Tema 1.1:Visión Panorámica y Conceptos Básicos

Garantía y Seguridad de la Información.

Tema 1.1: Visión Panorámica y Conceptos Básicos

Introducción

Seguridad de la Información

- **Proceso** para detectar y adoptar todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener:
  - **Confidencialidad** (***C****onfidentiality*)
  - **Integridad** (***I****ntegrity*)
  - **Disponibilidad** (***A****vailability*)

Garantía de la Información

- Es la **confianza** en que los sistemas protejan la información que manejan y funcionen como es necesario que lo hagan, cuando así se precise, bajo el control de sus legítimos usuarios.
  - Una garantía de la información eficaz ha de asegurar unos niveles apropiados de *confidencialidad*, *integridad*, *disponibilidad*, *no repudio* y *autenticidad*.

CBK: Common Body of Knowledge

- International Information System Security Certification Consortium, Inc [$(ISC)^2$], asociación creada en 1988
  - https://www.isc2.org/#
  - $(ISC)^2$ CBK | Common Body of Knowledge
    - *The $(ISC)^2$ CBK is a **collection of topics relevant to cybersecurity professionals around the world**. It establishes a common framework of information security terms and principles.*

- Según CBK, las cualidades clave de la información segura son:

  - **Confidencialidad**: grado de secreto de la información.
    - Sólo quien esté autorizado accederá al activo
  - **Integridad**: cualidad de que la información no ha sido manipulada.
    - El activo no ha sido modificado sin consentimiento
  - **Disponibilidad**: accesibilidad de la información en las condiciones aseguradas por la organización.
    - El activo deberá estar disponible para sus autorizados

Y NOSOTROS … Qué pensamos?

- En grupos de 3 (10 minutos):
  - Nos presentamos …
  - Ponemos en común:
    - ✓ Qué entendemos cuando decimos que algo 'es seguro' …
    - ✓ Qué tiene que ver la seguridad con la protección …
    - ✓ Qué relación puede tener seguridad y garantía …
    - ✓ Qué importancia tienen estas cuestiones en informática …
  - Un interlocutor designado nos traslada a todos quiénes han elaborado qué respuestas.

Conceptos Clave

- Activos (*Assets*)

- Vulnerabilidad
- Amenaza
- Ataque
- Riesgo

- Protección / medidas de seguridad /contramedidas

Activos (Elementos a asegurar): Tipos

- **Activo (Asset):**
  - Todo aquello que posee valor para la organización y puede llegar a ser comprometido o amenazado como consecuencia de vulnerabilidades explotables.
- **Hardware**:
  - errores intermitentes, conexiones sueltas, desconexión de tarjetas, etc.
- **Software**:
  - sustracción de programas, ejecución errónea, modificación, defectos en llamadas al sistema, etc.
- **Datos**:
  - alteración de contenidos, introducción de datos falsos, manipulación fraudulenta de datos, etc.
- **Usuarios**:
  - suplantación de identidad, acceso no autorizado, visualización de datos confidenciales, etc.

Definiciones

- **Vulnerabilidad:**
  - Debilidad (del sistema informático) que puede ser utilizada para causar un daño.
- **Amenaza**
  - Circunstancia que tiene el potencial de causar un daño o una pérdida
- **Riesgo**
  - Posibilidad de que una amenaza se produzca, dando lugar a un ataque que genera un pérdida de valor en uno o varios activos.
- **Ataque**
  - Método por el cual se intenta tomar el control, desestabilizar o dañar otro sistema.

En resumen …

- **Un RIESGO es una pérdida de valor asociada a un fallo de seguridad.**

- **El RIESGO depende de la probabilidad de que se produzca un ATAQUE, materializando una AMENAZA que explota una VULNERABILIDAD del sistema.**

- **La VULNERABILIDAD genera un RIESGO de que una AMENAZA se puede materializar en la realización de un ATAQUE.**

Tema 1.1: Visión Panorámica y Conceptos Básicos

Vulnerabilidades

Vulnerabilidad

- Debilidad de un activo o control que puede ser explotada por una **amenaza**.
- Es una vía de ataque potencial.

