PRINCIPIOS DE SEGURIDAD

Y ALTA DISPONIBILIDAD

SEGURIDAD Y ALTA DISPONIBILIDAD

1. INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA
2. FIABILIDAD, CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD
3. ELEMENTOS VULNERABLES EN EL SISTEMA INFORMÁTICO: HARDWARE, SOFTWARE Y DATOS
4. AMENAZAS
5. PROTECCIÓN

SEGURIDAD Y ALTA DISPONIBILIDAD

1. INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

Hoy en día un sistema informático totalmente seguro es imposible, la conectividad global, extiende el campo de posibles amenazas.

La seguridad informática: asegurar que los recursos del sistema de información sean utilizados de la manera que se decidió y que el acceso y modificación a la información, solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

SEGURIDAD Y ALTA DISPONIBILIDAD

Objetivos de la seguridad informática:

- ✓Detectar los posibles problemas y amenazas.
- ✓Garantizar la adecuada utilización de los recursos y de las aplicaciones de los sistemas.
- ✓Limitar las pérdidas y conseguir una adecuada recuperación en caso de un incidente.
- ✓Cumplir con el marco legal y con los requisitos impuestos a nivel organizativo.

SEGURIDAD Y ALTA DISPONIBILIDAD

2. FIABILIDAD, CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

- La seguridad absoluta no es posible.
- Seguridad informática: técnicas para obtener **altos niveles de seguridad** → **FIABILIDAD**.

Se suaviza la definición de **seguridad** y se pasa a hablar de **fiabilidad:** probabilidad de que un sistema se comporte tal y como se espera de él.

SEGURIDAD Y ALTA DISPONIBILIDAD

El experto Eugene H. Spafford cita en su frase célebre: "*el único sistema que es totalmente seguro es aquel que se encuentre apagado y desconectado, guardado en una caja fuerte de titanio que está enterrada en cemento, rodeada de gas nervioso y de un grupo de guardias fuertemente armados. Aún así, no apostaría mi vida en ello*".

Sistema seguro (o fiable), garantizar **CIDAN**: Confidencialidad, Integridad y Disponibilidad + Autenticación y No Repudio.

SEGURIDAD Y ALTA DISPONIBILIDAD

- **Confidencialidad**: privacidad o protección de información o comunicación.

- **Integridad**: comprobar que no ha sido alterada cierta información o comunicación.

- **Disponibilidad**: capacidad de un servicio, datos o sistema, a ser accesible y utilizable por los usuarios (o procesos) autorizados cuando estos lo quieran.

SEGURIDAD Y ALTA DISPONIBILIDAD

- **Autenticación**: verificación de la identidad de un usuario. Aporta algún modo que permita verificar que es quien dice ser (credencial: usuario o *login* + contraseña o *password)*.

- **No repudio o irrenunciabilidad** : permite probar la participación de las partes en una comunicación.

Existen dos posibilidades:

✓*No repudio en origen* : el emisor no puede negar el envío. La prueba la crea el propio emisor y la recibe el destinatario.

✓*No repudio en destino* : el receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción. En este caso la prueba irrefutable la crea el receptor y la recibe el emisor.

Práctica 1

CONFIDENCIALIDAD

EFS (Encrypted File System). Cifrado de archivos en sistema operativo Windows.

Permite a los archivos ser cifrados en las particiones NTFS en donde esté habilitado, para proteger datos confidenciales.

Práctica 2

INTEGRIDAD

Comprobación de integridad, no falsificación o modificación, de archivos del sistema (anti-rootkit).

En Windows (**SFC**) y GNU/Linux (**Rootkit Hunter**)

SFC(System File Checker): es una utilidad de los sistemas Windows que comprueba la integridad de los archivos de sistema y reemplaza los que están corruptos o dañados por versiones correctas, si es posible. Cuando se ejecuta SFC, crea un archivo LOG que se puede consultar en c:\windows\logs\cbs\cbs.log.

Práctica 3

DISPONIBILIDAD

Comprobación de disponibilidad de servicios, protocolos y aplicaciones inseguras: NMAP, NESSUS, etc.

NMAP: Es una herramienta para exploración de la red y auditoría de seguridad. Determina qué equipos se encuentran disponibles, qué servicios ofrecen, qué sistemas operativos ejecutan, etc.

Práctica 3

DISPONIBILIDAD

NESSUS: Aplicación que detecta vulnerabilidades, tanto para sistemas y aplicaciones de Windows como Linux.

MBSA (Microsoft Baseline Security Analyzer): es una herramienta diseñada para analizar el estado de seguridad según las recomendaciones de seguridad de Microsoft . Detecta los errores más comunes de configuración de seguridad y actualizaciones de seguridad. (No disponible para Windows 10)

SEGURIDAD Y ALTA DISPONIBILIDAD

2. FIABILIDAD, CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

- **Alta disponibilidad** (*High Availability*): es la capacidad de que aplicaciones y datos se encuentren operativos para los usuarios autorizados en todo momento y sin interrupciones , debido principalmente a su carácter crítico .

