SI 2.2. Ejercicio 1

La Confidencialidad: Es hacer llegar la información a una persona y no a personas no autorizadas.

Disponibilidad: Es que la información esté siempre disponible cuando se necesite.

Autorización: Cuando los usuarios están autenticados tienen una serie de privilegios sobre la información, acceso, lectura, escritura, ejecución y modificación.

Accounting: Hace un seguimiento de todas las acciones que hace un usuario registrado.

Vulnerabilidad: Punto débil del sistema que se puede usar en su contra. Se recomienda actualizar siempre el software y hardware.

Impacto: El alcance del daño causa de un ataque.

Plan de contingencia: Medidas de prevención en el sistema.

-Evaluación de peligro.

-Planificar una recuperación total.

-Pruebas de eficiencia y eficacia.

SI 3.2 Ejercicio 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.

-Creo que en clase hay un par de Lamers y no creo que ninguno quiera ser un Cracker.

1. 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-Lógica
    g. Control de acceso mediante el iris del ojo. Activa-Lógica
    h. Contraseña para acceder a un equipo. Activa-Lógica
    i. Control de acceso a un edificio. Activa-Física
2. 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. Lógico
3. 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

4. De las siguientes contraseñas indica cuales se podrían considerar seguras y cuáles no y por qué:
   a. mesa No porque hay un diccionario que tiene guardas palabras.
   b. caseta No porque hay un diccionario que tiene guardas palabras.
   c. c8m4r2nes Si
   d. tu primer apellido No porque hay un diccionario que tiene guardas palabras.
   e. pr0mer1s& Si
   f. tu nombre No porque hay un diccionario que tiene guardas palabras.
5. Ordena de mayor a menor seguridad los siguientes formatos de claves.
   a. Claves con sólo números. 4
   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. 5

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.
   Interrupción: Cortar la emisión de un servidor. Ejm: Cortar la emisión de un streaming.
   Interceptación:Recoger información mediante un keylogger (programa que recoge contraseñas) o crear una aplicación donde pueda coger capturas de pantalla.
   Modificación: Modificar los datos que se han conseguido después de la interceptación de datos. Ejm editar un documento.
   Fabricación o Suplantación: Alguien que se hace pasar por alguna identidad, y te envía un email. Ejm hacerse pasar por una entidad bancaria.
2. Busca qué es una ACL, entiéndelo, y explícalo en clase.
   Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.
   Concepto de Seguridad Informática, que controla el flujo de tráfico en equipos de Red, permite y deniega el tráfico de red.
3. Busca qué es sfc, entiéndelo, y explícalo en clase.
   El comando **sfc /scannow**, lo que hace es comprobar la integridad de los ficheros protegidos del sistema Windows, y repararlos en caso de que presenten algún tipo de corrupción o anormalidad.
4. Describe los medios de seguridad física y lógica que hay en el aula.
   Física: Extintor por posible incendio.
   Lógica: Contraseña para cada usuario.
5. Evalúa qué medidas de seguridad activa y pasiva tienes en torno a tu ordenador personal.

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

7. Busca en Internet las claves más comúnmente usadas.
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.