Seguridad de la Información

1er cuat. 2024

Lic. Rodolfo Baader
rbaader@dc.uba.ar

Información útil

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Clases teórico-prácticas

Lunes de 18:00 a 20:30

Miércoles de 18:00 a 20:30

Aula 1115

Correlativa:

Teoría de las comunicaciones

Material:

https://campus.exactas.uba.ar

Lista de correo: seginfdcubaar@googlegroups.com

Evaluación:

1 Parcial. 1 TP con presentación. Materia promocionable, sin final.

Objetivos

- **Establecer un conjunto de definiciones básicas de la Seguridad Informática, brindar un panorama evolutivo de la misma y mencionar las perspectivas futuras.**

- **Introducir al uso de Políticas de Seguridad.**

- **Analizar métodos para proteger física y lógicamente la información almacenada o en tránsito en los sistemas de computación.**

Fechas Importantes (tentativas)

Laboratorio Seguridad web
20 de mayo

Laboratorio pen-test
22 de mayo

Parcial
10 de junio

Presentación TP
3 de julio

Entrega final TP
14 de julio

Temario

Unidad 1 – Introducción

- Definiciones.
- Conceptos generales.
- Propiedades de la información.

Temario

Unidad 2 – Control de acceso

- Matriz de control de acceso.
- Control de acceso mandatorio , discrecional y por roles.
- Modelo Bell-LaPadula. Pared china.

Temario

Unidad 3 - Criptografía

- Fundamentos .
- Esquemas simétricos y asimétricos.
- Manejo de claves.
- FIPS.
- PKI.

Temario

Unidad 4 - Autenticación

- Mecanismos de autenticación y autorización.
- Passwords, tokens y biometría.
- Política de menor privilegio.

Temario

Unidad 5 – Seguridad en redes

- Topologías de redes.
- Firewalls y proxies.
- DMZ.
- Túneles.
- Sistemas de detección de intrusiones (NIDS).
- Ataques a TCP/IP.

Temario

Unidad 6 - Seguridad en servidores y aplicaciones

- Código malicioso.
- Buffer overflows y otros tipos de ataques.
- Desarrollo seguro. Procesos.
- Seguridad en aplicaciones web
- Entornos protegidos (sandboxes, chroot, jails, contenedores).
- SELinux
- Instalación segura

Temario

Unidad 7 – Prevención y análisis forense

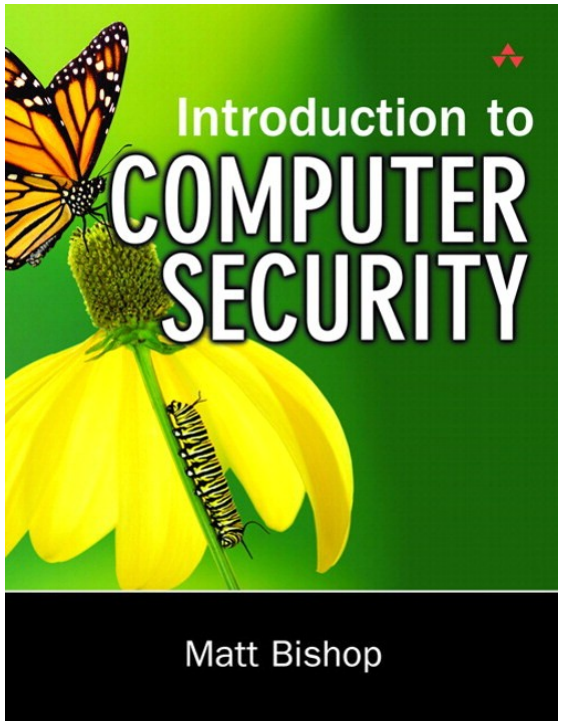
- Análisis de vulnerabilidades.
- Pen-Test.
- Detección de intrusos.
- Recolección y preservación de evidencia
- Análisis forense.