- Ejemplos:
  - Defectos en hardware o software
  - Carencia de políticas y procedimientos
  - Otros …

Vulnerabilidades: Registros Internacionales

- National Vulnerability Database (NVD)
  - Repositorio gubernamental de USA con datos para la gestión de vulnerabilidades.
    - *"A weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability. Mitigation of the vulnerabilities in this context typically involves coding changes, but could also include specification changes or even specification deprecations (e.g., removal of affected protocols or functionality in their entirety)."*
- CVE (Mitre Corporation)
  - Sponsored by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA)
- OVAL (Hasta 2015)

- **FIRST (Forum of Incident Response and Security Teams)**
- **ENISA (European Union Agency for CyberSecurity)**
  - Vulnerabilities and Exploits

Vulnerabilidades: Registros Nacionales

- Instituto Nacional de Ciberseguridad (INCIBE)
  - Avisos de seguridad
  - CERTSI (CERT de Seguridad e Industria)
    - CERT Nacional competente en la prevención, mitigación y respuesta ante incidentes cibernéticos en el ámbito de las empresas, los ciudadanos y los operadores de infraestructuras críticas.
    - https://www.incibe-cert.es/alerta-temprana/vulnerabilidades (En castellano, basado en CVE)
  - CERT (Computer Emergency Response Team).
    - Equipo de Respuesta ante Emergencias Informáticas (CERT, del inglés El CERT de Seguridad e Industria (CERTSI)

- Centro Criptológico Nacional (dependiente del Centro Nacional de Inteligencia (CNI)
  - CCN-CERT (Computing Emergency Response Team del CCN)
  - SAT (Sistema de Alerta Temprana)
  - ADA, AMPARO, ANA, CARLA, CARMEN (y no son nombres de mujer …)

Vulnerabilidades. Terminología

- **CVE**: Common Vulnerabilities and Exposures.
  - Código que la identifica de forma univoca.
- **CWE**: Common Weakness Enumeration.
  - Clasificación de las vulnerabilidades.
- **CVSS**: Common Vulnerability Scoring System.
  - Determina las características y los impactos de las vulnerabilidades.
  - Permite priorizar las actividades de corrección de la vulnerabilidad y calcular su severidad.
- **CPE**: Common Platform Enumeration.
  - Esquema de nomenclatura estructurado para sistemas, software y paquetes.
  - Identificar de manera única a los productos vulnerables afectados por una vulnerabilidad dada.

Zero-day vulnerability

- Vulnerabilidad no conocida hasta el momento
  - Son las más temidas porque el tiempo de respuesta de las contramedidas suele ser alto.

- Zero-day attack: explota una vulnerabilidad no conocida hasta el momento.
  - El ataque ocurre en el "día cero" del aviso de la vulnerabilidad.
  - Los desarrolladores han tenido cero días para parchear la vulnerabilidad.

Tema 1.1: Visión Panorámica y Conceptos Básicos

Amenazas

Amenaza (*Threat*)

- Cualquier posibilidad de violación de la seguridad, que existe cuando se da una circunstancia, capacidad, acción o evento que pudiera romper la seguridad y causar perjuicio.
  - Es decir, una amenaza es un peligro potencial asociado a la posibilidad real de sacar partido de una **vulnerabilidad.**

Amenaza (*Threat*)

- REVERSE TROJAN (Server-to-Client)
- TIME BOMB
- BOTS
- KEY LOGGERS
- SNIFFERS
- BACKDOORS
- ROOTKITS
- VIRUS
- WORM
- SPYWARE
- TROJAN HORSE

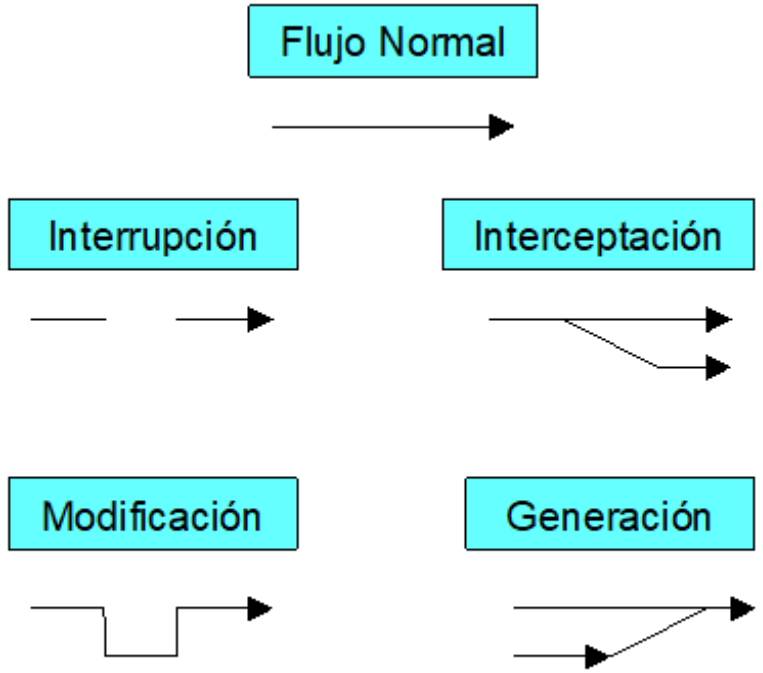
***Open Web Application Security Project* (OWASP)**

