TEMA-1.-Ciberseguridad.pdf

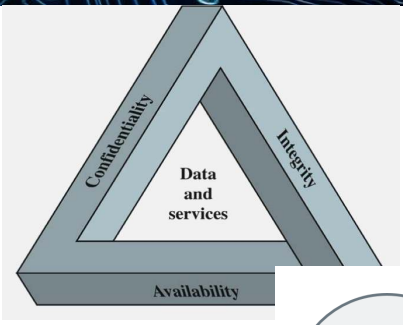
_GxIIsi7

Redes y Seguridad I

3º Grado en Ingeniería Informática

Facultad de Informática
Universidad Complutense de Madrid

TEMA 1. Ciberseguridad



PROBABILIDAD	IMPACTO		
	Bajo	Medio	Alto
Baja	Muy bajo	Bajo	Medio
Media	Bajo	Medio	Alto
Alta	Medio	Alto	Muy alto

ÍNDICE

1/6

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

ING BANK NV se encuentra adherido al Sistema de Garantía de Depósitos Holandés con una garantía de hasta 100.000 euros por depositante. Consulta más información en ing.es

Que te den **10 € para gastar** es una fantasía. ING lo hace realidad.

Abre la **Cuenta NoCuenta** con el código **WUOLAH10**, haz tu primer pago y llévate 10 €.

Quiero el cash

Consulta condiciones **aquí**

do your thing

Redes y Seguridad I

Banco de apuntes de la

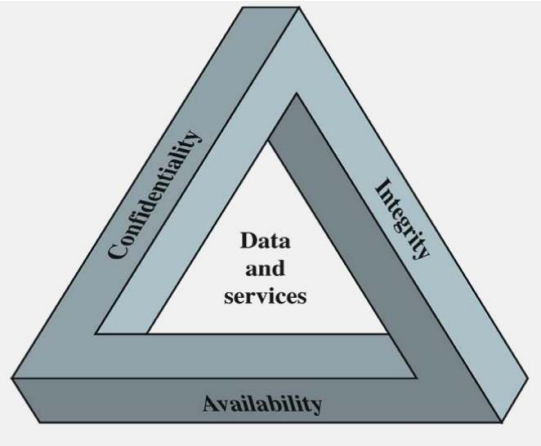
WUOLAH

Comparte estos flyers en tu clase y consigue más dinero y recompensas

1. Imprime esta hoja
2. Recorta por la mitad
3. Coloca en un lugar visible para que tus compis puedan escanar y acceder a apuntes
4. Llévate dinero por cada descarga de los documentos descargados a través de tu QR

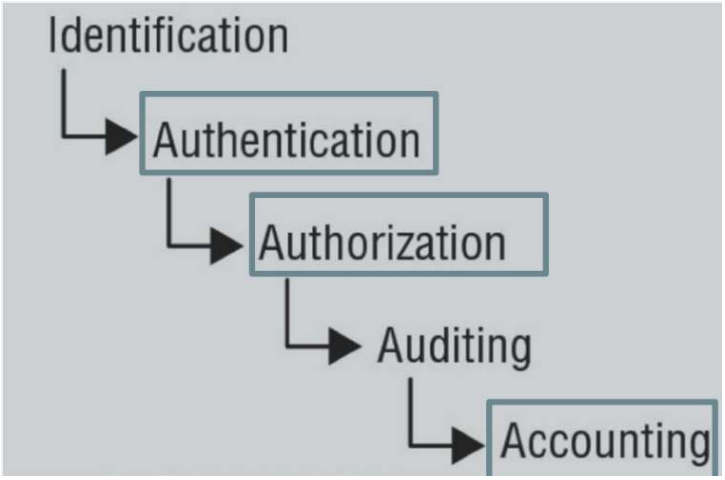
Introducción a la seguridad

Tríada CIA



- **Confidencialidad:** Asegurar que no se producen accesos no autorizados a datos, objetos y recursos.
- **Integridad:** Garantizar la fiabilidad y corrección de los datos almacenados, procesados y/o transmitidos.
- **Disponibilidad:** Garantizar que un sistema trabaja sin demora y que el servicio no es negado a los usuarios autorizados.

