SI 2.2.1

- **La confidencialidad**: Hacer que la información solo llegue a las personas que autorizas.
- **Disponibilidad**: La información debe ser capaz de llegar a las personas que la requieran.
- **Autorización**: Tras autenticarse los usuarios tendrán ciertos privilegios.
- **Accounting**: Trata de hacer el seguimiento de las acciones que hace todo usuario registrado.
- **Vulnerabilidad**: Posibilidad de que el sistema sea atacado, lo mejor es tener siempre actualizado el software y hardware.
- **Impacto**: Rango que pueden llegar a abarcar los daños.
- **Plan de contingencia**: Políticas de seguridad a seguir, pero aun siguiendo las hay aun riesgo de desastre. Los principios son: Evaluación del peligro, planificar cómo lograr una recuperación total y pruebas para comprobar su eficacia y eficiencia.
-

SI 2.3

- 1º 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. Fingir ser otra persona para sacarle información del ordenador o las tarjetas
- 2. Interceptar una señal para poder ver los mensajes que envía
- 3.Introducir un software maliciosa que deje inservible el ordenador
- 4. Ataque de fuerza bruta para lograr la clave de algun archivo o cuenta
- 5. Almacenar la informacion de las teclas que pulsa para descubrir contraseñas

- 2º 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, pues posee los conocimientos necesarios, e incluso ya lo a hecho alguna vez

- 3º De cada uno de los elementos expuestos a continuación, indica a qué tipo de seguridad están asociado.

Ventilador de un equipo informático: Activa y físico

Detector de incendio: **Pasiva y físico**
Detector de movimientos: **Pasivo y físico**
Cámara de seguridad: **Pasivo y físico**
Cortafuegos: **Activo y lógico**
SAI: **Pasivo y físico**
Control de acceso mediante el iris del ojo: **Activo y físico**
Contraseña para acceder a un equipo: **Activo y lógico**
Control de acceso a un edificio: **Activo y físico**

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

Terremoto: **física**
Subida de tensión: **física**
Virus informático: **lógica**
Hacker: **lógica**
Incendio fortuito: **física**
Borrado de información importante: **lógica**

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

Antivirus: **Ambos**
Uso de contraseñas: **Activa**
Copias de seguridad: **Pasivo**
Climatizadores: **Activo**
Uso de redundancia en discos: **Pasivo**
Cámaras de seguridad: **Pasivo**
Cortafuegos: **Activo**

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

mesa: **no segura**
caseta: **no segura**
c8m4r2nes: **segura**
tu primer apellido: **no segura**
pr0mer1s&: **seguro**
tu nombre: **no seguro**

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

Claves con sólo números.**5**
Claves con números, letras mayúsculas y letras minúsculas.**2**
Claves con números, letras mayúsculas, letras minúsculas y otros caracteres. **1**
Claves con números y letras minúsculas.**3**
Claves con sólo letras minúsculas.**4**

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

Es una lista de control de acceso que controla el flujo del tráfico en equipos de redes

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

Es un comando que nos permite verificar la integridad de todos aquellos archivos importantes para el normal funcionamiento

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

Alarma de incendios: **físico**

Salida de emergencias: **físico**

Restricción de paginas Web: **Logico**

Extintor: **físico**

Ventiladores: **físico**

Copias de seguridad: **lógico**

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

Activas: Antivirus, ventiladores Pasiva: Antivirus, extintor

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

No instalar nada innecesario, usar certificados digitales y firmas digitales.

7. Busca en Internet las claves más comúnmente usadas.

12345678 y password

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?

A la privacidad. Hacer copias de seguridad para no perder la información de los clientes

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.

Anclar a los muros estanterías o armarios que puedan tumbarse, determinar zona de seguridad externa al recinto, desconectar aparatos encendidos, eléctricos o de gas