SI

EJERCICIOS

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.

- **integridad**: significa que un documento no puede ser modificado si el autor no quiere
- **autenticacion**: sirve para intentar saber que una persona, ordenador o entidad dice ser quien es y no un impostor. Puede ser mediante una tarjeta, usuario y contraseña o biometria.
- **cifrado:** mecanismo mediante la informacion se codifica con una clave para que sea invisible para los que no saben la contraseña y una algoritmo para poder descifrarla.
- **no repudio:** que la comunicacion entre emisor y receptor queden garatizadas, para que ninguno de los dos pueda negar que ha existido.
- **en origen:** el emisor no puede negar la comunicacion por que el receptor obtiene pruebas de la comunicacion
- **en destino**: el receptor no puede negar la comunicacion por que el emisor obtiene pruebas de la recepcion
- **riesgo**: es la posiblidad de que ocurra una amenaza
- **desastres:** cualquier accion malintencionada o natural que interrumpe las operaciones o servicios de una organizacion
- **centro de procesos de datos** : es un lugar donde procesar y almacenar los datos

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.

- newbie: yo creo que habrá algún newbie, ya que todos empiezan por hay.
- hackers: alguno sera un hacker por que trabajaran ayudando empresas buscando fallos de seguridad.
- lammers: habra gente que sera lammer por que quieren ser hackers pero no saben suficiente o simplemente no valen para ello.

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
    b. Detector de incendio.
    c. Detector de movimientos
    d. Cámara de seguridad
    e. Cortafuegos
    f. SAI
    g. Control de acceso mediante el iris del ojo.
    h. Contraseña para acceder a un equipo
    i. Control de acceso a un edificio

a. física y activa
b. física y activa
c. física y activa
d. física y activa
e. lógica y activa
f. física y pasiva
g. física y activa
h. lógica y activa
i. física y activa

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

a. fisica
b. física
c. lógica
d. física
e. física
f. lógica

5. Asocia las siguientes medidas de seguridad con la seguridad activa o pasiva.
    a. Antivirus.
    b. Uso de contraseñas.
    c. Copias de seguridad.
    d. Climatizadores.
    e. Uso de redundancia en discos.
    f. Cámaras de seguridad.
    g. Cortafuegos.

a. activa y pasiva
b. activa
c. pasiva
d. activa
e. pasiva
f. activa
g. activa

6. De las siguientes contraseñas indica cuales se podrían considerar seguras y cuáles no y por qué:
    a. mesa
    b. caseta
    c. c8m4r2nes
    d. tu primer apellido
    e. pr0mer1s&
    f. tu nombre

a. no, porque es muy corta y
b. no, porque es muy corta y
c. si, porque tiene letras y numeros
d. no, porque hay que evitar apellidos
e. si, porque usa caracteres que no son ni numeros ni letras
f. no, porque hay que evitar nombres

7. 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.

- phishing: alguien que quiera obtener la contraseña de un banco, crea una copia exacta o muy parecida de la pagina de un banco y te manda un correo tambien exacto o similar al del banco con un enlace a dicha pagina diciendo que hay algun fallo y que pongas tu contraseña o numero de cuenta y asi consigue tus datos y te roba tu dinero.

- denegacion de servicio: haces un envio masivo de datos a un servidor para tumbarlo, con el fin de intentar inutilizar una organizacion o empresa, o simplemente molestar.

- keyloggers: consiste en almacenar las pulsaciones del teclado o incluso hacer capturas de pantalla, y se puede usar para conseguir contraseñas, datos de una persona o empresa y luego usarlos para tu beneficio o usarlos para extorsionar al que le has sacado la informacion.

- spoofing: se puede usar para suplantar la identidad de un router y asi cuando el dueño vaya a conectarse, pone su contraseña y ya la puedes usar tu.

- conexion no autorizada: consiste en encontrar un fallo de seguridad en el sistema y una vez dentro sacar todos los datos que quieras y usarlos como quieras o extorsionar al propietario.

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

- una ACL (lista de control de acceso) es una lista, la cual permite o deniega el acceso a la red para determinadas redes o protocolos. lo hacen filtrando los encabezados de los paquetes IP de origen y destino en la capa 3 y el tipo de protocolo usado y números de puerto en la capa 4.

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

- Comprobador de archivos de sistema ofrece a los administradores la posibilidad de examinar todos los archivos protegidos para comprobar sus versiones

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

- **seguridad fisica:**
- extintores

- **seguridad logica:**
- copias de seguridad
- contraseñas

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

- **seguridad pasiva:**
- contraseña
- antivirus

- **seguridad activa:**
- antivirus

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

- no tengo copia de seguridad
- si se va la luz se puede romper

7. Busca en Internet las claves más comúnmente usadas.

1. 123456
2. password
3. 12345678
4. lifehack

5. qwerty
6. abc123
7. 11111
8. monkey
9. consumer
10. 12345

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?

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.