Servicios AAA



- **Identificación:** Indicar quién eres (usuario, origen…).
- **Autenticación:** Probar quién eres (soy ese usuario, origen…).
- **Autorización:** Permiso para acceder a los recursos.
- **Auditoría:** Guardar registro de lo que ha sucedido.
- **Responsabilidad:** Asegurar que las acciones de una entidad son atribuidas de manera única a esa entidad.

No repudio

Un sujeto o entidad no puede negar que ha realizado una determinada acción.

Definiciones

- **Confidencialidad de datos:** Garantizar que la información privada o confidencial no es revelada a individuos no autorizados. Los datos deben estar protegidos contra el acceso, uso o divulgación no autorizados durante el almacenamiento, el procesamiento y la transmisión.
- **Privacidad:** Garantiza que los individuos controlan qué información personal puede ser recolectada y almacenada y por quién y a quién puede ser revelada.
- **Datos sensibles:** Aquellos cuya divulgación puede causar daño.

- **Seguridad de la información o Ciberseguridad:** Conjunto de actuaciones orientadas a asegurar, en la medida de lo posible, las redes y sistemas que constituyen el ciberespacio y la información, tanto almacenada como transmitida.
- **Ciberespacio:** El espacio virtual que engloba todos los sistemas TIC que están enlazados a nivel de datos en una escala global.

- **Activo:** Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización (información, datos, servicios, aplicaciones…).
- **Amenaza:** Posiblidad de violación de la seguridad del sistema, debido a que exista una entidad, circustancia, capacidad, acción o evento que pueda causar daño. Pueden ser accidentales (por error humano u omisión, mal funcionamiento de un equipo o desastre natural) o inteligentes (por entidad inteligente: cracker individual u organización criminal).
- **Vulnerabilidad:** Defecto o debilidad de un sistema informático en su diseño, implementación o en su operación y gestión que puede ser utilizada para violar la política de seguridad del sistema y causar daño.
- **Riesgo:** Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando un impacto en la organización.

- **Incidente:** Cualquier evento que no sea parte de la operación estándar de un servicio que ocasione, o pueda ocasionar, una interrupción o una reducción de la calidad de ese servicio.
- **Incidente de Seguridad:** Evento singular o serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información.
- **Black hat:** Alguien que rompe la seguridad, normalmente por razones maliciosas o beneficio personal (Cracker o cibercriminal).
- **White hat:** Especialista de seguridad con autorización que realiza pruebas de intrusión (Hacker ético).
- **Grey hat:** combinación de Black hat y White hat.
- **Script kiddie (skiddie):** no experto que usa herramientas automáticas escritas por otros con poco entendimiento.
- **Hacktivista:** Hacking para anunciar un mensaje social, ideológico, religioso o político.

Anatomía de un ataque

Tipos de ataque

- **Según la intención:**
  - **Pasivo:** el atacante intenta aprender o usar información del sistema pero no afecta a los recursos del sistema. Ejemplos: captura de paquetes (sniffing) o análisis de tráfico.
  - **Activo:** el atacante intenta alterar los recursos del sistema o afectar a su funcionamiento. Ejemplos: suplantación, repetición, modificación o denegación de servicios.
- **Según el punto de iniciación:**
  - **Interno:** iniciado por una entidad dentro del perímetro de seguridad (insider).
  - **Externo:** iniciado desde fuera del perímetro de seguridad por un usuario no autorizado (outsider).
- **Según el modo de direccionamiento (red):**
  - **Directo:** el atacante envía paquetes a la víctima.
  - **Indirecto:** el atacante envía paquetes a una tercera parte (reflector), que responde enviando paquetes a la víctima.

Ataques comunes

- Reconocimiento: Sniffing, footprinting, fingerprinting…
- Acceso: Man-in-the-middle, session hijacking, code injection…
- Denegación de servicio (DoS): Flooding, amplification/reflection…
- Software malicioso (malware): Virus, worms, Trojan horses, back doors…

Anatomía de un ataque

- **Reconocimiento (reconoissance, footprinting):**
  - Búsqueda en Internet y DNS.
  - Ingeniería social.
- **Exploración (scanning, fingerprinting):**
  - Exploración de redes y puertos.
  - Identificación de servicios y análisis de vulnerabilidades.
- **Obtención de acceso**
  - Explotación de vulnerabilidades y escalado de privilegios.
- **Mantenimiento del acceso**
  - Descifrado de contraseñas, rootkits y puertas traseras.
  - Movimientos laterales.
- **Ocultación de pistas**
  - Desactivado de auditoría y borrado de registros.
  - Corrupción de datos.

