DIARIO DE CLASE

Principios de la seguridad informática

7 de abril del 2021

La seguridad informática es un conjunto de medidas y controles que aseguran la confidencialidad, integridad y disponibilidad de los activos de los sistemas informáticos.

Obxectivos:

● Confidencialidad: Capacidad de garantizar que la información solo va estar accesible para las personas o sistemas autorizadas.

● Dispoñibilidade: Capacidad de garantizar que el sistema y los datos van estar disponible al usuario en todo momento.

● Integridad: Capacidad de garantizar que los datos no fueron modificados sin autorización.

● Non repudio: Capacidad de garantizar la participación de las partes en una comunicación.

La seguridad al 100% no existe

Ataques:

● Interrupción: Impide que la información del sistema es accesible para los usuarios

● Intercepción: Acceder a la información del sistema sin autorización.

● Modificación: La información del sistema se altera, de forma que se modifica, engade o elimina información sobre los datos originales.

● Fabricación: Generar información falsa, engañando a los usuarios para que crean que esa es la información obtenida del sistema. Estos ataques pueden ser realizados sobre información almacenada, que se transmite por la red o cuando se está procesando en un equipo informático.

Técnicas:

● Sniffing: Consiste en espiar datos que se intercambian entre dos equipos.

● Spoofing: Suplantación de identidad.

● Conexións non autorizadas: Aproveitan vulnerabilidades del sistema operativo, del software ou hardware del sistema o de los protocolos de redes utilizados

● Malware: Tipo de software que la intención es perjudicar al sistema informático.

● Keyloggers: Registrar las pulsaciones del teclado para la obtención de contraseñas o PINs.

● Denegación de servicio (DoS): Saturar peticiones en un determinado servicio para conseguir que los usuarios auténticos del mismo no pueda acceder a él.

● Phishing y enxeñaría social: Engañar a los usuarios para que eles mismos proporcionen la información,

Tarefa 1

Tendo en conta este instituto donde colocarias el servidor y justifica

Amenazas y cómo evitarlas

- Incendios: lejos de calderas, alejar de objetos altamente inflamables, sistema contra incendios
- Inundaciones: evitar calderas, canalizaciones de agua,
- Robos: habitación segura, cámaras de seguridad, habitación con poco tránsito, lejos de las ventanas, sistemas de seguridad biométricos
- Desastres naturales
- Apagones: sistemas de alimentación ininterrumpida

Ubicación

- 1 o 2 planta
- Entreplanta

Copia de seguridad

• Copia completa o total: copiase todos los archivos seleccionados para la copia.

• Copia diferencial: solo se copian los archivos que se modificaron desde la última copia total. En la última copia diferencial siempre se copian los archivos que se copiaron en las anteriores copias diferenciales.

• Copia incremental: sólo se copian los archivos que se modificaron con respecto a la última copia

Tarefa 2

Elabora un plan de copia de seguridad

Completa cada semana

Diferencial todos los días

9 de abril del 2021

Potencia necesaria de sistemas de alimentación ininterrumpida

Potencia consumida P(W) = V(V)*I(A) -> 1 mejor

280V-220V

Potencia aparente S(VA)=V(V)*I(A)*(FP)

Factor de Potencia =0.5-0.7

0.6

W=V*I

$I*R*I=I^2*R$

Tarea 3

Estudio comparativo que recoge los soportes de memoria

Tipo	Capacidad	precio GB	Precio	Uso
SSD	1 TB	0.19€	185€	Guardas juegos y arranque rápido
SSD interno	1 TB	0.1€	100€	Guardar máquinas y apuntes
SATA	1TB	0.07€	69€	Guardar máquinas y apuntes
HDD interno	1 TB	0.04€	40€	Guardar máquinas y apuntes
HDD interno	4 TB	0.02€	85€	Guardar máquinas y apuntes
SSD ME	1 TB	0.11€	114€	Guardar máquinas y apuntes
Disquetes	1,44 MB	40€	4€ 10 ud	Guardar apuntes
CD	512 KB	1 €	12€ 25 ud	Guardar fotos
CD	4.7 GB	0,05€	25€ 100ud	Guardar videos
Blu-Ray	50 GB	0,08€	20€ 5 ud	Guardar videos
USB 2.0	512 MB	4€	2€	Guardar apuntes
USB 2.0	16 GB	0.5€	8€	Guardar apuntes
USB 2.0	4 GB	1,25€	5€	Guardar apuntes
USB 3.0	256 GB	0.1€	25€	Guardar apuntes
USB 3.0	2TB	0.02€	40€	Guardar máquinas y apuntes

