Ejercicios

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

- **La confidencialidad:** Significa que solo pueda acceder a la información la gente a la que tu le dejes.
- **Disponibilidad:** Que puedas acceder a la información cuando la necesites.
- **Autorización:** Son los permisos que le das al usuario que pueda hacer con la información como podría ser lectura, escritura o ejecución.
- **Accounting:** Controla lo que hace el usuario.
- **Vulnerabilidad:** Punto débil del sistema por el cual podría ser atacado, lo que se recomienda tener todo actualizado tanto software como hardware.
- I**mpacto:** Evaluación de los daños producidos por el ataque
- **Plan de contingencia:** Medidas de seguridad para evitar una catástrofe o pérdida de datos etc. Podríamos tener en cuenta tres: Evaluar futuros peligros, hacer un plan de recuperación y hacer un simulacro para asegurar que sea eficaz.

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.**

Podría querer ser cracker para obtener la clave de wifi en su beneficio para tener internet gratis en su casa.

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.**

Activa,Física

    c. **Detector de movimientos**

Activa,Física

d. Cámara de seguridad

Activa,Física

e. Cortafuegos

Activa,Lógica

f. SAI

Activa,Pasiva,Física

g. Control de acceso mediante el iris del ojo.

Activa,Pasiva,Física

h. Contraseña para acceder a un equipo

Activa,Logica

i. Control de acceso a un edificio

Activa,Física

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

a. Terremoto.

física

b. Subida de tensión.

lógica

c. Virus informático.

lógica

d. Hacker.

lógica

e. Incendio fortuito.

física

f. Borrado de información importante.

lógica

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

a. Antivirus.

Activa, pasiva

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.

Activa

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

a. mesa

No segura, porque es una palabra muy corta de 4 letras, y no contiene ni signos ni numeros sería muy facil de descifrar.

b. caseta

No segura, porque es una palabra muy corta de 4 letras, y no contiene ni signos ni numeros sería muy facil de descifrar.

c. c8m4r2nes

Segura, porque contiene mezcla de letras y números y es larga.

d. tu primer apellido

No segura, porque si el atacante te conoce podria descifrarlo facilmente.

e. pr0mer1s&

Segura, porque contiene letras, palabras y signo ademas de que es larga.

f. tu nombre

No segura, porque tu nombre lo pueden obtener de muchas maneras para probarla y porque no contiene ni numeros ni signos.

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 > e > a

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 tumbar un servidor con spam como sería por ejemplo de películas, para que mi pagina de peliculas no tuviera competencia.
2. Crear una pagina parecida a la Caixa y pedir documentos del banco para obtener el dinero de esa persona.
3. Enviarle un virus a una persona por correo pasándose por su pagina favorita, por ejemplo el facebook o pasándose por uno de sus amigos, diciéndole que abra un enlace o descargue un programa para ejecutarlo,
4. A una novia/o para sacarle información de su facebook por ejemplo para obtener fotos, mensajes etc.
5.