

Ejercicios seguridad fisica y logica

1. Ponte de acuerdo con un compañero/a de clase. A continuación verás que hay una serie de definiciones de conceptos (confidencialidad, integridad, ...). Uno de los/las dos deberá leer las definiciones pares y el otro las impares. Una vez hecho esto, cada uno deberá explicarle a la otra persona las definiciones que ha leído y tendrás que:

- a. Escribir lo que has entendido en el cuaderno de clase.
- b. Explicar una de ellas en clase, para ver que efectivamente lo has entendido.

-Integridad: Hacer que los datos no sean alterados a no ser que el autor de su consentimiento

-Autenticación: Sirve para confirmar que una persona máquina o entidad no es un impostor, para eso podemos utilizar mediante una tarjeta, usuario y contraseña o una parte de tu cuerpo, cuanto más pongamos mejor.

-Cifrado: A un documento lo cifras , es decir que lo codificas con una clave y/o un algoritmo para que aquellas personas que no lo conozcan sea invisible o no lo puedan ver

-No repudio: La comunicación entre el emisor y receptor sea segura. Existen dos tipos no repudio en origen, que el emisor no puede negar la comunicación y el repudio en destino, que el receptor no puede negar la comunicación.

-Riesgo: Valorar el peligro de que una amenaza exista o se ejecute

-Desastres: Algún accidente ya puede ser intencionado o natural que obliga a interrumpir las operaciones.

-Centro de proceso de datos: Un lugar donde se procesan y se guardan los datos centralizados.

2. Piensa en los perfiles de atacantes que hay en el tema. ¿Hay alguien en tu clase que creas que el día de mañana pueda responder a uno de ellos? Explica por qué, aunque no pongas el nombre propio.

Yo creo que la mayoría si llegan,llegarian a hackers porque no les veo haciendo el mal, pero si diria que podría haber un cracker porque le gusta burlar la seguridad de internet por

beneficio propio pero otra gente que la tengo como hacker podría pasarse al bando del cracker por necesidad yo incluyendome.

3. De cada uno de los elementos expuestos a continuación, indica a qué tipo de seguridad están asociado (activa, pasiva, lógica y física)

- a. Ventilador de un equipo informático:** Activa,física
- b. Detector de incendio:** Pasiva, física
- c. Detector de movimientos:** Pasiva, físico
- d. Cámara de seguridad:** Pasiva, física
- e. Cortafuegos:** Activo, lógico
- f. SAI:** Pasivo,físico
- g. Control de acceso mediante el iris del ojo:** activo, lógico
- h. Contraseña para acceder a un equipo:** activa, lógica
- i. Control de acceso a un edificio:** activo, físico

4. Asocia las siguientes amenazas con la seguridad lógica y la seguridad física.

- a. Terremoto.** Físico
- b. Subida de tensión.** Físico
- c. Virus informático.** Logica
- d. Hacker.** Lógico
- e. Incendio fortuito.** Físico
- f. Borrado de información importante.** Lógico

5. Asocia las siguientes medidas de seguridad con la seguridad activa o pasiva.

- a. Antivirus.** Ambos.
- b. Uso de contraseñas.** Activo
- c. Copias de seguridad.** Pasivo
- d. Climatizadores.** Pasivo
- e. Uso de redundancia en discos.** Pasivo
- f. Cámaras de seguridad.** Pasivo
- g. Cortafuegos.** Activo

6. De las siguientes contraseñas indica cuales se podrían considerar seguras y cuáles no y por qué:

- a. mesa:** No porque al existir la palabra pueden sacarla en un diccionario
- b. caseta:** No porque al existir la palabra pueden sacarla en un diccionario
- c. c8m4r2nes:** Si porque es una palabra que no existe y tiene combinacion de letras y números
- d. tu primer apellido:** Porque es algo que cualquiera puede saber
- e. pr0mer1s&:** Si porque es una palabra que no existe y tiene combinacion de letras y números y un caracter especial
- f. tu nombre:** Porque es algo que cualquiera puede saber

7. Ordena de mayor a menor seguridad los siguientes formatos de claves.

- a. Claves con sólo números.**
- b. Claves con números, letras mayúsculas y letras minúsculas.**
- c. Claves con números, letras mayúsculas, letras minúsculas y otros caracteres.**
- d. Claves con números y letras minúsculas.**

e. Claves con sólo letras minúsculas.

c > b > d > a > e

Practicas seguridad fisica y logica

- 1. En el cuaderno de clase enumera 5 casos en los que alguien quisiera utilizar algún método que violara la seguridad, porque quiere vulnerar la seguridad y con qué fin.**

Uno que le piense que su novia es infiel averiguar su clave de facebook, gmail abrir una web wifi y actuar de sniffer para conseguir sus contraseñas

Intentar conseguir la contraseña de un juego para vender sus objetos con un keylogger

No tener idea de programar y extorsionar a la victima fisicamente para conseguir sus datos

Mandar un e-mail con una aplicacion que sea un script que te haga capturas de pantalla cada cierto tiempo y enviartelas a ti

Alguien que intenta mejorar la seguridad de un programa/pagina web y la ataca para luego parchear esos problemas

- 2. Busca qué es una ACL, entiéndelo, y explícalo en clase.**

ACL: Es un tipo de seguridad informática que se usa para separar los privilegios. Es una forma de hacer los permisos de acceso apropiados a un determinado objeto que depende de ciertos procesos que hace el que lo pide.

3. Busca qué es sfc, entiéndelo, y explícalo en clase.

Es un comando que analiza los archivos y si ve que uno esta sobrescrito lo devuelve a su estado original

4. Describe los medios de seguridad física y lógica que hay en el aula.

Física: Extintores

Lógica: contraseñas, usuarios.

5. Evalúa qué medidas de seguridad activa y pasiva tienes en torno a tu ordenador personal.

Activa: Antivirus, antispyware, firewall

Pasiva: Antivirus, copias de seguridad,

6. Analiza qué pautas de protección no cumple el sistema que tienes en tu casa.