Comunidad abierta dedicada a capacitar a las organizaciones para concebir, desarrollar, adquirir, operar y mantener aplicaciones en que se puedan confiar.

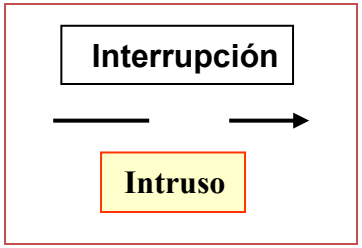
Técnicas para forjar amenazas

- Afectan principalmente al hardware, al software y a los datos.

- Técnicas usadas:
  - Interrupción
  - Interceptación
  - Modificación
  - Generación



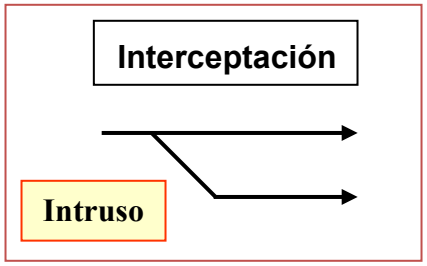
Amenaza/Ataque por Interrupción



- Se daña, pierde o deja de funcionar un punto del sistema.
- Su detección es inmediata.

Ejemplos: Destrucción del hardware.
Borrado de programas, datos.
Fallos en el sistema operativo.

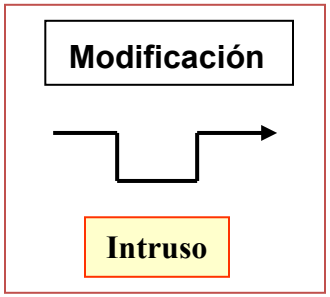
Amenaza/Ataque por Interceptación



- Acceso a la información por parte de personas no autorizadas. Uso de privilegios no adquiridos.
- Su detección es difícil, a veces no deja huellas.

Ejemplos: Copias ilícitas de programas.
Escucha en línea de datos.

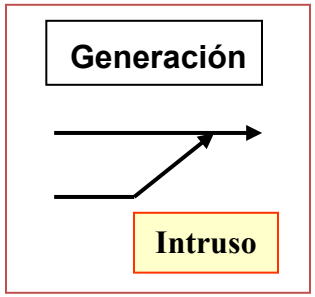
Amenaza/Ataque de Modificación



- Acceso no autorizado que cambia el entorno para su beneficio.
- Su detección es difícil según las circunstancias.

Ejemplos: Modificación de bases de datos.
Modificación de elementos del HW.

Amenaza/Ataque por Fabricación/Generación



- Creación de nuevos objetos dentro del sistema.
- Su detección es difícil: delitos de falsificación.

Ejemplos: Añadir transacciones en red.
Añadir registros en base de datos.

Tema 1.1: Visión Panorámica y Conceptos Básicos

Ataques

Ataque (*Attack*)

- Un asalto inteligente y fabricado a la seguridad del sistema, derivado de una o varias **amenazas**
  - acto consciente y deliberado para eludir los servicios de seguridad y violar la política de seguridad de un sistema.
- Cualquier **acción** que comprometa la seguridad de la información de una organización

Ataques (*Attack*)

- Brute Force: Fuerza Bruta
- Cache Poisoning: Envenenamiento de Caché
- DNS Poisoning: Envenenamiento de DNS
- Cross-Site Request Forgery (CSRF) o Falsificación de petición en sitios cruzados
- Cross-Site Scripting (XSS) o Secuencias de comandos en sitios cruzados
- Denial of Service (DoS)
- LDAP injection
- Man-in-the-middle
- Session hijacking attack
- SQL Injection: Inyección SQL