Objetivo: mantener los sistemas funcionando 24 horas al día, 7 días a la semana, 365 días al año, a salvo de interrupciones. El mayor nivel de exigencia de alta disponibilidad acepta 5 minutos de inactividad al año, disponibilidad de 5 nueves: 99,999%.

–*Ejemplo de AD*: Centros de procesamiento de datos (CPD).

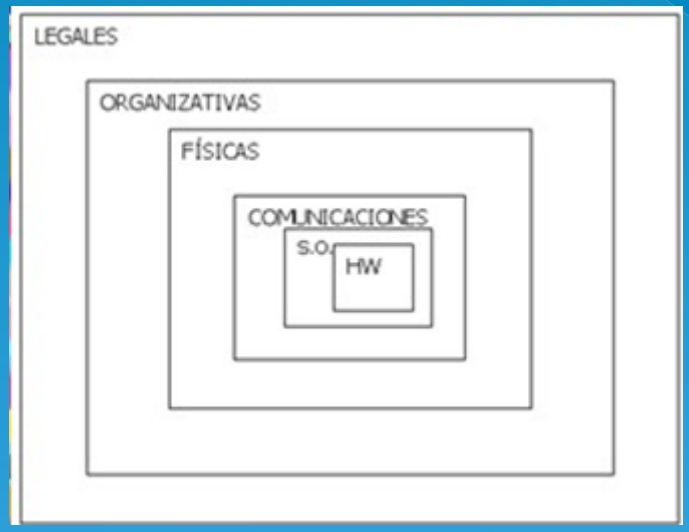
SEGURIDAD Y ALTA DISPONIBILIDAD

3. ELEMENTOS VULNERABLES EN EL SISTEMA INFORMÁTICO: HARDWARE, SOFTWARE Y DATOS

- La seguridad es un **problema integral**.
- Los problemas de seguridad informática no pueden ser tratados aisladamente ya que la seguridad de todo el sistema es igual a la de su punto más débil.
- Habitualmente los **datos** constituyen el principal elemento de los tres a proteger, ya que es el más amenazado y seguramente el más difícil de recuperar.

SEGURIDAD Y ALTA DISPONIBILIDAD

La seguridad informática comprende el hw y el s.o, las comunicaciones (p.e. protocolos y medios de transmisión seguros), medidas de seguridad físicas (ubicación de los equipos, suministro eléctrico, etc), los controles organizativos (seguridad de usuarios, acceso, contraseñas, etc.) y legales (p.e. LOPD).



SEGURIDAD Y ALTA DISPONIBILIDAD

El esquema previo sirve de base para analizar la **seguridad informática** desde distintas perspectivas:

- **Seguridad pasiva:** Seguridad física y ambiental y copias de seguridad en los sistemas informáticos.
- **Seguridad lógica:** control de acceso a los sistemas, gestión de s.o: usuarios, privilegios, contraseñas, software de seguridad *antimalware* y cifrado en la información y comunicaciones.
- **Seguridad en redes corporativas:** protocolos y aplicaciones seguras como SSH, TLS/SSL, configuraciones seguras en redes inalámbricas.

SEGURIDAD Y ALTA DISPONIBILIDAD

4. AMENAZAS

Las amenazas pueden ser provocadas por:
personas, condiciones físicas-ambientales y software o lógicas.

Personas:

- Personal de una organización: el propio personal puede producir un ataque intencionado , nadie mejor conoce los sistemas y sus debilidades. Por otro lado ex-empleados o personas descontentas con la organización pueden aprovechar debilidades que conocen.

- Hacker: experto en aspectos técnicos relacionados con la informática. Se distingue entre aquellos cuyas acciones son de carácter constructivo, informativo (hacker) o que además lo son de tipo destructivo (cracker).

SEGURIDAD Y ALTA DISPONIBILIDAD

Físicas o ambientales:

- Afectan a las instalaciones y/o el hardware contenido en ellas y suponen el primer nivel de seguridad a proteger para garantizar la disponibilidad de los sistemas.

- Robos, incendio, inundación, terremoto, cortes de suministro eléctrico, interferencias electromagnéticas, etc.

Lógicas o de software:

- Software o código que de una forma u otra pueden afectar o dañar a nuestro sistema.
- Malware (virus, gusano, troyano, etc).

SEGURIDAD Y ALTA DISPONIBILIDAD

4. AMENAZAS

Técnicas de ataque:

- Malware
- Ingeniería social / Scam / Phishing
- Botnet
- Dos / Ddos
- Spam
- Sniffing
- Spoofing / Pharming
- Password cracking / Shoulder surfing

SEGURIDAD Y ALTA DISPONIBILIDAD

- ***Malware***: Programas malintencionados(virus, espías, gusanos, troyanos, etc.) que afectan a los sistemas con pretensiones como : controlarlo o realizar acciones remotas, dejarlo inutilizable, reenvío de spam, etc.