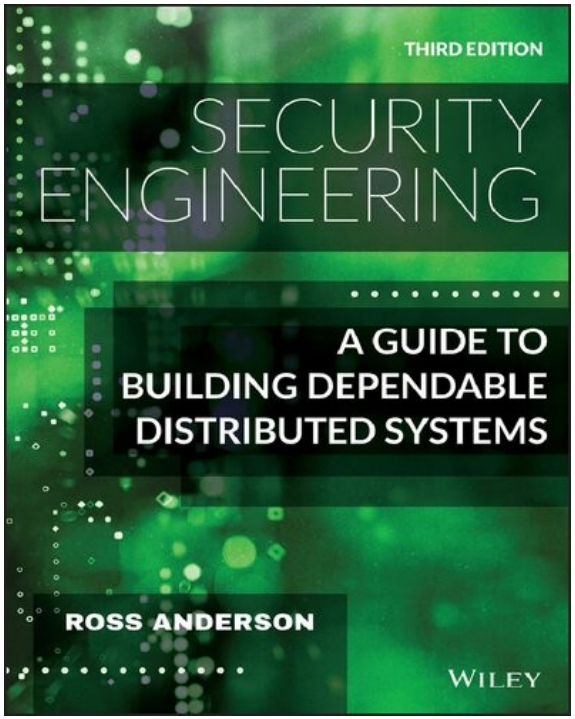
Temario

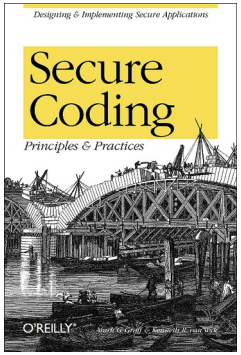
Unidad 8 – Evaluación y gestión de seguridad

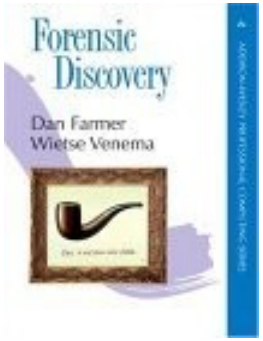
- TCSEC / Common Criteria
- ISO 27001
- CVSS
- Auditoría
- Análisis de riesgos

Bibliografía









Casos Reales

- **Se mostrarán en la mayoría de las clases noticias relacionadas con la temática de la materia.**

- **Incluyen análisis de noticias relevantes, tanto nacionales como internacionales, explicación de ataques, información erronea publicada en los medios, etc.**

https://notasdeseginf.blogspot.com/

Unidad 1: Introducción

- **Información :**

  Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Conceptos generales

- **Información**
  - Documentos, informes, archivos, …
  - Comunicaciones
  - Sistemas
  - Datos personales, claves, …
  - Cualquier dato relevante

Seguridad de la información

La seguridad de la información se entiende como la preservación de las siguientes características:

- Confidencialidad
- Integridad
- Disponibilidad

Confidencialidad

Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Ej: Cifrar una declaración de impuestos no permitirá que nadie la lea. Si el dueño necesita verla, debe descifrarla con la clave que sólo él conoce. Si alguien logra obtener la clave de cifrado, la confidencialidad de la declaración de impuestos ha sido comprometida.

Integridad

Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento. La integridad incluye la integridad de los datos (el contenido) y el origen de los mismos.

Ej: Un periódico puede dar información obtenida de la casa rosada pero atribuirla a una fuente incorrecta. Es un ejemplo de integridad de la información, pero con integridad de origen corrupta.

Disponibilidad

Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Ej: Es el último día de inscripciones en la facultad y se produce un corte de energía eléctrica que dura todo el día. Las UPS funcionan durante 2 horas y luego apagan los servidores. Resultado: Los alumnos rezagados no pueden inscribirse a las materias.

Vulnerabilidades, amenazas, etc.

