SI 2.2.1

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.**

- **Confidencialidad :** Poder transmitir información a un solo individuo o grupo sin que los demás se enteren.
- **Disponibilidad:** disponen de la información siempre que se necesite.
- **Autorización:** Una vez ya validado sus credenciales dispone de los medios asignados como usuario (lectura escritura ejecución).
- **Accounting:** Intentar hacer un seguimiento de las acciones que hace un usuario.
- **Vulnerabilidad:** es una brecha en el sistema que se pueden aprovechar para atacar pueden ser brechas conocidas o no y siempre urge la necesidad de corregirlas.
- **Impacta:** Es el resultado de un ataque.
- **Plan de contingencia:** En el caso de que ocurra algo, son la serie de medidas que se toman para paliar algo.

SI 2.3.1

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.**
   Todos en esta clase podemos ser atacantes, yo mismo puedo estar atacando te mientras lees esto, por eso estamos estudiando seguridad informática para poder saber que protecciones hay y saltarnos las sin ser detectados pero claro luego te vendo la protección contra otros como yo. Encajaría en el perfil de un hacker, no me gusta ir fastidiando a la gente porque puedo, pero yo creo que no hay muchas personas en la clase con un perfil de atacante, y si los hay serian como yo, a no ser que sea por venganza entonces sí que podrían querer fastidiar a alguien.

3. **De cada uno de los elementos expuestos a continuación, indica a qué tipo de seguridad están asociado (activa, pasiva, lógica y física)**
    - **Ventilador de un equipo informático.** Activo y físico.
    - **Detector de incendio.** Pasivo y físico.

- **Detector de movimientos.** Activo y físico.
- **Cámara de seguridad.** Activo, pasivo y físico.
- **Cortafuegos.** Activo y lógico.
- **SAI.** Activo, 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.

4. **Asocia las siguientes amenazas con la seguridad lógica y la seguridad física.**
   - **Terremoto.** Seguridad física
   - **Subida de tensión.** Seguridad física
   - **Virus informático.** Seguridad lógica
   - **Hacker.** Seguridad lógica
   - **Incendio fortuito.** Seguridad física
   - **Borrado de información importante.** Seguridad lógica.

5. **Asocia las siguientes medidas de seguridad con la seguridad activa o pasiva.**
   a. **Antivirus.** Seguridad activa y pasiva.
   b. **Uso de contraseñas.** Seguridad activa
   c. **Copias de seguridad.** Seguridad pasiva
   d. **Climatizadores.** Seguridad activa
   e. **Uso de redundancia en discos.** Seguridad pasiva
   f. **Cámaras de seguridad.** Seguridad activa y pasiva
   g. **Cortafuegos.** Seguridad activa.
6. **De las siguientes contraseñas indica cuales se podrían considerar seguras y cuáles no y por qué:**
   a. **mesa.** sería una mala contraseña solo de 4 caracteres, sin números ni mayúsculas, ni caracteres ni tampoco caracteres no alfanuméricos.
   b. **caseta.** sería una mala contraseña solo de 6 caracteres, sin números ni mayúsculas, ni caracteres ni tampoco caracteres no alfanuméricos.
   c. **c8m4r2nes.** Si tuviera mayúsculas y caracteres no alfanuméricos sería muy segura, es de más de 8 caracteres y alberga tanto letras como números
   d. **tu primer apellido.** A no ser que seas un droide de la guerra de las galaxias tu apellido puede ser todo lo largo que quieras pero no tendrá ni números ni caracteres no alfanuméricos, a demas que seria facil de sacar porque hay registros en bases de datos en todo el mundo donde está tu apellido, por lo que no es seguro.

e. **pr0mer1s&.** Sería una buena contraseña ya que es de más de 8 caracteres posé letras, números y caracteres no alfanuméricos y si tuviera mayúsculas, sería casi totalmente segura.
f. **tu nombre.** A no ser que seas un droide de la guerra de las galaxias tu nombre puede ser todo lo largo que quieras pero no tendrá ni números ni caracteres no alfanuméricos, a demas que seria facil de sacar porque hay registros en bases de datos en todo el mundo donde está tu nombre, por lo que no es seguro.

7. **Ordena de mayor a menor seguridad los siguientes formatos de claves.**
   a. **Claves con sólo números.** 5º
   b. **Claves con números, letras mayúsculas y letras minúsculas.** 2º
   c. **Claves con números, letras mayúsculas, letras minúsculas y otros caracteres.** 1º
   d. **Claves con números y letras minúsculas.** 3º
   e. **Claves con sólo letras minúsculas.** 4º

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.**
   Un programador que se ha quedado sin dinero, por culpa de un banquero sin escrúpulos que lo ha estafado y decide aplicar sus conocimientos de informática para hackear sus cuentas bancarias y quitárselo todo.
   Un hacker que hackea el móvil de una famosa para robarle fotos en las que sale desnuda.
   Una persona compra en una subasta un artículo de gran valor y una persona se entera, entra en su casa y se lo roba.
   Una exnovia con la que compartiste tu contraseña de una red social, se mete dentro para alterar tu perfil, por despecho.
   Un programador hacker el servidor de google para que se fijen en el y lo contraten.
2. **Busca qué es una ACL, entiéndelo, y explícalo en clase.**
   ACL(access control list) o lista de control de acceso es una base de datos donde se almacenan los diferentes logins y sus correspondientes privilegios, en mi caso lo mas parecido seria cuando haces un ls -l en linux para poder ver los permisos de escritura lectura y ejecución de los usuarios, grupos y otros.
3. **Busca qué es sfc, entiéndelo, y explícalo en clase.**
   Es una herramienta disponible sólo en windows que comprueba los archivos protegidos del sistema, como los archivos de sistema (.dll) y mira si están alterados.

4. **Describe los medios de seguridad física y lógica que hay en el aula.**
   Sistemas de seguridad física: La cerradura de la puerta, el detector de movimiento de la alarma, las bridas que enganchan los cables, el cajetín con cerradura que guarda la llave allen de las persianas.
   Sistemas de seguridad lógica: Las contraseñas alojadas en cada ordenador, la clave del router, los permisos que se dan a cada usuario.
5. **Evalúa qué medidas de seguridad activa y pasiva tienes en torno a tu ordenador personal.** En mi ordenador