RA01: Adopción de pautas de seguridad informática

SAD

RA01:
“Adopción de pautas de seguridad informática”

RESULTADOS DE APRENDIZAJE

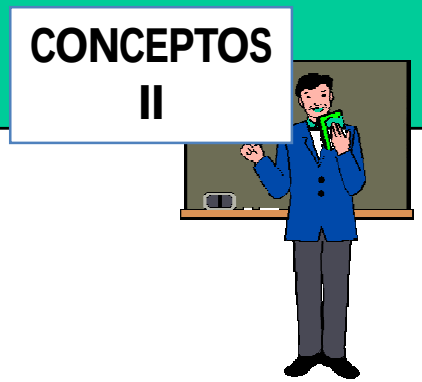
Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema

RA01:
"Adopción de pautas de seguridad informática"

- **Fiabilidad, confidencialidad, integridad y disponibilidad.**
- **Elementos vulnerables en el sistema informático: hardware, software y datos.**
- **Análisis de las principales vulnerabilidades de un sistema informático.**
- **Amenazas. Tipos:**
  - **Amenazas físicas.**
  - **Amenazas lógicas.**
- **Seguridad física y ambiental:**
  - **Ubicación y protección física de los equipos y servidores.**
  - **Sistemas de alimentación ininterrumpida.**
  - **Sistemas biométricos: Funcionamiento. Estándares.**

RA01:

“Adopción de pautas de seguridad informática”



- **Seguridad lógica:**
  - **Copias de seguridad e imágenes de respaldo.**
  - **Medios de almacenamiento.**
    - Soportes de almacenamiento.
    - Almacenamiento redundante y distribuido: RAID y Centros de Respaldo.
    - Almacenamiento remoto: SAN, NAS y almacenamiento clouding.
    - Políticas de almacenamiento.
  - **Control de acceso lógico:**
    - Identificación, autenticación y autorización
    - Política de contraseñas.
  - **Auditorias de seguridad informática .**
    - Concepto. Tipos de auditorias.
    - Pruebas y herramientas de auditoria informática.
  - **Introducción a la Criptografía.**
    - Objetivos. Conceptos. Historia.
    - Cifrado y Descifrado.

RA01:
“Adopción de pautas de seguridad informática”

CONCEPTOS II

- **Medidas de seguridad:**
  - Política de seguridad.
  - Seguridad activa y Seguridad pasiva.
- **Análisis forense en sistemas informáticos:**
  - Funcionalidad y fases de un análisis forense.
  - Respuesta a incidentes.
  - Análisis de evidencias digitales.
  - Herramientas de análisis forense.

RA01:

“Adopción de pautas de seguridad informática”

Pruebas escritas

RA01:
“Adopción de pautas de seguridad informática”

EXPOSICIÓN DE TAREAS O ACTIVIDADES I

1. **Estar al día:** Visitar los sitios web www.incibe.es (Instituto Nacional de Ciberseguridad – anteriormente INTECO) ó www.securitybydefault.com ó http://www.criptored.upm.es/ ó https://www.ccn-cert.cni.es/ , https://www.ccn.cni.es/ y escoger un artículo de tu interés.

   Enciclopedia: www.intypedia.com.Utiliza los documentos (Guión,Diapositivas,Ejercicios)de la lección que tenga más intéres para el alumno para hacer un breve resumen

2. **Confidencialidad:**

   Utilizar en Windows EFS (Encryted File System).

   Utilizar PGP en Linux.

3. **Integridad:**

   Utilizar en Windows SFC (System File Checker).

   Utilizar en GNU/LINUX Rootkit Hunter.

4. **Disponibilidad:**

   a.-Utilizar NMAP, ZNMAP o ZENMAP (www.nmap.org)

   b.-Utilizar NESSUS (www.nessus.org)

RA01:
"Adopción de pautas de seguridad informática"

EXPOSICIÓN DE TAREAS O ACTIVIDADES II

5. Vulnerabilidades

a) Realiza un **breve informe** sobre **vulnerabilidades actuales detectas en aplicaciones y sistemas operativos** como Windows, Linux, Apple, Android, Wireless, Chrome, ….etc. (http://www.securityfocus.com)

b) Realiza un **breve informe** sobre **vulnerabilidades en sistemas operativos Microsoft.** **y utiliza alguna herramienta de detección de vulnerabilidades Microsoft** en alguno de sus productos.
(https://technet.microsoft.com/es-es/security/)

c) Realiza un **breve informe** referente a:

- ¿Qué es un exploit?. Formas de protegerse.
- Tipos de exploits.
- ¿Qué es Metasploit?
- **Utiliza Metasploit** para intentar descubrir vulnerabilidades en tu PC local o en tu red.