12 de abril del 2021

Diferencia entre DAS, NAS y SAN

DAS	NAS	SAN
APP	APP	APP
	RED	
SF	SF	SF
		Red Fibra
DISCO	DISCO	DISCO

Estratexias de copias de seguridad

- Simple
    - Sinxelo
    - Pouca redundancia
    - Pouco backup histórico
- Pai (F)-Fillo (S)
    - fillos copias diferencial y diaria
    - pai copias completas y semanais
    - Sinxela
    - 8 dias de backup histórico
    - Só temos 8 días de backup con 4 cintas

- Avo-Pai-Fillo

    9 copias ao mes

    fillos copias diferencial y diaria

    pai copias completas y semanais

    avo copias total mensual

    mais redundancia

    1 mes de backup histórico

    mais complexo de xestionar as copias

- Torres de Hanoi
    - 1D

      2A

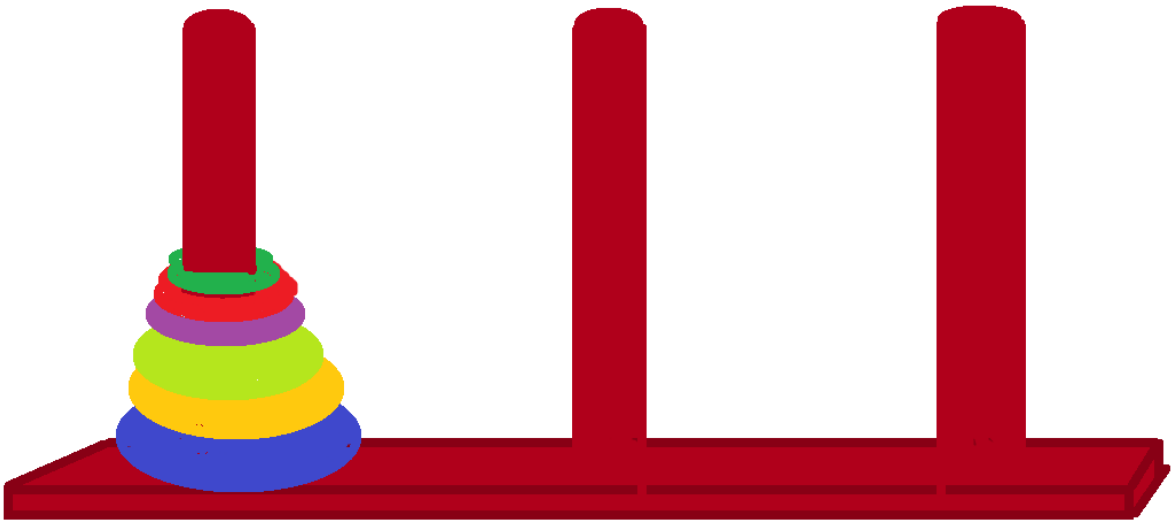
      1A

      3D

      10

      2D

      1D
    - $a_n=2_{an+}1 +1$



RAID

- RAID 0

A1	A2
A3	A4
A5	A6
A7	A8

- RAID 1 (mismos)

A1	A1
A2	A2
A3	A3
A4	A4

- RAID 5

A1	A2	A3	Ap
B1	B2	Bp	B3
C1	Cp	C2	C3
Dp	D1	D2	D3

110 011 000

Ap=101

1-> número impar

0-> número par

Tarea 4

Compara tecnologías NAS y DAS y da ventajas y desventajas.

- NAS
  - Ventajas
    - Capacidad de compartir las unidades
    - Menor costo
    - Utilización de la misma infraestructura de red
    - Gestión más sencilla
  - Desventajas
    - Menor rendimiento
    - Menor fiabilidad debido al uso compartido de las comunicaciones
- DAS
  - Ventajas
    - Costes reducidos
    - Estabilidad
    - Compatibilidad
    - Sencillez de los diseños
    - Seguridad
    - Inaccesibilidad de los datos en red
    - Velocidad de transferencia
  - Desventajas
    - Dificultad de escalabilidad
    - Difícil expansión
    - Difícil configuración

14 de abril del 2021

Alta disponibilidad

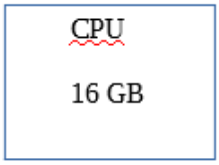
Capacidad para que los datos estén siempre disponibles

