Ejercicios:

Ejercicio 1 (Parte impar)

1. Ve al apartado del tema donde se ofrecen una serie de definiciones como integridad, confidencialidad, no repudio, …
2. Ponte de acuerdo con un compañero/a de clase.
3. Uno de los/las dos deberá leer las definiciones pares y el otro las impares.
4. Una vez hecho esto, cada uno deberá explicarle a la otra persona las definiciones que ha leído y tendrás que:
5. Escribir lo que has entendido en el cuaderno de clase.
6. Explicar una de ellas en clase, para ver que efectivamente lo has entendido

- 1.-Integridad -> Un archivo en el que solo se puede modificar mediante autorización del creador.
- 3.-Autenticación -> Es una forma de seguridad con la que demuestras que eres quien dice ser.
- 5.-Cifrado -> Codificación de un mensaje para que solo lo pueda ver la gente que esté autorizada.
- 7.-No repudio -> Es la garantización de que una comunicación haya existido.
- 9.-Riesgo -> Es la medida de exposición ante un ataque.
- 11.-Desastre -> Interrupción de los planes de una empresa o compañía
- 13.-Centro de proceso de datos -> Es un servidor donde se almacenan datos.

Ejercicio 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.

- Yo creo que Javier va a ser un hacker o un intento de ello ya que ese tema le gusta mucho, esta “todos” los dias investigando y creo que lo será.

Ejercicio 3

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/Físico
    2. Detector de incendio. -> Pasivo/Lógico
    3. Detector de movimientos -> Activo/Físico
    4. Cámara de seguridad -> Pasivo/Físico
    5. Cortafuegos -> Activo/Lógico
    6. SAI -> Activo/Físico
    7. Control de acceso mediante el iris del ojo. -> Activo/Físico
    8. Contraseña para acceder a un equipo -> Activo/Lógico
    9. Control de acceso a un edificio -> Activo/Físico

Ejercicio 4

1. Asocia las siguientes amenazas con la seguridad lógica y la seguridad física.
    1. Terremoto. -> Física
    2. Subida de tensión. -> Lógica
    3. Virus informático. -> Lógico
    4. Hacker. -> Lógico
    5. Incendio fortuito. -> Física
    6. Borrado de información importante. -> Lógio

Ejercicio 5

1. Asocia las siguientes medidas de seguridad con la seguridad activa o pasiva.
    1. Antivirus. -> Activa y Pasiva
    2. Uso de contraseñas. -> Activa
    3. Copias de seguridad. -> Pasiva
    4. Climatizadores. -> Activa

5. Uso de redundancia en discos. -> Pasiva
6. Cámaras de seguridad. -> Pasiva
7. Cortafuegos. -> Activa

Ejercicio 6

1. De las siguientes contraseñas indica cuales se podrían considerar seguras y cuáles no y por qué:
    1. mesa -> No segura ya que es muy fácil adivinar debido a sus pocos caracteres y 0 combinaciones de letras, números y signos.
    2. caseta -> No segura ya que es muy fácil adivinar debido a sus pocos caracteres y 0 combinaciones de letras, números y signos.
    3. c8m4r2nes -> Es segura ya que mezcla al menos números y letras.
    4. tu primer apellido -> No segura ya que es muy fácil adivinar debido a sus pocos caracteres y 0 combinaciones de letras, números y signos.
    5. pr0mer1s& -> Es segura ya que mezcla letras, números y signos.
    6. tu nombre -> No segura ya que es muy fácil adivinar debido a sus pocos caracteres y 0 combinaciones de letras, números y signos.

Ejercicio 7

1. Ordena de mayor a menor seguridad los siguientes formatos de claves.
    1. Claves con sólo números.

2. Claves con números, letras mayúsculas y letras minúsculas.
3. Claves con números, letras mayúsculas, letras minúsculas y otros caracteres.
4. Claves con números y letras minúsculas.
5. Claves con sólo letras minúsculas.

Mayor Menor

C-B-D-A-E

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.**

1.- Intentar entrar en una empresa de la competencia para ver sus cosas.

2.- Alguien que haya sido despedido y se quiera vengar entrando en la empresa y revelando todo

3.- Algún pederasta que quiera conseguir fotos de menores mediante virus.

4.- Robar cuentas bancarias con el fin de sacar dinero.

5.- Chantajear gente para así sacar dinero o cuentas o lo que sea que busque.

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

Es un concepto de seguridad informática usado para fomentar la separación de privilegios. Lo que hace es comprobar la integridad de los ficheros protegidos del sistema Windows, y repararlos en caso de que presenten algún tipo de corrupción o anormalidad.

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

Lo que hace es comprobar la integridad de los ficheros protegidos del sistema Windows, y repararlos en caso de que presenten algún tipo de corrupción o anormalidad.

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

Física -> El extintor, los ventiladores y que no se pueda comer y beber

Lógica -> Los antivirus, los proxys de consellería, las contraseñas y las autenticaciones de los correos.

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

Activa -> El antivirus, el cortafuegos, las contraseñas.

Física -> Las fundas y no beber muy cerca del PC

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

Pues de momento lo único es que no dispongo de SAI.

7. **Busca en Internet las claves más comúnmente usadas.**

La más usada es la 123456, la siguiente es password y le sigue la 1245678.

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 afecta estos datos a la formación de tu empresa? ¿Qué medidas de seguridad tendrás que tomar cuando almacenamos esta información?**

Afecta en que no pueden coger los datos sin su consentimiento ya que hay una ley que lo prohíbe, tienen que pedirlo para que éste acepte.

Las medidas serían tener una fichero por usuaria y cada fichero encriptarlo para que no puedan sacar la información tan fácilmente y también que a esos ficheros solo pueda acceder una persona o varias en caso de que el servidor lo manejan varias personas.

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.**