SI 6. 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: No se pueden cambiar los datos sin el consentimiento del autor o creador.
    Autenticación: Significa que tienes que verificar que eres real, cuantos más métodos de verificación tenga, mas seguro es.
    Cifrado: Es como ponerle una contraseña a un mensaje, o a la información, y al no verificar dicha información se hace ilegible o imposible de acceder.
    No repudio: Confirma la comunicación entre un emisor y un receptor, hay dos tipos; en origen, que viene a referirse a que el emisor es el que no puede negarse, porque queda reflejado; y en destino, que en este caso es al revés, el receptor no puede negarse a reconocerlo.
    Riesgo: Nivel de peligro a que se produzca un ataque.
    Desastres: Incidente natural que no deja seguir el trabajo.
    Centro de proceso de datos: Lugar donde se guarda toda la información. (Servidor o Dominio).

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.

    Si, uno de ellos podría ser Sniffer, porque tiene facilidad con el tema de las redes y a parte con algo de seguridad. Y Hacker, porque tiene bastantes conocimientos sobre la seguridad informática.

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 y Física.
    b. Detector de incendios: Pasiva y Física.
    c. Detector de movimientos: Pasiva y Física.
    d. Cámara de seguridad: Pasiva y Física.
    e. Cortafuegos: Activa y Lógica.
    f. SAI: Pasiva y Física.
    g. Control de acceso mediante el iris del ojo: Activa y Física.
    h. Contraseña para acceder a un equipo: Activa y Lógica.
    i. Control de acceso a un edificio: Activa y Física.
4. Asocia las siguientes amenazas con la seguridad lógica y la seguridad física.
    a. Terremoto: Física.
    b. Subida de tensión: Física.
    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: 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.
    b. caseta: No segura.
    c. c8m4r2nes: Segura.
    d. tu primer apellido: No segura.
    e. pr0mer1s&: Segura.
    f. tu nombre: No segura.
7. Ordena de mayor a menor seguridad los siguientes formatos de claves.
    a. Claves con sólo números: 5
    b. Claves con números, letras mayúsculas y letras minúsculas: 2
    c. Claves con números, letras mayúsculas, letras minúsculas y otros caracteres: 1
    d. Claves con números y letras minúsculas: 3
    e. Claves con sólo letras minúsculas: 4

SI 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. Un virus, por ejemplo un keylogger, para sacar información del ordenador, y conseguir la cuenta de un banco para sacar dinero.
    b. Crackear una clave wifi mediante una taque de fuerza bruta, para conectarse a una red sin pagar una tarifa mensual.
    c. Saturar un servidor, para conseguir tumbarlo. Un ejemplo sería una empresa que tiene competencia y le interesa que solo funcione su servicio.
    d. Suplantar la identidad de alguien, para sacar información de una empresa.
    e. Crear una página similar a la que hace pagos regularmente, para engañar a esa persona y sacarle dinero.

2. Busca qué es una ACL, entiéndelo, y explícalo en clase.
   Es una lista de control de acceso, es decir, una lista que almacena el tráfico de datos, indicando los permisos de cada dato, permitiendo controlar el tráfico en la red.

3. Busca qué es sfc, entiéndelo, y explícalo en clase.
   Es un comando que se utiliza para analizar los archivos de windows y evitar el formateo del sistema por infección de virus.

4. Describe los medios de seguridad física y lógica que hay en el aula.
   Física: Alarma de incendios, Ventiladores, Extintor.
   Lógica: Antivirus, Restricción de páginas web, Copia de seguridad.

5. Evalúa qué medidas de seguridad activa y pasiva tienes en torno a tu ordenador personal.
   Activa: Contraseñas, Encriptación, Antivirus.
   Pasiva: Copia de seguridad.

6. Analiza qué pautas de protección no cumple el sistema que tienes en tu casa.
   Gestionar y revisar los logs de las aplicaciones y el sistema operativo, Avisos por SMS o eMail para informarnos de ataques y Tener listas de control de acceso (ACL)

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

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 afectan estos datos a la formación de tu empresa? ¿Qué medidas de seguridad tendrás que tomar cuando almacenamos esta información?
   Afecta a la privacidad de los datos de la empresa, como medida, haría copias de seguridad y cifraría la información importante.

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.

   Caso de incendio: Solo si estas capacitado, usar el extintor, si no, se avisará a los bomberos (de esto se encarga la persona que esté al mando en estas operaciones de emergencia). Hay que cortar la corriente y los suministros de gas. La evacuación debe ser en fila y por el lado derecho de la ruta de emergencia, para dar paso en el lado izquierdo a las operaciones de los especialistas.

   Para no perder la información, contrataría un servidor a una empresa de estos, para duplicar mi información, haciendo una copia de seguridad de los datos.