SI 2.2.1

- **Integridad:** Capacidad de que los datos lleguen sin ser alterados.
- **Autenticación:** Permite que los que intentan acceder a la información deban de presentar credenciales que los autoricen, ya sea a través de información -usuario y contraseña- como de maneras físicas -escáner de retina-.
- **Cifrado:** Una técnica que nos permite encriptar o codificar un mensaje para que cualquiera que no posea la manera de descifrarlo, no lo pueda leer o ver.
- **No repudio:** El mensaje entre el emisor y el receptor queda confirmado, no se puede negar su existencia. Puede darse el no repudio en origen si el emisor no puede negar que el mensaje le haya llegado por pruebas que le presente el receptor, y el no repudio en destino es al contrario, el receptor no puede negar que el mensaje haya llegado porque el emisor le presenta pruebas.
- **Riesgo:** Es la probabilidad de que seas atacado al realizar una acción.
- **Desastres:** Los desencadenantes de una catástrofe, ya sea natural o accidental.
- **Centro de proceso de datos:** Un sitio, normalmente centralizado, donde se almacenan y procesan los datos.

6 Ejercicios

1. La respuesta está en SI 2.2.1.
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.
    a. Pienso que uno de mis compañeros podría convertirse en Cracker, especialmente para robar cuentas del WoW.
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 → Física Activa
    b. Detector de incendio → Física Activa
    c. Detector de movimientos → Física Activa
    d. Cámara de seguridad → Física Activa
    e. Cortafuegos→ Lógica Activa
    f. SAI → Física Activa y 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 → Física Activa
4. Asocia las siguientes amenazas con la seguridad lógica y la seguridad física.
    a. Terremoto. → Física
    b. Subida de tensión. → Fisica
    c. Virus informático. → Lógica

d. Hacker. → Lógica
e. Incendio fortuito. → 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. → Pasiva
    d. Climatizadores. → Activa
    e. Uso de redundancia en discos. → Pasiva
    f. Cámaras de seguridad. → Activa
    g. Cortafuegos. → Activa
6. De las siguientes contraseñas indica cuales se podrían considerar seguras y cuáles no y por qué:
    a. mesa → No es segura. Es una palabra simple, en minúsculas, que está en cualquier diccionario.
    b. caseta → Lo mismo que a.
    c. c8m4r2nes → Es segura. Son varias letras sin sentido, con números entre medias.
    d. tu primer apellido →No es segura. Los nombres y apellidos también están en los diccionarios.
    e. pr0mer1s& →Lo mismo que c. Esta contraseña también usa el caracter &.
    f. tu nombre → Lo mismo que d.
7. Ordena de mayor a menor seguridad los siguientes formatos de claves.
    a. Claves con sólo números. → Quinta
    b. Claves con números, letras mayúsculas y letras minúsculas. →Segunda
    c. Claves con números, letras mayúsculas, letras minúsculas y otros caracteres. → Primera
    d. Claves con números y letras minúsculas. →Tercera
    e. Claves con sólo letras minúsculas. →Cuarta

7 Prácticas

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.
    a. Alguien que te roba la cuenta del Facebook para borrarla, con el fin de fastidiar.
    b. Una persona que accede al móvil de otro para robarle fotos embarazosas y subirlas a internet.

    c. Acorrarlar a alguien en un cajero de manera física, y amenazarle con violencia para que saque dinero de su cuenta y se lo de.
    d. Instalar un keylogger en el ordenador de alguien para descubrir qué cuenta y contraseña utiliza en un juego online para robarla.
    e. Alguien que hace un man in the middle para sniffear los paquetes de una red y conseguir información clasificada.
2. Busca qué es una ACL, entiéndelo, y explícalo en clase.
    a. Se utiliza para separar privilegios. Filtran el tráfico de la red, concediendo o denegando acceso a los distintos objetos de la red en base a ciertas condiciones programadas.
3. Busca qué es sfc, entiéndelo, y explícalo en clase.
    a. Es una utilidad que se asegura de que los archivos no están modificados de ninguna forma que no haya sido registrada oficialmente. En caso de que ocurra, borrará el archivo sospechoso y buscará de nuevo el archivo sin modificar.
4. Describe los medios de seguridad física y lógica que hay en el aula.
    a. De medios físicos tenemos: extintores.
    b. De medios lógicos: contraseñas en los ordenadores.
5. Evalúa qué medidas de seguridad activa y pasiva tienes en torno a tu ordenador personal.
    a. De medidas activas tengo: contraseña en el ordenador.
    b. De medidas pasivas tengo: imagen de los discos duros que hago una vez al mes.
6. Analiza qué pautas de protección no cumple el sistema que tienes en tu casa.
    a. No tengo una temperatura adecuada en el cuarto durante las épocas de mayor calor.
7. Busca en Internet las claves más comúnmente usadas.
    a. 12345678, abc123, password, 11111111, blahblah, pokemon.
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?
    a. Habrá que formar a los trabajadores para que manejen la información confidencial de manera adecuada. Se tendrán que cifrar los datos para que incluso aunque se acceda a ellos de manera ilegal, no se puedan leer. Y por supuesto, tener medidas de seguridad en el servidor para deflectar los ataques en primer lugar.
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.
    a. "primeros intervinientes" (bomberos, policia,Cruz Roja, Proteccion Civil, etc.) que serán los que optimicen las medidas de protección y

eviten el empeoramiento de la situación, soliciten ayuda especializada si no se ha hecho, faciliten el acceso a los implicados, mantengan las funciones vitales aplicando las técnicas básicas e instrumentales de reanimación”