SI 2.2.1

- **Integridad**:c*uando un dato no puede ser modificado sin permiso del autor*
- **Autenticación**: *Esta característica consiste en verificar que eres quien dices ser,que se puede realizar por ejemplo: mediante tarjeta,ID,contraseña o mediante de huella dactilar (biometria)*
- **Cifrado**: *es una manera en la que podemos proteger el mensaje por ejemplo:*
- *claves o códigos muy difícil de descifrar*
- **No repudio**: *para no poder negar que ha habido una conversación.Por ejemplo:grabar una llamada telefónica.*
- **Riesgos:** *Grado de exposición a que una amenaza se materialice.*
- **Desastre**: *Evento accidental,natural,o malintencionado*
- **Centro de procesos de datos:** *Lugar donde se almacenan y se procesan datos.*

SI 2.3.1

1. 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.

Hay un compañero de clase que puede ser un Sniffer,porque tiene mucho conocimiento sobre las redes.

2. 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:pasiva,física
    c. Detector de movimientos:pasiva,física
    d. Cámara de seguridad:pasiva,física
    e. Cortafuegos:activa,lógica
    f. SAI:activa,fisico
    g. Control de acceso mediante el iris del ojo:activo,fisico
    h. Contraseña para acceder a un equipo:activa,logica
    i. Control de acceso a un edificio:activa,fisica
3. Asocia las siguientes amenazas con la seguridad lógica y la seguridad física.
    a. Terremoto.FIsica
    b. Subida de tensión.Física
    c. Virus informático.Lógica
    d. Hacker.Lógica
    e. Incendio fortuito.Físico
    f. Borrado de información importante.Lógico
4. 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. Pasiva
d. Climatizadores.Activo
e. Uso de redundancia en discos.Pasiva
f. Cámaras de seguridad.Pasiva
g. Cortafuegos.Activa

5. De las siguientes contraseñas indica cuales se podrían considerar seguras y cuáles no y por qué:
    a. mesa.No porque hay un dicionario con todas las palabras usadas por el ser humano
    b. caseta.No porque hay un dicionario con todas las palabras usadas por el ser humano
    c. c8m4r2nes.Si porque esta es una palabra que no esta en ningún dicionario ya que no existe.
    d. tu primer apellido.Eso es una cosa que cualquiera puede saber
    e. pr0mer1s&:No porque hay un diccionario con todas las palabras usadas por el ser humano
    f. tu nombre Eso es una cosa que cualquiera puede saber
6. Ordena de mayor a menor seguridad los siguientes formatos de claves.
    a. Claves con sólo números.
    b. Claves con números, letras mayúsculas y letras minúsculas.
    c. Claves con números, letras mayúsculas, letras minúsculas y otros caracteres.
    d. Claves con números y letras minúsculas.
    e. Claves con sólo letras minúsculas.

c>b>d>e>a

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.

Uno que cree que su novia es infiel e intenta conseguir la contraseña de su Facebook para ver lo que esta ocurriendo en realidad.
Intentar conseguir la clave wifi para tener MB gratis
Conseguir la cuenta de algun juego que tenga una persona y pasarte sus objetos a tu cuenta
Usar la fuerza bruta para conseguir la tarjeta de credito y todo el dinero....
Hacer una pagina como Sabadell para sacar los datos bancarios de los cliente.

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

Restringir quien puede a acdecer a que cosa

Una lista de control de acceso o **ACL** es un concepto de seguridad informática usado para fomentar la separación de privilegios. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición. Sin embargo, también tienen usos adicionales, como por ejemplo, distinguir "tráfico interesante" (tráfico suficientemente importante como para activar o mantener una conexión) en RDSI.

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

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

Seguridad Física: lExtintores,ventiladores,luz de emergencia.

Seguridad Lógica:Contraseñas y Usuarios

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

Seguridad activa : Antivirus,firewall,antispyware,tapar la camara

Seguridad pasiva:copias de seguridad,Antivirus

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

Sistemas Físico no tengo un SAI para evitar las subidas de tensión

7. Busca en Internet las claves más comúnmente usadas.

- 123456
- password
- 12345678
- qwerty
- 12345
- 123456789
- football
- 1234
- 1234567
- baseball
- welcome
- 1234567890
- abc123
- 111111
- 1qaz2wsx
- dragon
- master
- monkey

- letmein
- login
- princess
- qwertyuiop
- solo
- passw0rd
- starwars

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?

Encriptar la información de los usuarios.

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.