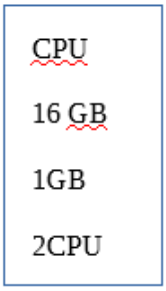
Tipos de interrupciones

- Interrupciones previstas -> cambios del sistema, mejoras del sistema mantenimiento físico
- Interrupciones imprevistas -> Incendios, inundaciones, robos, desastres naturales,apagones

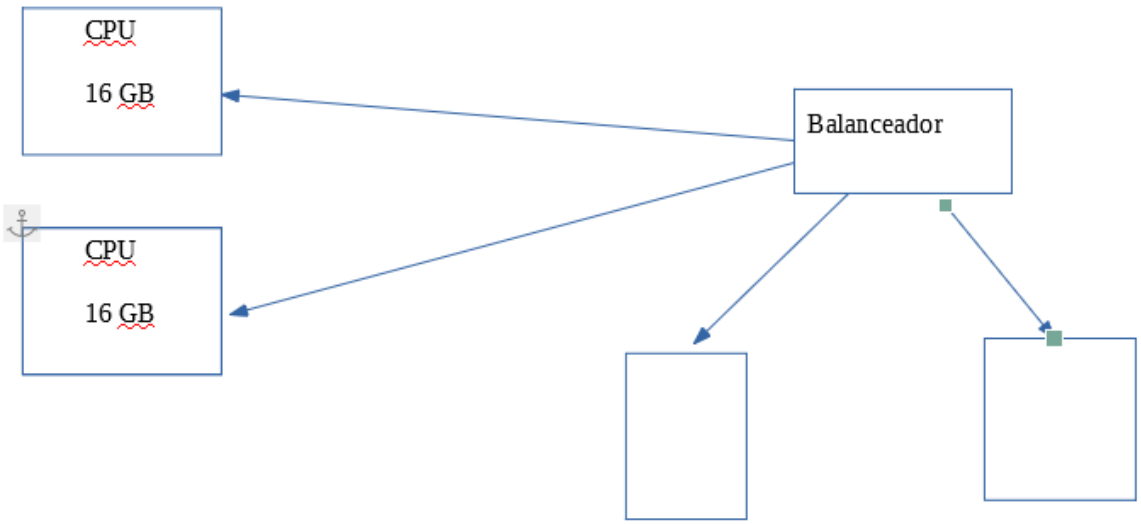
Escalabilidad

- escalabilidad vertical-> partiendo de un equipo se añaden más recursos





- escalabilidad horizontal -> derivamos o ampliando el número de equipos



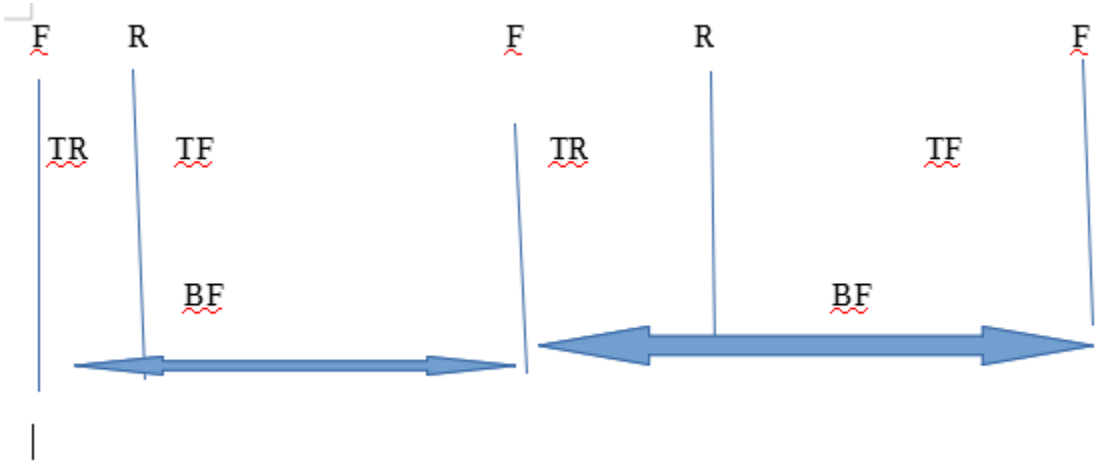
Redundancia y tolerancia a datos

- SPOP

Métricas

- MTTF (Mean time to Faiture) -> mide el tiempo entre el fallo y que se arregle se calcula : tiempo funcionando /nºfallos
- MTTR (Mean time to Recover) -> mide el tiempo medio tomado para recuperar el sistemas se calcula : tiempo inactivo / nºfallos
- MTBF (Mean time Between Faiture) -> mide el tiempo entre fallos

  se calcula : tiempo total/nºfallos



Disponibilidad	Fuera de servicio
90% ->	36.5d al año
	72h al mes
99%->	3.65 días al mes
99.9%->	8.76h al año
99.99%->	52.56 minutos al año
	1h a la semana
99.999%->	5,26 minutos al año

Tarea 5

2PC-> 75W/PC

2x monitor -> 25W/PC

FP -> 1.4

¿Cual tiene que tener un SAI para alimentar eso?

