Tema 1 ejercicio 2

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

# Ponte de acuerdo con un compañero/a de clase.

# 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:

# Escribir lo que has entendido en el cuaderno de clase.

# Explicar una de ellas en clase, para ver que efectivamente lo has entendido.

-**Confidencialidad:**Es hacer que una información le llegue solo a las personas autorizadas. Por tanto un documento confidencial solo puede ser entendido por la persona que esté autorizada

**-Disponibilidad:** Es la capacidad de hacer llegar la información a las personas.

**-Autorización:** Una vez autentificado los usuarios tendrán ciertos privilegios como por ejemplo el acceso, la lectura, la escritura, etc.

**-Accounting:** Seguimiento de operaciones que hace toda persona registrada

**-Vulnerabilidad:** Fallo en un sistema el cual puede ser usado para atacar. Estas pueden ser reconocidas o no reconocidas

**-Impacto:** Cantidad de daño producido ante un ataque

**-Plan de contingencia:** Procesos de seguridad que se siguen para la prevención de un sistema. Estos procesos no provocan que no haya probabilidad de que ocurra un fallo. Consiste en evaluar los peligros, planificar las actuaciones y hacer pruebas para evaluar la eficacia

**Ejercicio 2.3**

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.

-Robar tu dinero en un cajero externo para su uso propio

-Robar tus contraseñas del ordenador para arruinarte un poco la vida

-Entrar en la red de una empresa para saber cierta información y venderla

-Liberar tu teléfono de la empresa en cuestión de forma que puedas instalar y modificar lo que tu quieras

-Crear un troyano para que le des acceso a tu internet, y así no tiene que tener el internet propio

**Ejercicio 2.3.2**

1. 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.

Si, veo varios *crackers* en la clase, por su carácter de querer poder molestar a otros y poder hacer cosas sin pagar etc.

Un sniffer, porque solo por su nombre le hará gracia

**Ejercicios final de tema**

1. De cada uno de los elementos expuestos a continuación, indica a qué tipo de seguridad están asociado (activa, pasiva, lógica y física)
   1. Ventilador de un equipo informático **activa física**
   2. Detector de incendio. **pasivo** **físico**
   3. Detector de movimientos **pasivo**  **físico**
   4. Cámara de seguridad **activo físico**
   5. Cortafuegos **activo lógico**
   6. SAI **activa y pasiva, física**
   7. Control de acceso mediante el iris del ojo. **activa física**
   8. Contraseña para acceder a un equipo **activo lógico**
   9. Control de acceso a un edificio **activo físico**
2. Asocia las siguientes amenazas con la seguridad lógica y la seguridad física.
   1. Terremoto. **F**
   2. Subida de tensión. **F**
   3. Virus informático. **L**
   4. Hacker. **F**
   5. Incendio fortuito. **F**
   6. Borrado de información importante. **L**
3. Asocia las siguientes medidas de seguridad con la seguridad activa o pasiva.
   1. Antivirus. **AP**
   2. Uso de contraseñas. **A**
   3. Copias de seguridad. **P**
   4. Climatizadores. **A**
   5. Uso de redundancia de discos. **A**
   6. Cámaras de seguridad. **A**
   7. Cortafuegos. **AP**
4. De las siguientes contraseñas indica cuales se podrían considerar seguras y cuáles no y por qué:
   1. mesa  **no porque es fácil y débil**
   2. caseta **no porque es fácil y débil**
   3. c8m4r2nes **sí porque es compleja**
   4. tu primer apellido **no porque es fácil y débil**
   5. pr0mer1s& **sí porque es compleja**
   6. tu nombre **no porque es fácil y débil**
5. Ordena de mayor a menor seguridad los siguientes formatos de claves.
   1. Claves con sólo números. **4**
   2. Claves con números, letras mayúsculas y letras minúsculas. **2**
   3. Claves con números, letras mayúsculas, letras minúsculas y otros caracteres. **1**
   4. Claves con números y letras minúsculas. **3**
   5. Claves con sólo letras minúsculas. **5**
6. Busca qué es una ACL, entiéndelo, y explícalo en clase.

**Lista de control de accesos, sirve para controlar las diferentes categorias de accesos, para controlar que un usuario normal por ejemplo no pueda hacer cosas de administrador**

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

**Es un comando para corregir los archivos que pueden haberse estropeado o quedado inservibles por nuevas actualizaciones, etc**

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

**Físicos: Extintor, ventana, caja del switch, ventiladores del procesador**

**Lógicos: La ACL**

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

**Activo: SAI, antivirus, regletas, ventilador de procesador, zona ventilada, espacio**

**Pasivo: SAI, antivirus**

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

**A mi me parece correcto**

1. Busca en Internet las claves más comúnmente usadas.

**La de 1234, tu y tu pareja, fecha de nacimiento, 1234 y fecha de nacimiento, nombre mascota, nombre cantante o grupo, nombre youtuber favorito**

1. 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?

**Son datos privados de la gente y tendrás que tener un buen sistema de seguridad para almacenar esos datos, además de copias de seguridad**

1. 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.

**Plan de recuperación ante desastres: Consiste en una serie de procesos para recuperar los datos sobre el hardware y el software, de forma que la empresa en cuestión no se quede sin nada y pueda volver a empezar o almenos salir del paso**