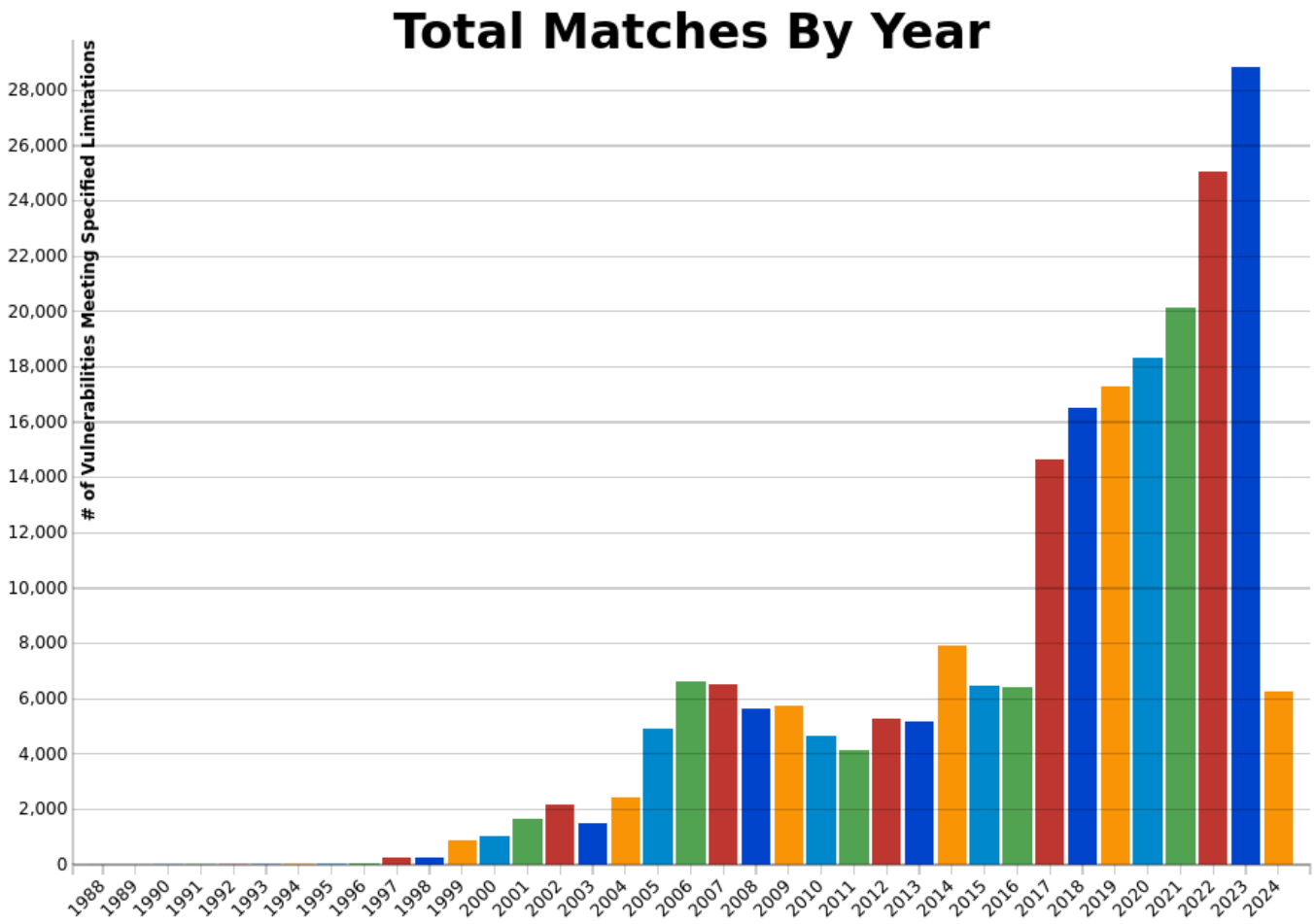
- Una **vulnerabilidad** es una debilidad en un activo.

- Una **amenaza** es una violación potencial de la seguridad. No es necesario que la violación ocurra para que la amenaza exista. Las amenazas "**explotan**" vulnerabilidades.

- Hay que protegerse o estar preparado para las acciones que podrían causar dicha violación.

- Dichas acciones son llamadas **ataques**. Los que ejecutan las acciones, o producen la ejecución de las mismas, son llamados **atacantes o intrusos**.

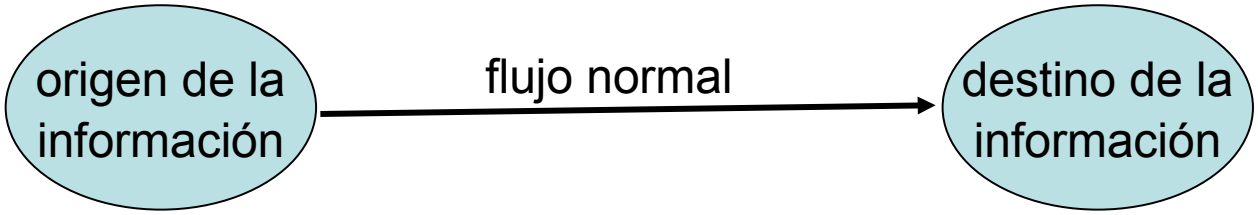
Vulnerabilidades – algunos números



Fuente: https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&search_type=all&isCpeNameSearch=false

