SI 2.2.1

- **Integridad:** Los datos no se pueden modificar sin el permiso del autor.
- **Autentificación:** Se intenta confirmar que una persona es quien dice ser.
- **Cifrado:** Se usa para codificar algo con una clave o algoritmo.
- **No repudio:** El emisor no puede negar la comunicación y el receptor no puede negar la comunicación, porque el emisor tiene pruebas de la recepción.
- **Riesgo:** Grado de exposición a una amenaza.
- **Desastres:** Evento accidental natural o malintencionado que interrumpe los servicios de una organización.
- **Centro de procesos de datos:** Lugar donde se procesan y almacenan datos.

SI 2.3

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. **Suplantación, hacerse pasar por YouTube o Gmail para requerir una recuperación de contraseña a alguna persona para cambiarle la contraseña y quedarme con sus datos.**
2. **Interrupción, hacer caer un servidor de un banco durante un período de tiempo a modo de amenaza.**
3. **Interceptación, realizar un *man in the middle* para conseguir información comprometida para una persona y luego chantajear.**
4. **Modificación, modificar un proyecto importante hecho por tí pero la empresa te ha despedido y se ha quedado todo el mérito.**
5. **Suplantación, hacerse pasar por Facebook o cualquier red social para modificar tus datos.**

SI. SEGURIDAD FÍSICA Y LÓGICA - EJERCICIOS

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.**
   Pienso que alguno podría llegar a ser Sniffer debido a sus conocimientos actuales.

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 - Física/Pasiva**
    c. **Detector de movimientos - Activa/Física**
    d. **Cámara de seguridad - Física/Pasiva**
    e. **Cortafuegos - Activa/Lógica**
    f. **SAI - Física/Pasiva**
    g. **Control de acceso mediante el iris del ojo - Física/Activa**
    h. **Contraseña para acceder a un equipo - Lógica/Activa**
    i. **Control de acceso a un edificio - Activo/Físico**

4. **Asocia las siguientes amenazas con la seguridad lógica y la seguridad física.**
    a. **Terremoto - Física**
    b. **Subida de tensión - Física**
    c. **Virus informático - Lógico**
    d. **Hacker - Lógico**
    e. **Incendio fortuito - Físico**
    f. **Borrado de información importante - Lógico**

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 - Pasiva**
    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 se puede averiguar fácilmente.**
    b. **caseta - No segura por el mismo motivo que ¨mesa¨.**
    c. **c8m4r2nes - Segura (no mucho) porque usa números y letras.**
    d. **tu primer apellido - No segura porque se puede averiguar fácilmente.**
    e. **pr0mer1s& - Segura porque usa letras, números y símbolos.**
    f. **tu nombre - No segura, porque se averigua fácilmente.**

7. **Ordena de mayor a menor seguridad los siguientes formatos de claves.**
   C - B - D - E - A

SI. SEGURIDAD FÍSICA Y LÓGICA - PRÁCTICAS

2. **Busca qué es una ACL, entiéndelo, y explícalo en clase.**
   ACL (Lista de control de acceso), permite controlar el flujo de tráfico en redes. Permite y deniega el tráfico de acuerdo a alguna condición. Sólo necesita saber quién eres y qué necesitas y te responde si tienes permiso o no de hacerlo.

3. **Busca qué es sfc, entiéndelo, y explícalo en clase.**
   Es un comando que analiza los archivos protegidos del sistema y reemplaza los archivos dañados en una copia almacenada en el caché.

4. **Describe los medios de seguridad física y lógica que hay en el aula.**
   Física -> extintor
   Lógica -> usuarios y contraseñas.

5. **Evalúa qué medidas de seguridad activa y pasiva tienes en torno a tu ordenador personal.**
   Activa -> contraseñas
   Pasiva ->

6. **Analiza qué pautas de protección no cumple el sistema que tienes en tu casa.**
   - **No instalar nada que no sea estrictamente necesario.**
   - **Revisar las configuraciones del software.**
   - **Gestionar y revisar los logs de las aplicaciones y el sistema operativo.**

7. **Busca en Internet las claves más comúnmente usadas.**
   123456
   password
   123

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?**
   Los datos afectan que si no hay buena seguridad podrían robarte los datos de muchas personas.
   Se tendrían que hacer copias de seguridad de los usuarios y la información.

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.**
   Para no perder la información de la organización lo mejor es tener copias de seguridad en un servidor externo lo cual si le ocurre algo a los equipos la información estará asegurada.