Tipos de Ciberataques

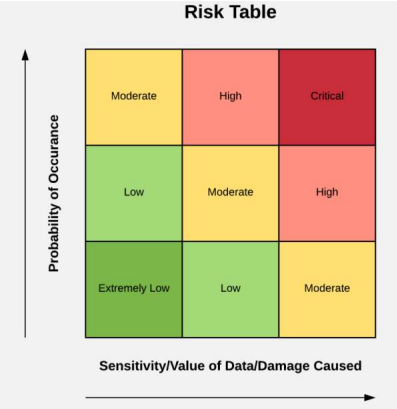
Ataque de DDoS, Phishing, Backdoor, Man in the middle, SQL Injection, Ransomware…

Aspectos de la seguridad que se comprometen en un ataque

- **Confidencialidad:** Un atacante podría robar información sensible como contraseñas u otro tipo de datos si viajan en texto claro a través de redes.
- **Integridad:** Mientras la información se transmite, un atacante podría interceptar el mensaje y realizar cambios en determinados bits del texto cifrado con la intención de alterar los datos del criptograma.
- **Disponibilidad:** Podría utilizar los recursos de la organización, como el ancho de banda de la conexión DSL para inundar de mensajes el sistema víctima y forzar la caída del mismo.

Prevención de ataques

Para prevenir un ataque es necesario: Hacer un análisis de riesgos y tener implementados mecanismos y servicios de seguridad.



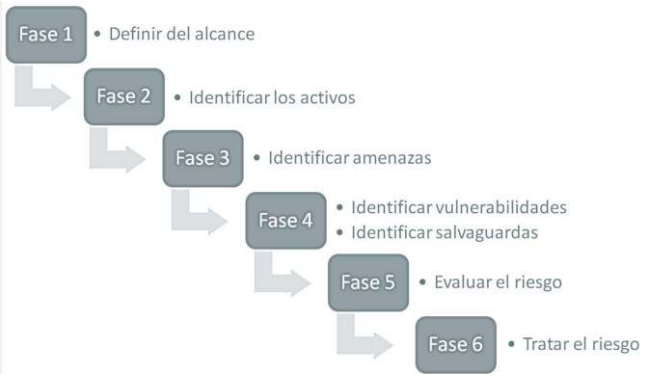
Gestión de la seguridad

Una empresa u organismo público tiene que proteger: Sus datos, los de sus clientes, sus transacciones, su página web, sus servidores, sus instalaciones, etc. Necesita saber cómo priorizar las decisiones para garantizar la confidencialidad, integridad y disponibilidad de la información (Tríada CIA). Para lo que es importante:

- Realizar una evaluación de riesgos.
- Tener servicios y mecanismos de seguridad implementados.
- Tener un plan de recuperación ante un incidente.

Uno de los aspectos más importantes es la **gestión de riesgos**.

El Plan Director de Seguridad (PDS) es la **definición y priorización** de un conjunto de proyectos en materia de **seguridad de la información**, dirigido a **reducir los riesgos** a los que está expuesta una organización hasta unos **niveles aceptables**.



1. **Definir el alcance** del estudio.
2. **Identificar los activos** más importantes que guardan relación con el departamento, proceso, o sistema objeto del estudio.
3. **Identificar las amenazas** a las que estos están expuestos los principales activos.
4. **Identificar vulnerabilidades y salvaguardas**: La siguiente fase consiste en estudiar las características de nuestros activos para identificar puntos débiles o vulnerabilidades Analizar y documentar las medidas de seguridad implantadas en la organización (salvaguardas).
5. **Evaluar el riesgo**: Para cada par activo-amenaza, estimaremos la probabilidad de que la amenaza se materialice y el impacto sobre el negocio que esto produciría.

6. **Tratar el riesgo:**
    a. Transferir.
    b. Eliminar.
    c. Asumir.
    d. Mitigar.