EJERCIO 2 TEMA 1

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:** Capacidad que tiene uno para hacer que otra persona no pueda cambiar otro documento.
- **Autenticación:** La capacidad que tiene un ordenador, una web, etc. de identificar para demostrar que no eres un impostor, mediante una contraseña.
- **Cifrado:** Es la forma de codificado de un mensaje, para que solo los que sepan como se ha cifrado puedan leerlo.
- **No repudio:** Es que la comunicación no pueda ser negada ni por el emisor ni por el receptor. No repudio en origen, es que, el emisor no puede negar que ha existido esa comunicación. No repudio en destino, el receptor no puede negar que ha existido esa comunicación.
- **Riesgo:** Es la probabilidad que una amenaza se realice.
- **Desastres:** Cualquier evento (terremotos, explosiones....) que interrumpen los servicios o las operaciones.
- **Centro de proceso de datos:** Es un sitio donde se almacena y se procesan los datos.

Apartado 2.3
Ejercicio 1

1 caso: Una persona a la que vayan a despedir, con el fin de robar o destruir información de la empresa
2 caso: La propia empresa para comprobar si sus sistemas tienen vulnerabilidades
3 caso: Entre empresas rivales, para intentar que una empresa pueda robar información de la otra para usarla en su contra
4 caso: La policía para buscar a delincuentes con el fin de detenerlos
5 caso: Hacerse pasar por una persona para obtener su información privada

Apartado 2.3.2
Ejercicio 1

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 sí que muchos de la clase acaben siendo hacker porque no tienen maldad pero puede que haya alguno que sí vaya ha ser cracker

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** → Activo/Físico
b. **Detector de incendio.** → Pasivo/Físico
c. **Detector de movimientos** → Pasivo/Físico
d. **Cámara de seguridad** → Pasivo/Físico
e. **Cortafuegos** → Activo/Lógico
f. **SAI** → Pasivo porque previene que se apague el ordenador cuando se va la luz y activo porque elimina los picos de energía y evita los microcortes de luz/Físico
g. **Control de acceso mediante el iris del ojo.** → Activo/Físico
h. **Contraseña para acceder a un equipo** → Activo/Lógico
i. **Control de acceso a un edificio** → Físco/Activo

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

a. **Terremoto.** → Seguridad física
b. **Subida de tensión.** → Seguridad física
c. **Virus informático.** → Seguridad lógica
d. **Hacker.** → Seguridad lógica
e. **Incendio fortuito.** → Seguridad 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 en discos.** → Activo
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 segura porque es una palabra fácil de adivinar
b. caseta → No es segura porque es una palabra corta
c. c8m4r2nes → Es segura porque contiene números y letras
d. tu primer apellido → No es segura porque es de las primeras palabras que se utilizan para intentar averiguar una contraseña
e. pr0mer1s& → Es segura porque mezcla letras números y caracteres especiales
f. tu nombre → No es segura porque es de las primeras palabras que se utilizan para intentar averiguar una contraseña

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

a. **Claves con sólo números.** → 5
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.** → 4

Practicas

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 caso: Una persona a la que vayan a despedir, con el fin de robar o destruir información de la empresa
2 caso: La propia empresa para comprobar si sus sistemas tienen vulnerabilidades
3 caso: Entre empresas rivales, para intentar que una empresa pueda robar información de la otra para usarla en su contra
4 caso: La policía para buscar a delincuentes con el fin de detenerlos
5 caso: Hacerse pasar por una persona para obtener su información privada

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

Significa lista de control de acceso, se usa para fomentar la separación de privilegios, es una forma de determinar los permisos de acceso a algún archivo, comunicación, etc.

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

Es un comprobador de archivos y ofrece a los administradores la posibilidad de examinar todos los archivos protegidos para comprobar sus versiones

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

Lógica: Antivirus, cortafuegos
Físicas: Ventiladores, ventanas

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

Antivirus, cortafuegos y filtrado de MAC

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

No tengo SAI y no tengo componentes que pueden controlar los picos de energía

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

1) 123456
2) password
3) 12345678
4) qwerty
5) 12345

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?**

- Como son datos importantes y privados hay que protegerlos para que no se pierdan
- Tener varias copias de seguridad

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
- Tienen que haber unos encargados de activar el protocolo de evacuación
- Al recibir el comunicado el encargado tiene que informar de la manera más precisa como actuar, indicar las salidas de emergencia, etc