(http://www.seguridadpc.net http://www.metasploit.com/)

RA01:
"Adopción de pautas de seguridad informática"

EXPOSICIÓN DE TAREAS O ACTIVIDADES III

6. Amenazas:

1a) FISICAS: Busca en Internet al menos una noticia relacionada con amenazas físicas a sistemas informáticos respecto a:

- Robos, sabotajes, destrucción de sistemas.
- Catástrofes, Incendios.
- Cortes de suministro eléctrico

1b) LÓGICAS: Busca en Internet al menos una noticia relacionada con amenazas lógicas respecto a:

- Ataques a un sistema informático
- Ciberdelitos.
- Ciberfraudes
- Vulnerabilidades y Amenazas

RA01:
"Adopción de pautas de seguridad informática"

EXPOSICIÓN DE TAREAS O ACTIVIDADES IV

6. Amenazas:

MALWARE:

2a) Busca al menos un antivirus on line y un antivirus en modo local y realiza su comprobación en el PC para compararlos. Anota en dicha documentación de comparación: (Número archivos analizados, % Ocupación de CPU en ejecución, opciones avanzadas de escaneo, tiempo de escaneo, vulnerabilidades y virus encontrados y desinfectados).

2b) Instala al menos dos aplicaciones antimalware en modo local y realiza su comprobación en el PC para compararlos. Anota en dicha documentación de comparación: (Número archivos analizados, % Ocupación de CPU en ejecución, opciones avanzadas de escaneo, tiempo de escaneo, vulnerabilidades y *malware* encontrado y desinfectados).

RA01:
"Adopción de pautas de seguridad informática"

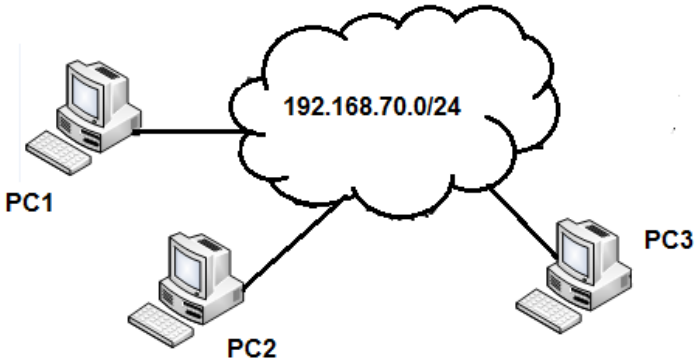
EXPOSICIÓN DE TAREAS O ACTIVIDADES V

6. Amenazas:

3) ATAQUES: (Reconocimiento)

(*individual o en grupos de dos alumnos).*

Simulación de un ataque de Reconocimiento:



Pautas:

Desde el ordenador atacante (PC1- Windows/Linux)

a) Barrido de pings y detectar el sistema operativo de los equipos activos en la red (comando o herramientas: Superscan, IP Scanner, etc)

b) Visualizar o escanear los puertos que tiene abiertos el ordenador amenazado (PC3).

c) Captura los paquetes de la red desde "Man in the Midle" situado en PC2 (Windows/Linux).

Desde el ordenador amenazado (PC3 – Windows/Linux):

a) Cerrar o abrir puertos (Windows y Linux).

b) Realiza un informe sobre software anti-sniffers Y SI LO CONSIDERAS NECESARIO UTILIZA EL MISMO para detectar desde PC3 sniffers situados en la red.

RA01:
"Adopción de pautas de seguridad informática"

EXPOSICIÓN DE TAREAS O ACTIVIDADES VI

7. Seguridad física y ambiental:

UBICACIÓN Y PROTECCIÓN FÍSICA DE LOS EQUIPOS Y SERVIDORES DEL AULA:

1a) Se necesita realizar **un estudio de la ubicación y protección física de los equipos y servidores del aula,** desde el punto de vista de:

a) Acondicionamiento físico (Extintores, Sistema de aire acondicionado, Generadores eléctricos autónomos, racks)

b) Robo o sabotaje: Control de acceso físico y vigilancia mediante personal y circuitos cerrados de televisión (CCTV).

c) Condiciones atmosféricas y naturales adversas (Ubicación de sistemas, centros de respaldo en ubicación diferente al centro de producción, mecanismos de control y regulación de temperatura, humedad, etc.)

Para elaborar dicho estudio recogido en un documento se sugiere visitar entre otros los enlaces:

http://www.accesor.com http://www.abast.es/cs_condis_cpd.shtml

1b) Instalación de una cámara IP y transmisión de la imagen por una red LAN.

Descarga el manual del proceso de instalación de una cámara IP y su gestión mediante software.

Se sugiere visitar el enlace:

http://www.ovislink-espana.com/es/4_4_22/Videovigilacia-Seguridad/

RA01:
"Adopción de pautas de seguridad informática"

EXPOSICIÓN DE TAREAS O ACTIVIDADES VII

SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA:

2a) **Busca un único SAI para todos los sistemas informáticos del aula.** Realiza un inventario de los sistemas informáticos a utilizar y justifica tu respuesta **utilizando un selector de SAIs**. Se sugiere visitar entre otros los enlaces: http://selector.salicru.com http://www.apc.com/home/es/es/ http://www.mgeups.co.uk/ http://www.riello-ups.com/?es/configuratore http://www.emersonnetworkpower.com/

2b) Instalación, configuración y administración de un SAI o UPS.