Potencia de trabajo de SAI tiene que ser siempre < 70% Potencia Total

V=W * FP

V=1.4 * [(75 * 2) +(25*2)]

V=280

280=70% Potencia Total

280*100/70=400Va

200W(PC)

50W(monitor)

a. **¿Cuántos equipos de estas características puede alimentar un SAI de 6000VA?**
b. **Estos equipos están conectados a un router de 0.2A**
c. **De qué tipo debe ser el SAI si sufrimos numerosos picos de tensión y si solo se tratase de un par de equipos domésticos ?**

a. V=W * FP

   V=1.4*250

   V=350VA por equipo

   70% Pt*6000=4200VA

   4200VA/350VA por equipo = 12 equipos

b. 0.2A-> W=230 W *0.2

   230 es la corriente eléctrica

   W=46W

   VA= 46W*1.4

   VA=64.4VA

   4200+64.4=4264.4VA

   4264.4/6000*100=71%

c. El On-line

   El off-line

Tenemos 3 SAI 1400VA, 1800VA, 2000VA

Una oficina con 2 servidores que tiene un consumo de 250W/u, 2 PCs que tiene un consumo de 100W/u, 3 monitores que tiene un consumo de 30W/u, 1 switch que tiene un consumo de 0.2A y 1 router que tiene un consumo de 0.1A

Que SAI elegimos comprar

FP=1,4

P=W*V*A

P=230*0.2

P=46W de switch

P=230*0.1

P=23W de router

P=250+100+30+46+23

P=859 de total

S=P*FP

S=859*1.4

S=1.202VA

SAI

1400*0.7=980VA

1800*0.7=1260VA

200*0.7=1400VA

Solución: el SAI de 1260VA

Tarea 6

Un servidor ha caído 3 veces en un mes con un tiempo total de inactividad de 5,5 horas.

MTTR (recuperación)

MTTF (hasta fallo)

MTBF (entre fallos)

Su nivel de disponibilidad

MTTR = 5,5/3

MTTR=1.83 horas

MTBF=30*24/3

MTBF=240 horas

MTTF= (30*24)-5.5/3

MTTF= 238.16 horas

238,16/240=0.99

99% de nivel de disponibilidad

16 de abril del 2021

Calcular el MTTR de un servidor que ha caído 5 veces en un año con un tiempo total de inactividad de 17 horas.

MTTR = 17/5=3.4 horas

Una empresa nos garantiza una disponibilidad de 99.9% al mes y la segunda nos garantiza que nuestra web no estará más de 2 días al año offline

99,9% -> 0.36 días/año

100% -> 365

x -> 363

x= 363/365*100

x=99,4%

Por lo que es mejor la primera

Un servidor ha sufrido 6 caídas en los últimos 4 meses las 5 primeras se solucionaron en 6 minutos y la última de 40 minutos. Calcula las tres métricas y el nivel de disponibilidad

Tiempo inactivo=6*5+40

Tiempo inactivo= 70 minutos

Tiempo inactivo= 1,17 horas

MTTR = 1,17/6

MTTR= 0.2 horas = 11.67 minutos

MTBF=30*24*4/6

MTBF=480 horas = 28800 minutos = 20 días

MTTF= (30*24*4)-1.17/6

MTTF= 479.81 horas

479.81/480=0.9999

99.9% de nivel de disponibilidad

Cuanto tiempo puede estar inactivo al mes un equipo para obtener la disponibilidad de 5 nueves

100% -> 1 mes

99.999% -> x

1 mes = 24*30*60 = 43200 minutos

x= 43200*99.999/100

x=43199.56 minutos

43200-43199.56= 0.43 minutos = 25.92 segundos

Tarea 7

Trabajos sobre Ransomware (en un documento aparte)

