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.**

- **Integridad**: Es la capacidad de hacer que los datos no sean alterados sin el consentimiento del autor.
- **Autenticación**: Intenta demostrar tanto si eres una persona o una máquina que eres lo que dices ser.
- **Cifrado**: Mecanismo para codificar de manera inteligible para personas no autorizadas el acceso a cierta información.
- **No repudio**: Es no poder negar una comunicación que ha ocurrido.
    - No repudio de origen: El emisor no puede negar la conversación ya que ha estado enviando información.
    - No repudio de destino: El receptor no puede negar la conversación ya que ha estado recibiendo información.
- **Riesgo**: Es lo expuesto que está un sistema a las diferentes vulnerabilidades.
- **Desastres**: Es cualquier evento que interrumpe totalmente los servicios y operaciones de una organización.
- **Centro de procesos de datos:** Es el sitio centralizado donde almacenan o procesan los datos.

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.**

Yo pienso que Javi puede llegar a ser Hacker, ya que le interesa mucho en el tema.

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 y física.
    b. **Detector de incendio**→ Pasiva y física.
    c. **Detector de movimientos**→ Pasiva y física.
    d. **Cámara de seguridad**→ Pasiva y física.
    e. **Cortafuegos**→ Activa y lógica.
    f. **SAI**→ Pasiva y física.
    g. **Control de acceso mediante el iris del ojo**→ Activa y física.
    h. **Contraseña para acceder a un equipo**→ Activa y lógica.
    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**→Física.
    f. **Borrado de información importante**→Lógica.

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

    a. **Antivirus**→Activa y pasiva.
    b. **Uso de contraseñas**→Activa.
    c. **Copias de seguridad**→Activa.
    d. **Climatizadores**→Pasiva.
    e. **Uso de redundancia de discos**→Activa.
    f. **Cámaras de seguridad**→Pasiva.
    g. **Cortafuegos**→Pasiva.

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

    a. **mesa**→No, es demasiado fácil.
    b. **caseta**→No, es demasiado fácil.
    c. **c8m4r2nes**→Si, ya que tiene letras y números y por lo tanto es más difícil de adivinar.
    d. **tu primer apellido**→No, cualquier persona que te conozca podría acceder.
    e. **pr0mer1s&**→Si, ya que tiene letras y números y por lo tanto es más difícil de adivinar.
    f. **tu nombre**→No, cualquier persona que te conozca podría acceder.

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

    a. Claves con sólo números. →4.
    b. Claves con números, letras mayúsculas y letras minúsculas. →2.
    c. Claves con números, letras mayúsculas, letras minúsculas y otros caracteres. →1.
    d. Claves con números y letras minúsculas. →3.
    e. Claves con sólo letras minúsculas. →5.

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.**

    - Alguien que trabaja en una empresa y le van a despedir, haría lo posible para acceder a sus datos, con el fin de fastidiar a la empresa.
    - Si eres de una empresa y quieres acceder a los datos de otra empresa la cual te hace competencia, con el fin de robar datos, robarlos o incluso venderlos.
    - Si alguien te cae muy mal y quieres fastidiarle.
    - Una empresa para ver si su sistema el vulnerable.

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

Listado de control de acceso. Forma de determinar los permisos de acceso apropiados a un objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

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

Ofrece a los administradores la posibilidad de examinar todos los archivos protegidos para comprobar sus versiones, si descubre que un archivo se ha sobrescrito, recupera la versión correcta.

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

Física: ventiladores.
Lógica: cortafuegos, antivirus.

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

Filtrado de MAC, antivirus y cortafuegos.

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

Creo que cumplo con todo.

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

- password
- 123456
- qwerty

- abc123
- letmein
- monkey
- myspace1
- password1
- blink182
- (tu nombre)

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

-Cuantos más datos tenga en la empresa, mejor.

-Yo haría varias copias de seguridad de los datos y archivos de la empresa para asegurarme de no perderlos.

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.**

- Establecer objetivos claros que permitan la atención rápida de un accidente.
- Poner a encargados para activar el protocolo de evacuación.
- El encargado debe informar de la manera más precisa como actuar ante el desastre, indicar las salidas de emergencia, ayudar en todo lo que pueda, etc