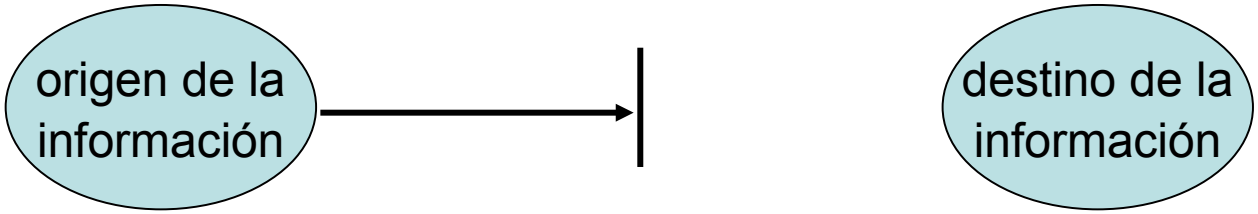
Tipos de amenazas

- **Flujo normal de información**



Tipos de amenazas

- **Interrupción del flujo de información**

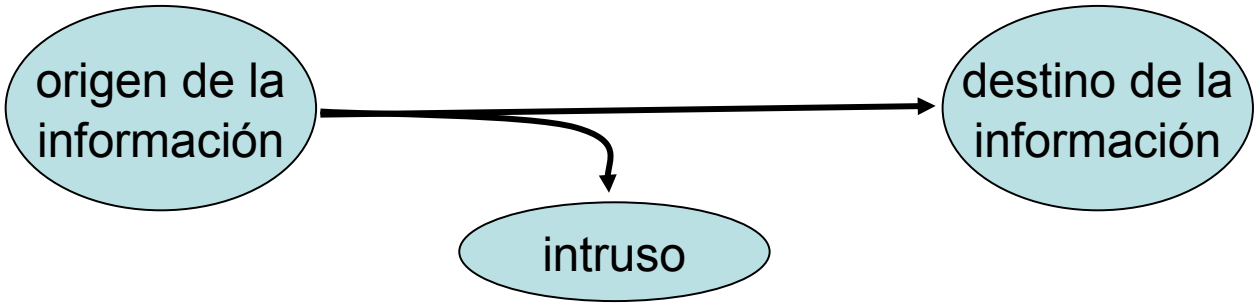


  - Destrucción del recurso
  - Bloqueo del recurso
  - Saturación del recurso

- **Amenaza a la *disponibilidad* de la información**

Tipos de amenazas

- **Intercepción de información**

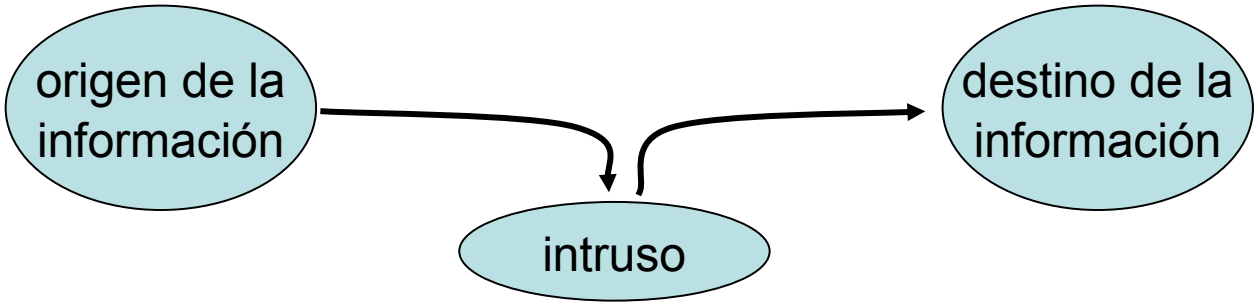


  - Acceso no autorizado al recurso
  - Monitoreo de información
  - Ingeniería social

- **Amenaza a la *confidencialidad* de la información**

Tipos de amenazas

- **Alteración de información**

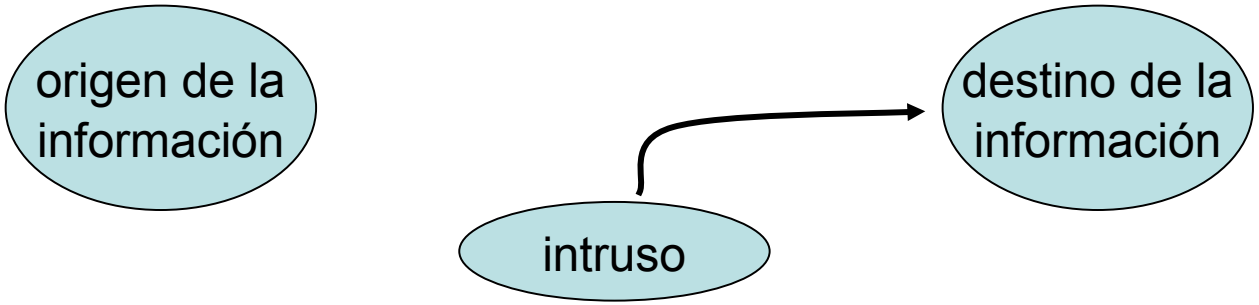


  – Modificación del recurso

- **Amenaza a la *integridad* de la información**

Tipos de amenazas

- **Fabricación de información**



  - Incorporación de información
  - Envío de mensajes falsos (*phishing*)