Descarga algún manual y analiza el proceso de instalación del SAI o UPS y su gestión mediante software.
http://catalogo.salicru.com/es/domestico/familia/sistemas-alimentacion-ininterrumpida/serie/sps-one
http://powerquality.eaton.com/Products-services/legacy/patriot-info.asp

SISTEMAS BIOMÉTRICOS:

3) Ampliar el estudio realizado del apartado 7.1a) del aula con la implantación de sistemas biométricos

Se sugiere visitar los enlaces: http://www.zksoftware.es/ http://www.biometriaaplicada.com/ http://www.kimaldi.com/productos/sistemas_biometricos/ http://www.agedum.com/BioCloser/tabid/110/Default.aspx

RA01:
"Adopción de pautas de seguridad informática"

EXPOSICIÓN DE TAREAS O ACTIVIDADES VIII

8. Seguridad lógica:

COPIAS DE SEGURIDAD E IMÁGENES DE RESPALDO:

1a) Demuestra el uso de una **copia de seguridad con herramientas del sistema o mediante aplicaciones específica.** *Debe realizarse también la restauración.* Se sugiere utilizar algunos de los indicados a continuación:

Herramientas del sistema: En GNU/Linux: tar y crontab, rsync.
En Windows: Copias de seguridad y Restaurar Sistema.

Aplicaciones específicas: En GNU/Linux: fwbackup.
En Windows: Cobian Backup

Herramientas de recuperación de datos: En GNU/Linux: TextDisk, Foremost, Scalpel.
En Windows: Recuva.

1b) Crear una **imagen de respaldo de tu equipo utilizando software del mercado y realiza una demostración práctica de uno de ellos.**

RA01:
"Adopción de pautas de seguridad informática"

EXPOSICIÓN DE TAREAS O ACTIVIDADES IX

MEDIOS DE ALMACENAMIENTO:

2a) Realiza **un informe con los servicios de almacenamiento que ofrecen las empresas:**

HP, Dell y EIDSERVICIOS: www.hp.com www.dell.es http://eidservicios.com/

2b) Utiliza en un entorno simulado un **medio de almacenamiento "RAID 1" con máquinas virtuales GNU/Linux o Windows**

2c) Utiliza un **sistema de almacenamiento "clouding"** (DropBox,iCloud,GoogleDrive,...) y demuestra su uso desde un punto de vista de la movilidad del usuario.

CONTROL DE ACCESO LÓGICO:

3) Control de acceso lógico: Realiza la creación de una cuenta de usuario y su contraseña (política fuerte de contraseñas - modo comando/ modo gráfico) que permite posteriormente acceder o no al sistema en sistemas Windows y sistemas GNU/Linux .

AUDITORIAS DE SEGURIDAD INFORMÁTICA:

4) Verifica la auditoria de control de acceso "Visor de sucesos" de dicho usuario en Windows y Linux .

RA01:
"Adopción de pautas de seguridad informática"

EXPOSICIÓN DE TAREAS O ACTIVIDADES
X

INTRODUCCIÓN A LA CRIPTOGRAFÍA:

5) Encripta y desencripta varios ficheros utilizando diferentes sistemas de cifrado en sistemas Windows y GNU/Linux.

Se sugiere utilizar los programas:

En sistemas Windows **CryptoForge para Sistemas Windows** **http://www.cryptoforge.com.ar/**

Gp4win **http://www.gpg4win.org**

En sistemas GNU/Linux: comando **tr**.

9. Medidas de seguridad:

Realiza un breve informe sobre el aula de la clase para implantar medidas de **seguridad activa** y **seguridad pasiva**.

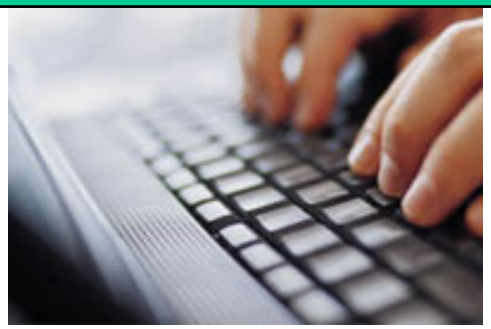
10. Análisis forense en sistemas informáticos:

Realiza un análisis forense de tu equipo informático en entorno Windows como si hubiera sido saboteado. (sigue el índice del documento de INCIBE: (https://www.incibe.es/extfrontinteco/img/File/intecocert/ManualesGuias/incibe_toma_evidencias_analisis_forense.pdf)

y utiliza alguno de los comandos o herramientas de análisis forense indicados en el documento.

RA01:

“Adopción de pautas de seguridad informática”



REALIZACIÓN DE TAREAS O ACTIVIDADES POR EL ALUMNO