Open Web Application Security Project (OWASP)

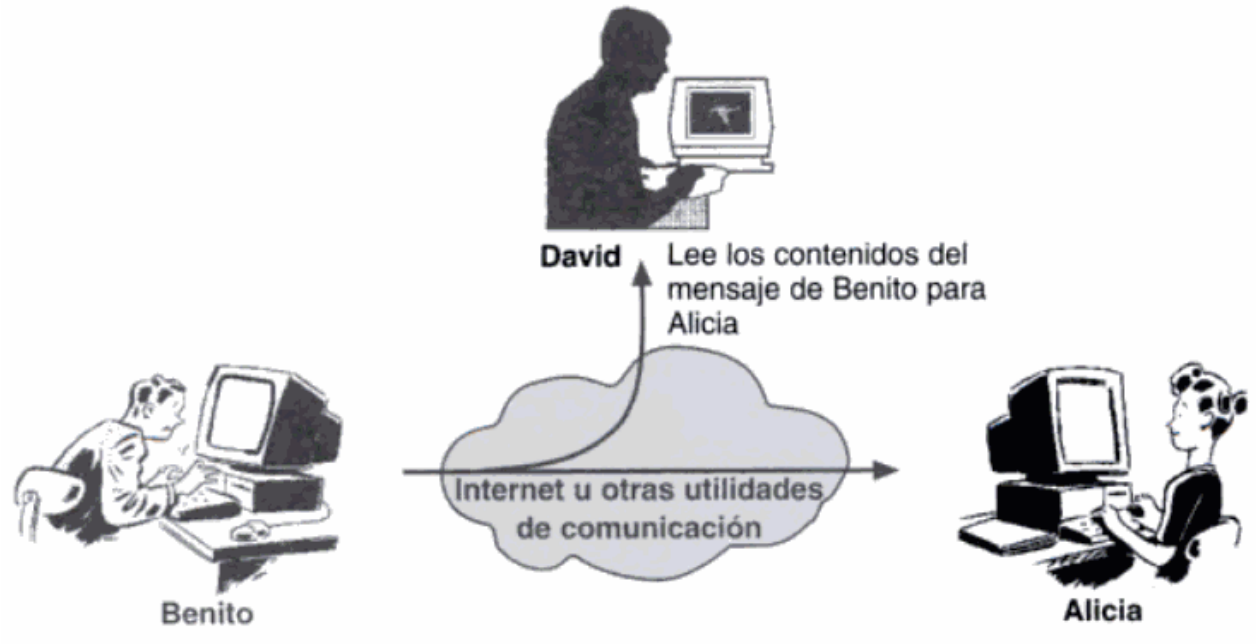
Tipos de ataques

- Pasivos
  - Intenta conocer o hacer uso de información del sistema, pero no afecta a los recursos del mismo
  - Se dan en forma de **escucha** o de observación no autorizada de las transmisiones. El objetivo del oponente es obtener información que se esté transmitiendo
  - Muy **difíciles de detectar**, ya que no implican alteraciones en los datos
  - Contra estos ataques se debe poner más énfasis en la **prevención** que en la detección.

- Posible solución: **cifrado**

Ataques pasivos

- Obtención del contenido del mensaje



Ataques pasivos

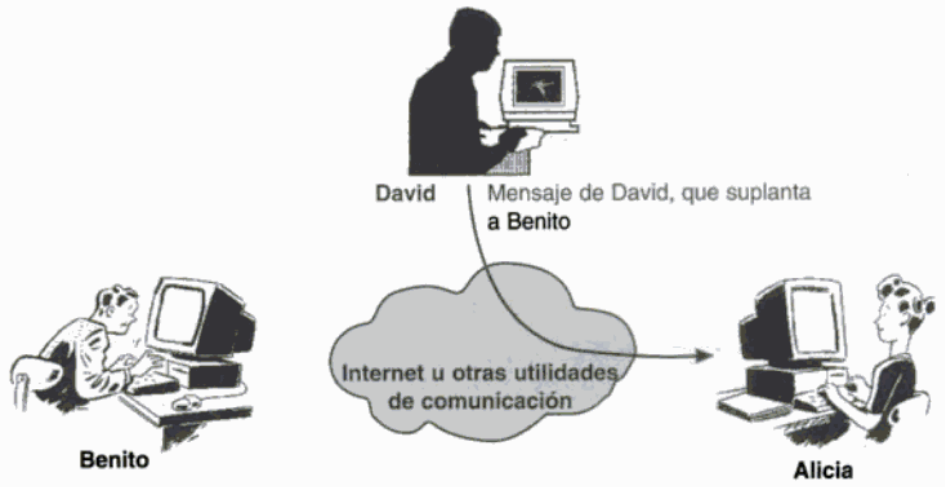
- Análisis del tráfico
  - Aún con protección mediante cifrado, un oponente puede observar el patrón de los mensajes, determinar la **localización** y la **identidad** de los servidores que se comunican y descubrir la **frecuencia** y la **longitud** de los mensajes que se están intercambiando.
  - Esta información puede ser útil para averiguar la naturaleza de la comunicación que está teniendo lugar.

