la **seguridad en sistemas**.

Seguridad en una organización

¿Por qué a veces sólo se habla de **seguridad en redes**?

Debido a que no hay un límite claro entre estas dos formas de seguridad, pues todos los sistemas actuales son distribuidos por naturaleza.

Activos

Activos

Hardware:

- Computadoras
- Dispositivos secundarios: discos, memorias, impresoras, etc.
- Equipamiento y componentes de la red de computación

Software:

- Sistemas operativos
- Aplicaciones
- Desarrollos propios ★

Datos:

- Fotos, videos, música, correo electrónico, bases de datos, etc. ★

Factores relativos a la seguridad

En los sistemas computacionales actuales la seguridad informática debe estar presente y debe ser considerada como un aspecto de suma relevancia.

Deberán aplicarse políticas, medidas y controles sobre sistemas de la organización (*hardware* + *software* + redes) por la existencia de:

- Existencia de diversos protocolos de red.
- Diferentes medios para transferencia de datos: celulares, notebooks, etc.
- Acceso masivo a Internet: hogar y trabajo.

Factores relativos a la seguridad

Se suelen pasar por alto aspectos relativos a:

- control de tráfico;
- control de seguridad física;
- seguridad interna a la organización
- políticas de seguridad;
- políticas de control;
- políticas de auditorias;
- accesos remotos: VPNs;
- EDUCACION

Factores relativos a la seguridad

Tener en cuenta que la seguridad en sistemas debe aplicarse en:

- en el trabajo;
- en la empresa;
- en el hogar;
- en la movilidad

Factores relativos a la seguridad

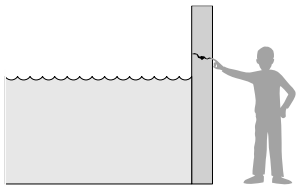
Puntos débiles actuales? …

- Redes *wifi*
- Redes cableadas
- Protocolos no seguros (sin utilización/combinación con otros seguros)
- Software con errores
- **Otros?** (formas de compartir la información, actitudes, etc.)

Terminología básica

- ✓ Vulnerabilidad
- ✓ Amenaza
- ✓ Ataque
- ✓ Contramedidas y control

Amenaza y vulnerabilidad



Objetivos de la Seguridad en sistemas

"El objetivo de la seguridad informática será mantener la integridad, disponibilidad, privacidad (sus aspectos fundamentales), control y autenticidad de la información manejada por computadoras".

Se debe proteger la información en los sistemas informáticos, es decir proteger los datos.

Características de la información:

- ✓ Es crítica
- ✓ Es valiosa
- ✓ Es sensitive

Objetivos de la Seguridad en sistemas

La protección de los datos implica:

- Integridad
- Confidencialidad
- Control
- Autenticidad

Se deben considerar aspectos adicionales:

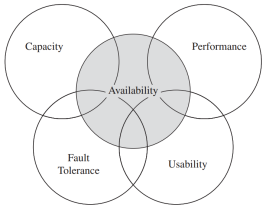
- No repudio
- Consistencia
- Control de acceso
- Protección a la réplica
- Aislamiento (cercano a la confidencialidad)
- Auditoría

Servicios: triada CIA

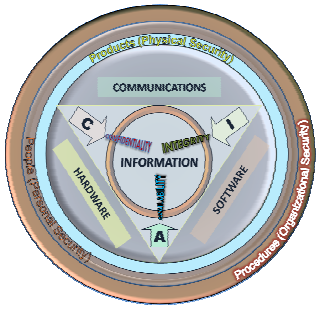
- **Confidencialidad**:
  capacidad de un sistema para asegurar que un activo sea visto solo por las partes autorizadas.
  Ejemplo: protección sobre la información transmitida, privacidad de los datos.
- **Integridad**:
  capacidad de un sistema para garantizar que un activo sea modificado solo por las partes autorizadas.
  Ejemplo: asegurar que los datos recibidos sean iguales a los enviados, es decir, detectar la modificación de mismos.

Servicios: triada CIA

- **Disponibilidad**:
  capacidad de un sistema para garantizar que un activo pueda ser utilizado por cualquiera de las partes autorizadas.
  Ejemplo: evitar la ocurrencia de eventos que impidan el acceso a los recursos por parte de los usuarios.