- ***Ingenieria social***: Obtener información confidencial como credenciales (usuario-contraseña). Dicha información servirá para la obtención de beneficios económicos mediante robo de cuentas bancarias, etc.

- ***Scam***: Estafa electrónica por medio del engaño como compra de productos fraudulentos, etc

SEGURIDAD Y ALTA DISPONIBILIDAD

- ***Spam***: Correo o mensaje basura, no solicitados, no deseados, o de remitente no conocido habitualmente de tipo publicitario. Suele ser una de las técnicas de ingeniería social empleada para la difusión de scam, phishing, malware, etc.
- ***Sniffing***: Rastrear monitorizando el tráfico de una red para hacerse con información confidencial.
- ***Spoofing***: Suplantación de identidad o falsificación, por ejemplo IP, MAC, tabla ARP.

SEGURIDAD Y ALTA DISPONIBILIDAD

- ***Pharming***: Redirigir un nombre de dominio a otra máquina distinta falsificada y fraudulenta.
- ***Phishing***: Estafa basada en la suplantación de identidad y la ingeniería social para adquirir acceso a cuentas bancarias.
- ***Password cracking***: Descifrar contraseñas de sistemas y comunicaciones. Los métodos más comunes son mediante *sniffing*, observando directamente la introducción de credenciales *(shoulder surfing*), ataques de fuerza bruta, probando todas las combinaciones posibles.

SEGURIDAD Y ALTA DISPONIBILIDAD

- ***Botnet***: Conjunto de robots informáticos que se ejecutan de manera autónoma y automática, normalmente infectados, permite controlar todos los ordenadores/servidores infectados de forma remota. Sus fines normalmente son rastrear información confidencial o incluso cometer actos delictivos.

- ***Denegación de servicio o Denial of Service (Dos)***: Causar que un servicio o recurso sea inaccesible a los usuarios legítimos. Una variante es ataque distribuido de Dos o Ddos, a través de una *botnet, siendo esta técnica el ciberataque más usual y eficaz.*

SEGURIDAD Y ALTA DISPONIBILIDAD

5. PROTECCIÓN

Auditoría: Análisis de amenazas y riesgos potenciales. Adoptar medidas de seguridad.

Requisitos de auditoría y sistemas de gestión de seguridad: estándar **ISO 27001**.

Fases de auditoría:

- Enumeración de sistemas operativos, servicios, aplicaciones, topologías y protocolos de red.
- Detección, comprobación y evaluación de vulnerabilidades.
- Medidas específicas de corrección.
- Recomendaciones sobre implantación de medidas preventivas.

SEGURIDAD Y ALTA DISPONIBILIDAD

Tipos de auditoría:

- Interna
- perimetral
- test de intrusión

Ejemplos prácticos:

- Auditoría de conexiones inalámbricas o wireless
- Auditoría de acceso a sistemas operativos
- Auditoría de acceso a datos y aplicaciones seguras
- Auditoría de versiones inseguras de aplicaciones y sistema operativo

SEGURIDAD Y ALTA DISPONIBILIDAD

Medidas de seguridad

Según el recurso a proteger:

1. **Seguridad física**

   Trata de proteger el hardware, teniendo en cuenta entre otros aspectos la ubicación y las amenazas de tipo físico: robos, catástrofes naturales, etc. Algunas medidas son el estudio de la ubicación correcta, medidas preventivas contra incendios o inundaciones o el control de acceso físico.

SEGURIDAD Y ALTA DISPONIBILIDAD

2. **Seguridad lógica**

Protege el software tanto a nivel de s.o. como de aplicación, sin perder nunca de vista el elemento fundamental a proteger que son los **datos** de usuario. Dentro de sus medidas se encuentran: copias de seguridad, contraseñas, permisos de usuario, cifrado de datos, software específico antimalware, actualizaciones, etc.

SEGURIDAD Y ALTA DISPONIBILIDAD

Según el momento de ponerlas en marcha:

1. **Seguridad activa**

   Son **preventivas** y evitan grandes daños en los sistemas informáticos, por tanto, se consideran acciones previas a un ataque. P.e. las medidas de seguridad lógica.

2. **Seguridad pasiva**

   Son **correctivas**, minimizan el impacto y los efectos causados por accidentes, es decir, se consideran acciones posteriores a un ataque o incidente. P.e. copias de seguridad y todas las medidas de seguridad física.

Realizar un informe con el uso y manejo de todas las utilidades asociadas a **Confidencialidad**, **Integridad** y **Disponibilidad**.

Nombre a dar al informe:
SEGURIDAD-01-Nombre alumno