- **Amenaza a la *autenticidad* de la información**

Tipos de amenazas

- **Amenazas Pasivas**
  - No se interfiere con los sistemas
  - Son difíciles de detectar
  - Dependen del medio físico de transmisión

  - Monitoreo de datos (*sniffing*)
  - Análisis de actividad (*side channel attack*)

Tipos de amenazas

- **Amenazas Activas**
  - Captura de información (*keylogger)*
  - Suplantación de identidad
  - Retransmisión de mensajes
  - Falsificación de datos (*tampering*)
  - Escaneo de puertos (*port scanning*)
  - Aprovechamiento de software vulnerable (*exploit*)
  - Intercepción (*man in the middle*)
  - Denegación de servicios (*DOS*)
  - …

Tipos de amenazas

- **Origen de las amenazas**
  - Intencionales / Accidentales
  - Externas / Internas

Políticas y mecanismos

- Una **política de seguridad** es una declaración de lo que está permitido y lo que no.
- Un **mecanismo de seguridad** es un método, herramienta o procedimiento para hacer cumplir una política de seguridad.
- Los mecanismos pueden ser no técnicos. Ej: Requerir libreta universitaria antes de cambiarle la clave a un alumno.
- En general, las políticas necesitan algunos procedimientos que la tecnología no puede hacer cumplir.

Objetivos de la Seguridad

- **Prevención:** Significa que el ataque fallará. Por ejemplo, si uno intenta entrar a un sistema a través de Internet, pero el mismo no esta conectado a dicha red, el ataque fue prevenido.

- **Detección:** Puede ser usado cuando un ataque no puede ser prevenido, o para medir la efectividad de los mecanismos de prevención. Los mecanismos de detección dan por hecho que un ataque va a ocurrir, y su objetivo es reportar los ataques que se produzcan.

- **Recuperación:** Luego de producido un ataque, se procede a detenerlo. Se debe determinar y reparar daños. Volver a operar correctamente. Ej: Si un atacante borrá un archivo, se puede recuperar el mismo de los back-ups.

Cuestiones Operacionales

- Cualquier política y mecanismo útil deben balancear los beneficios de la protección con el costo del diseño, implementación y utilización del mecanismo.

- Este balance puede ser determinado analizando los riesgos y la probabilidad de ocurrencia.

Ej: Una base de datos provee la información de salario de los empleados de una empresa, y es utilizada para imprimir los cheques. Si dicha información es alterada, la compañia puede sufrir graves perdidas financieras. Por eso, es claro que se deben utilizar mecanismos que permitan garantizar la integridad de la información. Sin embargo, si tenemos un segundo sistema que copia diariamente dicha base de datos a cada filial, para que tenga valores de referencia a la hora de contratar nuevo personal (la decisión es de la casa central), la necesidad de mantener la integridad en cada filial no es tan alta.

Leyes

- **Las leyes restringen la disponibilidad y el uso de la tecnología y afectan los controles y procedimientos.**

- **Ej:**
  - Restricciones a la exportación de software criptográfico en EEUU, año 2000.
  - Ley 25.506 de Firma Digital.
  - Ley 25.326 Protección de Datos Personales
  - Ley 26.338 Délito Informático
  - Ley 27.411 Convenio de ciberdelito (Budapest)
  - Ley 27.699 Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal

- **Toda política y sus mecanismos asociados deben tener en cuenta consideraciones legales.**

Evaluación de riesgos

- Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria de la organización.

Cuestiones Humanas

- Es complejo implementar controles de seguridad informática, y en una organización grande los controles pueden volverse vagos o incómodos.

- Si se los configura en forma inadecuada o se los usa incorrectamente, hasta los mejores controles de seguridad se vuelven inútiles y hasta en algunos casos peligrosos.

Cuestiones Humanas

- Personal no entrenado puede ser una amenaza para la seguridad de un sistema. Ej: Un operador que no sabe que debe verificar el contenido de los backups antes de almacenarlos.

- El entrenamiento necesario no solamente es técnico. Muchos ataques exitosos provienen del uso de la **Ingeniería Social**. Si los operadores cambian las claves de acceso a través de pedidos telefónicos, todo lo que un atacante necesita es saber el nombre de uno de los usuarios del sistema y hacer un llamado.