

Ejercicios

1. Ve al apartado del tema donde se ofrecen una serie de definiciones como integridad, confidencialidad, no repudio, ...

confidencialidad: Sólo quién tu quieras puede saber la información.

disponibilidad: Poder ver la información cuando se quiera

autorización: darle permisos a alguien

accounting: seguir los pasos de una persona

vulnerabilidad: que se puede atacar ya que tiene un fallo

impacto: “coste” de los daños

plan de contingencia: Medidas de prevención. Se podría resumir en hacer una evaluación, luego planificar y hacer pruebas.

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 un de ellos? Explica por qué, aunque no pongas el nombre propio.

Cracker, ya que alguno seguro que el día de mañana hace daño a equipos solo por obtener beneficios

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 - física y activa
- b. Detector de incendio - física y pasiva
- c. Detector de movimientos - física y activa
- d. Cámara de seguridad - física y activa
- e. Cortafuegos - lógica y pasiva
- f. SAI - física y pasiva
- g. Control de acceso mediante el iris del ojo - física y activa
- h. Contraseña para acceder a un equipo - lógica y activa
- i. Control de acceso a un edificio - física y activa

4. Asocia las siguientes amenazas con la seguridad lógica y la seguridad física.
 - a. Terremoto. física
 - b. Subida de tensión. física
 - c. Virus informático. lógica
 - d. Hacker. lógica
 - 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. activa
 - b. Uso de contraseñas. activa
 - c. Copias de seguridad. pasiva
 - d. Climatizadores. activa
 - e. Uso de redundancia en discos. pasiva
 - f. Cámaras de seguridad. activa
 - g. Cortafuegos. pasiva
1. De las siguientes contraseñas indica cuales se podrían considerar seguras y cuáles no y por qué:
 - a. mesa - corta y fácil de averiguar por programas
 - b. caseta - corta y fácil de averiguar por programas
 - c. c8m4r2nes - es buena ya que contiene números y letras
 - d. tu primer apellido - típica contraseña, poco segura ya que si te conoce la puede averiguar
 - e. pr0mer1s& - buena, ya que contiene letras y caracteres
 - f. tu nombre - típica contraseña, poco segura ya que si te conoce la puede averiguar
7. Ordena de mayor a menor seguridad los siguientes formatos de claves.

Claves con números, letras mayúsculas, letras minúsculas y otros caracteres.

Claves con números, letras mayúsculas y letras minúsculas.

Claves con números y letras minúsculas.

Claves con sólo letras minúsculas.

Claves con sólo números.

Prácticas

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.

Intercepción: Querer conseguir alguna contraseña para poder suplantar su identidad

Modificación: Cambiar los datos de un texto para conseguir que no haga algún acuerdo una empresa y así poder hacerle perder dinero

Suplantación: Suplantar la identidad de alguien para difundir información y que la tachen en la sociedad

Interrupción: Querer hacer caer un servidor para poder meterle algún malware

Amenaza pasiva: Querer ver lo que escribe una empresa para adelantarte a sus pasos y hacerle “counter”

-

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

Es una lista de control de acceso, su objetivo principal es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición.

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

Comprobador de archivos de sistema, es una utilidad de Windows que permite a los usuarios detectar daños en los archivos de sistema de Windows y restaurar archivos dañados.

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

Contraseñas de los usuarios, lógica

Proxy de conselleria, lógica

Copia de seguridad del sistemas o de los sistemas, lógica

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

Bridas para los cables: activa

Antivirus: activa

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

El único fallo de protección que me falta en mi casa es un SAI, ya que por lo demás estoy seguro.

7. Busca en Internet las claves más comúnmente usadas.

- 1) 123456
- 2) password
- 3) 12345
- 4) 12345678
- 5) qwerty
- 6) 123456789
- 7) 1234
- 8) baseball
- 9) dragon
- 10) football
- 11) 1234567
- 12) monkey

8. Decides montar una empresa en Internet que se va a dedicar a ofrecer un disco duro on-line. Necesitas de cada usuario: nombre, teléfono y dirección de correo electrónico. ¿En qué afectar estos datos a la formación de tu empresa? ¿Qué medidas de seguridad tendrás que tomar cuando almacenamos esta información?

En mi opinión habría que tener una base de datos en excel u otro programa similar con toda la información organizada y guardarla diariamente, semanal, mensual o trimestral y tenerlo en la nube o un disco duro externo para que no se pierda por un posible virus o programa malicioso.

9. Busca en Internet un protocolo de actuación ante un desastre natural, cita las cosas que veas interesantes (que tipo de personas interviene), pues las vas a explicar en clase, y añade a ese protocolo las medidas que consideres para no perder la información de la organización.

PROTOCOLO Evacuación:

Avisar a los servicios de emergencia y desalojar a las personas del recinto donde se requiera una evacuación, siempre con tranquilidad como bien se dice “dame prisa e iré lento” no por ocurrir un desastre hay que alocarse ya que hay que seguir un orden para la evacuación para no colapsar a todo el mundo por la misma salida y así poder salir del recinto más rápido y con seguridad para todos.

Tiene que haber una persona para guiar a los demás desalojar más rápido y salir por la salida más cercana y otra que asegure que no queda nadie en el recinto por desalojar (sobre todo si es en un edificio con plantas).