Seguridad lógica

21 de abril del 2021

Todo aquello que no queremos lo prohibimos

Principales amenazas

- **Acceso**
- **Modificaciones**

Protección

- **Control de acceso lógico**
    - **Usuario y contraseña**
        - **Ataques para romper la contraseña**
            - **Fuerza bruta**
            - **Por diccionario**
        - **Forma más fácil de evitar estos ataques**
            - **Limitar el número de intentos**

Política de contraseña

- **Mínimo 8 -16**
- **Mayúsculas, minúsculas y signos**
- **Tiempo de cambio de contraseña**
- **Evitar tener la contraseña en blanco**
- **No utilizar las mismas contraseñas**
- **No poner el usuario**

  Ejemplo: 33#13@asi.PSD

Niveles de contraseñas

- **1º: BIOS**
    - **usuario**
    - **administrador**
- **2º: Gestor de arranque**
- **3º: Sistema Operativo**
- **4º: Datos /aplicaciones**

Software Malware

Software programa diseñado para perjudicar al equipo

2000: gusanos o bonet

2010 Ataques bancarios

2012 Ataques de espionaje, dispositivos móviles, ataques especializados

Objetivos

- **Robo de información sensible**
- **Crear una red de ordenadores infectados**
- **Infección de equipos para vender antivirus falso (Rogueware)**
- **Chantajear a alguien porque has conseguido información sensible o cifrar la información (Ransomware)**

Clasificación

- **Virus: Alterar el funcionamiento de un dispositivo. Necesita la intervención del usuario, Al ejecutarse infecta los ficheros del ordenador, toma el control y se propaga dañando seriamente el dispositivo. Suele ser programas ejecutables. Los intentos 17%**
- **Gusanos: No necesitan ser ejecutados por el usuario. Se replica a sí mismo para expandirse. Por correos, bornet. Los intentos 7.7%**
- **Troyanos: Se disfraza de archivos legítimos para que una vez que lo ejecutes aproveche las vulnerabilidades del equipo y empiece a robar la información. No se propaga a sí mismo.Generan puertas traseras.Los intentos 65%**

Clasificación genérica

- **Infosteaters**
- **Crimeware**
- **Greyware**
    - **Adware-> mostrar anuncios**
    - **Spyware-> coger las páginas que visitas**
    - **Hoax -> bulos**

Tarea 8

¿Qué es un day-zero? Con ejemplos

Es un ataque contra un sistema aprovechando una vulnerabilidad que era desconocida para los usuarios y el fabricante por lo que no hay un parche

Un ejemplo es el ataque a Chrome etiquetada como CVE-2021-21166, es uno de los dos errores de seguridad reportados en el mes de febrero por investigadores del Microsoft Browser Vulnerability Research. Afecta al manejo de un componente de audio y es de gravedad crítica, un Zero Day para la que no se conocía solución de seguridad.
Google reconoció la existencia de un exploit que explotaba esta vulnerabilidad, pero no llegó a compartir más detalles para permitir que los usuarios instalaran las correcciones y con ello evitar que otros ciberdelincuentes crean malware aprovechando el fallo.

La actualización llegó a principios de marzo con la versión Chrome 89.0.4389.72 y además de corregir el 0-Day, incluye parches para otros 46 problemas de seguridad de distinta gravedad.

23 de abril del 2021

Métodos de infección

- **Vulnerabilidades aprovechar las vulnerabilidades**
  - **actualizar la versión del programa**
- **Ingeniería social abuso de confianza para obtener la información**
- **Archivos maliciosos utilizar el cracker**
- **Dispositivos extraíbles con gusanos en USB, CD**
- **Cookies maliciosas**

Método de protección

- **Uso de problemas legítimos**
- **Usar antivirus con actualizaciones periódicas**
- **Regla 321**
  - **3 copias**
  - **2 soportes**
  - **1 fuera de la empresa**

Tarea 9

Define y en qué se diferencian virus, gusanos y troyanos?

- Virus: Alterar el funcionamiento de un dispositivo. Necesita la intervención del usuario, Al ejecutarse infecta los ficheros del ordenador, toma el control y se propaga dañando seriamente el dispositivo. Suele ser programas ejecutables. Los intentos 17%
- Gusanos: No necesitan ser ejecutados por el usuario. Se replica a sí mismo para expandirse. Por correos, bornet. Los intentos 7.7%
- Troyanos: Se disfraza de archivos legítimos para que una vez que lo ejecutes aproveche las vulnerabilidades del equipo y empiece a robar la información. No se propaga a sí mismo.Generan puertas traseras.Los intentos 65%

Tarea 10

Busca distintos proveedores de antivirus y compara servicios y precios.