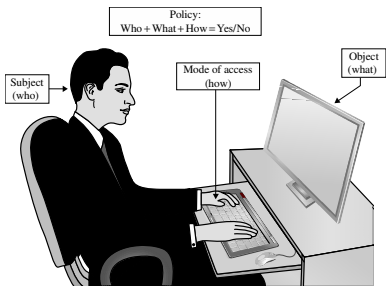
Triada CIA e interrelación con otros aspectos



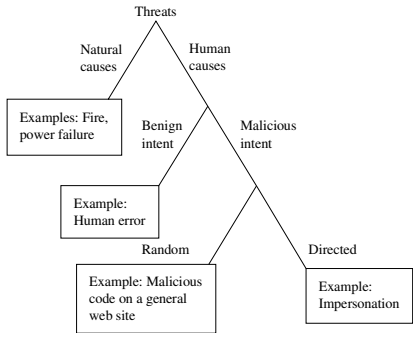
Servicios adicionales deseables

- **Autenticación**:
  capacidad de un sistema para confirmar la identidad de un remitente.
  Ejemplo: asegurar que la comunicación sea auténtica.
- **No repudio**:
  capacidad de un sistema para confirmar que un remitente no puede negar convincentemente haber enviado algo.
  Ejemplo: no permitir que un emisor niegue ocurrencia de una acción/mensaje.
- **Control de acceso**:
  capacidad de limitar y controlar el acceso a un sistema. Prevenir el uso inapropiado de recursos.

Control de acceso



Tipos de amenazas



Origen de amenazas

Dada una organización podemos tener diferentes orígenes de amenazas:

- Individuos: externos e internos.
- Software: con errores de programación, malicioso, etc.
- Catástrofes: fuego, inundaciones, terremotos, etc.

Amenaza persistente avanzada (APT)

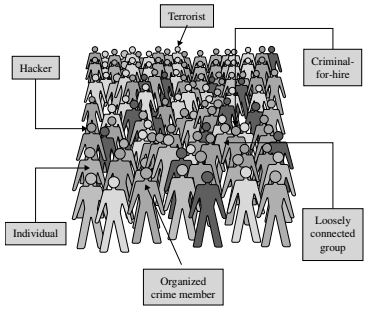
Tipo de ataque en el que se combinan diferentes atributos:

- Organizado
- Dirigido
- Bien financiado
- Paciente
- Silencioso

Población de riesgos

- Aviones de pasajeros
- Bancos
- Distribución energía eléctrica
- Control de tráfico urbano
- Correo electrónico
- Historias clínicas
- TV/radio
- Ascensores
- Trenes
- Registros policíacos
- Organismos estatales
- Organismos de recaudación de impuestos
- Ventas electrónicas
- Control de tráfico aéreo
- Organismos de defensa
- Complejos de defense
- Plantas de energía atómica
- Sistemas de armas

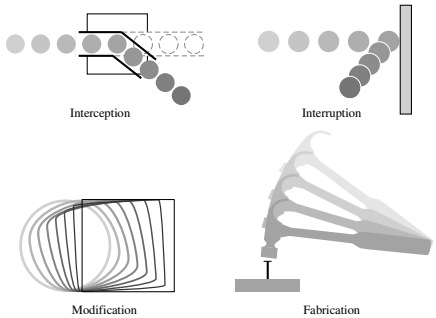
Tipos de atacantes



Flujo normal de la información

Durante un **flujo normal** de la información, la transferencia (de un archivo, región de memoria, etc.) se hace desde la fuente hacia el destino (otro archivo, memoria, etc.).

Tipos de ataques



Tipos de actos que pueden dañar los activos

- **Interceptación**: Entidades no autorizadas logran acceder y visualizar objetos del sistema.
- **Modificación**: Entidades no autorizadas logran efectuar cambios en el sistema.
- **Interrupción**: Afecta a objetos del sistema haciendo que se pierdan, queden inutilizables no disponibles.
- **Fabricación**: Entidades no autorizadas crean objetos en el sistema.

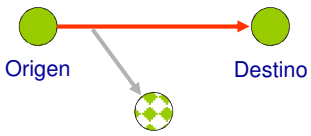
Interrupción

Algo de valor (servicio o característica) en el sistema es destruido o pasa a un estado no disponible.

Ataque a la disponibilidad

Ejemplos: destrucción de hardware, corte de una línea de comunicación, deshabilitación de un sistema de archivos (*umount*).

Intercepción

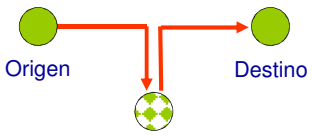


Alguien no autorizado gana acceso sobre algo de valor. El "no autorizado" puede ser una persona, una máquina o un programa.

Ataque a la confidencialidad

Ejemplos: captura de información en una red, una copia no autorizada de archivos.

Modificación

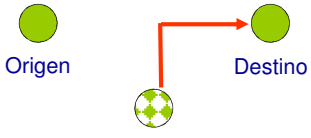


Alguien o algo no solo gana acceso sino que también modifica contenido.

Ataque a la integridad

Ejemplos: cambiar valores en un archivo, alterar un programa para que se comporte diferente, modificar un mensaje transmitido en una red de computadoras.