Ataques activos

- Intentan alterar los recursos del sistema o afectar a su funcionamiento
- Implican alguna modificación del flujo de datos o la creación de un flujo falso
- Presentan características opuestas a los pasivos:
  - Son difíciles de prevenir por completo
  - El objetivo es **detectarlos** y recuperarse de ellos
    - La detección tiene efecto disuasivo -> contribuye a la prevención
- Se pueden dividir en cuatro categorías:
  - Suplantación de identidad
  - Repetición / retransmisión
  - Modificación
  - Interrupción del servicio

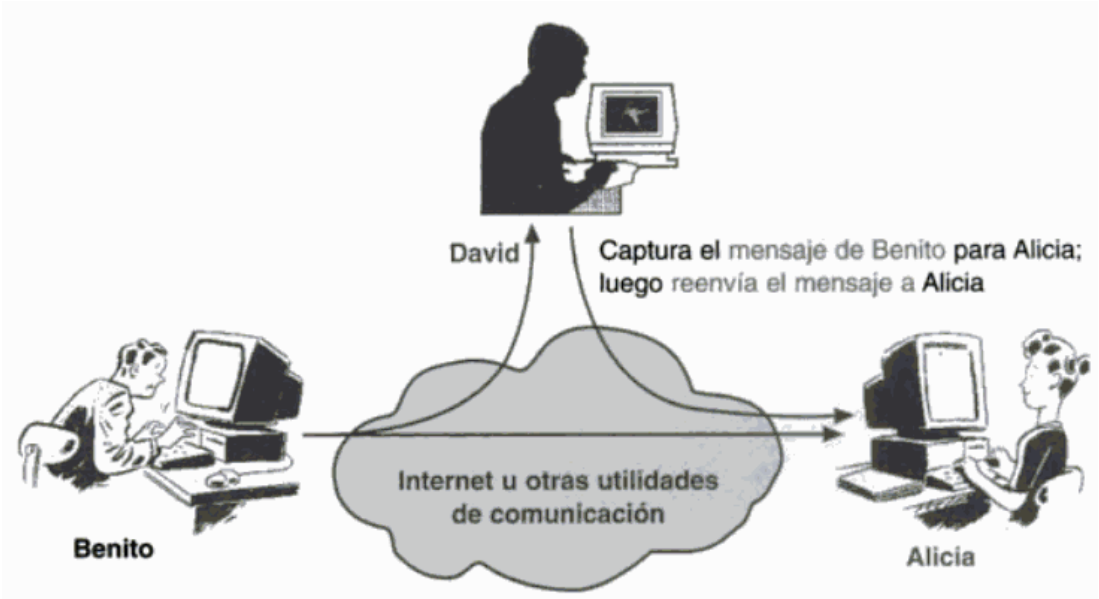
Ataques activos

- Suplantación de identidad
  - Se produce cuando una entidad finge ser otra
  - Un ataque de este tipo incluye habitualmente una de las otras formas de ataque activo.
- Por ejemplo, las secuencias de autenticación pueden ser capturadas y repetidas después de que una secuencia válida haya tenido lugar



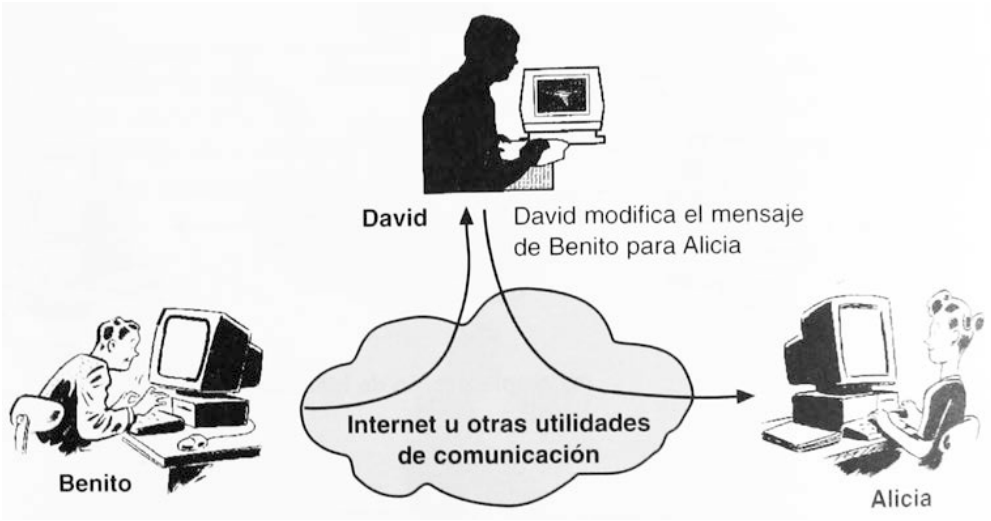
Ataques activos

- Repetición / Retransmisión
  - Implica la captura pasiva de una unidad de datos y su retransmisión posterior para producir un efecto no autorizado



Ataques activos

- Modificación de mensajes
  - Una parte de un mensaje es alterada, o los mensajes se han retrasado o reordenado, para producir un efecto no autorizado



Ataques activos

- Interrupción del servicio
  - Impide el uso o la gestión normal de las utilidades de comunicación

Tipos de ataques: otra clasificación

- Ataques sobre la **identidad** de las entidades:
  - Interceptación
  - Suplantación
- Ataques sobre la **información**:
  - Revelación
  - Reenvío
  - Manipulación
  - Repudio
- Ataques sobre los **servicios**:
  - Denegación del servicio

Tema 1.1: Visión Panorámica y Conceptos Básicos

Protección

Medidas de Seguridad (MS)

- Objetivo: SEGURIDAD
  - Para minimizar **riesgos** y evitar el mayor número de **ataques** posible, debemos conocer en profundidad las **vulnerabilidades** de nuestro sistema y las **amenazas** que puedan afectarle.

- Así, plantearemos MEDIDAS DE SEGURIDAD adecuadas
  - Disuasión
  - Detección
  - Defensa

Tipos de MS: Disuasión

- Disuasión:
  - PRINCIPIO:
    - **Disminuir la probabilidad de exposición a los ataques.**
  - Los atacantes deberán buscar otras alternativas de mayor complejidad para buscar zonas de riesgo.
    - Amenaza de una persecución legal, la presencia de cámaras o sistemas de monitorización.
    - Dificultades añadidas para el acceso ilegal (mensajes de correo a los empleados, registro de lugares de internet visitados, registro de accesos externos y horas de conexión, etc.).

Tipos de MS: Detección

- Detección:
  - PRINCIPIO:
    - **Disminuir el tiempo de respuesta ante un ataque.**
  - Facilitar actuación inmediata en situación de riesgo:
    - Minimizar el daño en caso ataque
    - Desencadenar mecanismos y procesos encargados de hacer cumplir las directivas de seguridad y recuperar la estabilidad del sistema.
    - Auditoría, análisis de logs, sistemas de detección de intrusión, resúmenes e informes de actividad, etc.

Tipos de MS: Defensa

- Defensa:
  - PRINCIPIO:
    - **Salvaguardar / proteger los activos de interés.**
  - Medidas activas o pasivas de protección ante atacantes
    - Reducen las posibilidades de ataques y disminuyen el riesgo de daños.
    - La carencia de medidas defensivas deja expuesta información sensible y es una fuente de problemas.
    - Uso de firewalls, access lists en routers, spam filters, virus filters, etc.

Tema 1.1: Visión Panorámica y Conceptos Básicos

Bibliografía a revisar

Bibliografía

- Ver Lecturas recomendadas en Campus Virtual:
  - Capítulo 1 de Pfleeger, Whitman, Anderson, Jacobs
  - Algunas webs importantes
  - Esquema Nacional de Seguridad