Fabricación

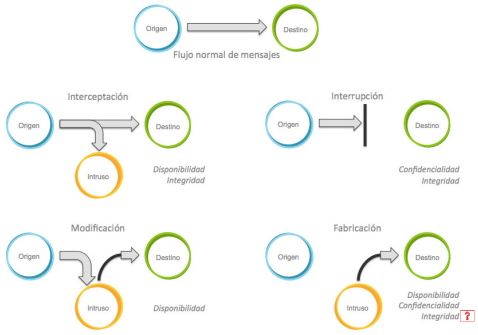


Alguien (o algo) inserta objetos falsos en el sistema.

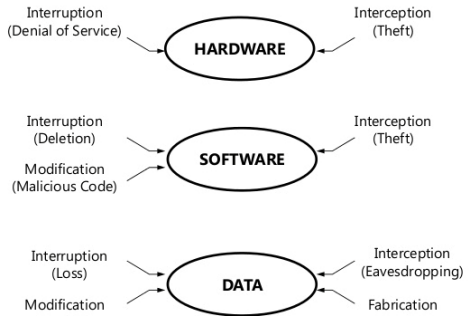
Ataque a la autenticidad (+ integridad)

Ejemplos: inserción de mensajes espurios en una red, inserción de registros falsos en un archivo.

Análisis: propiedades no afectadas por tipo de ataque



Amenazas sobre los sistemas informáticos



Método, oportunidad y motivo

¿Cuándo estamos relamente seguros?

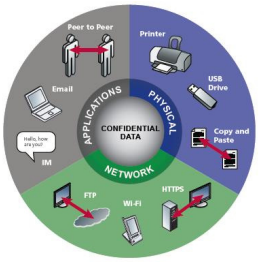
De lo único que podemos estar seguros es que:
que no sabemos todo.

Sobre qué elementos trabajar en seguridad

Elementos asociados:

- Equipamiento
- Sistemas
- Físicos
- Educación

Fuentes de información:



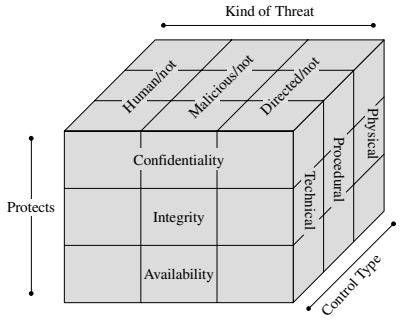
Mecanismos de control/protección

- Mecanismos de control/protección
- Prevención: bloquear el ataque o corregir la vulnerabilidad.
- Desaliento: hacer que el ataque sea difícil pero no imposible.
- Desvío: hacer de que otro objetivo sea más atractivo.
- Mitigación: hacer que el impacto sea lo menos severo posible.
- Detección: detectarlo cuando sucede o poco tiempo después de sucedido.
- Recuperación: de los efectos producidos.

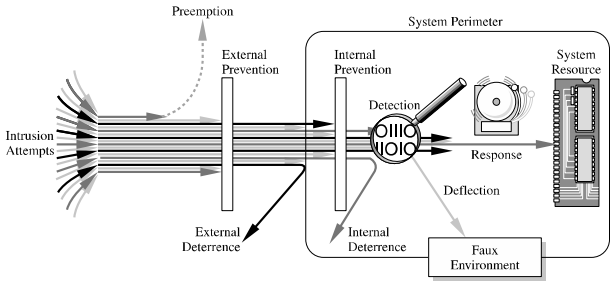
Mecanismos de defensa

- Políticas: definición y control de aplicación.
- Educación.
- Cifrado de datos.
- Controles en el software. (Ejemplo: acceso limitado/restringido, siempre acceso mínimo. Limitar acceso a bases de datos, proteger a un usuario de otro sobre recursos de un sistema).
- Controles del hardware.
- Auditorías.
- Controles físicos.

Control y contramedidas



Tipos de control



Aspectos para alcanzar un nivel de seguridad adecuado

- 30% de la seguridad se logra con educación.
- 30% con políticas, aplicación y supervisión de las mismas.
- 30% con tecnología correctamente aplicada y utilizada.

Resumen

- Las vulnerabilidades son debilidades en un sistema, las amenazas explotan las debilidades.
- Los controles se establecen para protegernos de esas debilidades y su explotación.
- Confidencialidad, integridad y disponibilidad son los **tres aspectos básicos** asociados a la seguridad.
- Existente diferentes tipos de atacantes los cuales plantean diferentes tipos de amenazas según sus capacidades y motivaciones.
- Diferentes controles abordan diferentes amenazas y existen en diferentes puntos de un sistema.