Tema 1 ejercicio 1

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:** Es la forma de hacer que una información no se pueda modificar sin el consentimiento de su autor.
- **Autenticación:** Es una técnica para confirmar la autenticidad de algo mediante cosas como una tarjeta, nombres de usuario, etc.
- **Cifrado:** Es un mecanismo para codificar un mensaje con un nuevo lenguaje el cual lo hace ininteligible si no tienes las herramientas adecuadas para descifrar ese lenguaje.
- **No repudio:** La comunicación entre emisor y receptor para que quede garantizada y que no se pueda negar su existencia.
    - No repudio en origen: El emisor no puede negar la comunicación porque a la otra persona se le envían pruebas de dicha conversación
    - No repudio en destino: El receptor no puede negar la comunicación porque la otra persona tiene pruebas de que ha recibido esa información.
- **Riesgo:** Estimación de las probabilidades que hay de que ocurra una amenaza
- **Desastres:** Eventos los cuales pueden ser casuales o no e interrumpen tus operaciones o servicios.
- **Centro de procesos de datos:** Lugar donde se utiliza y guarda información.

Tema 1 ejercicio 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.

- En la clase considero que bastante gente puede acabar siendo cracker viendo su personalidad, también hay algunos que es probable que acaben siendo programadores de malware

Tema 1 ejercicio 3

De cada uno de los elementos expuestos a continuación, indica a qué tipo de seguridad están asociado (activa, pasiva, lógica y física)

-Ventilador de un equipo informático **->** Físico y activo
-Detector de incendio. **->** Físico y pasivo
-Detector de movimientos **->** Físico y pasivo
-Cámara de seguridad **->** Físico y activo
-Cortafuegos **->** Lógico y activo
-SAI **->** Físico y activo/pasivo
-Control de acceso mediante el iris del ojo. **->** Físico y activo
-Contraseña para acceder a un equipo **->** Lógico y activo
-Control de acceso a un edificio **->** Físico y activo

Tema 1 ejercicio 4

Asocia las siguientes amenazas con la seguridad lógica y la seguridad física.

-Terremoto. **->** Físico
-Subida de tensión. **->** Físico
-Virus informático. **->** Lógico
-Hacker. **->** Físico
-Incendio fortuito. **->** Físico
-Borrado de información importante. **->** Lógico

Tema 1 ejercicio 5

Asocia las siguientes medidas de seguridad con la seguridad activa o pasiva.

-Antivirus. **->** Activo y pasivo
-Uso de contraseñas. **->** Activo
-Copias de seguridad. **->** Pasivo
-Climatizadores. **->** Pasivo
-Uso de redundancia de discos. **->** pasivo
-Cámaras de seguridad. **->** Activo
-Cortafuegos. **->** Activo

Tema 1 ejercicio 6

De las siguientes contraseñas indica cuales se podrían considerar seguras y cuáles no y por qué:

-mesa **->** No es segura, contraseña corta sin caracteres especiales o números.

-caseta **->** No es segura, contraseña corta sin caracteres especiales o números.

-c8m4r2nes **->** No es segura, contraseña corta sin caracteres especiales

-tu primer apellido **->** No es segura, contraseña corta sin caracteres especiales o números, además fácil de adivinar

-pr0mer1s& **->** Segura, mezcla caracteres normales, especiales y números

-tu nombre **->** No es segura, contraseña corta sin caracteres especiales o números, además fácil de adivinar

Tema 1 ejercicio 7

Ordena de mayor a menor seguridad los siguientes formatos de claves.

-Claves con sólo números. 4

-Claves con números, letras mayúsculas y letras minúsculas. 2

-Claves con números, letras mayúsculas, letras minúsculas y otros caracteres. 1

-Claves con números y letras minúsculas. 3

-Claves con sólo letras minúsculas 5

Tema 1 práctica 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.

- Robar tu dinero en un cajero automático para obtener tu contraseña y robarte dinero
- Entrar en la red de una empresa para robar información
- Hacer que los ordenadores de una empresa vayan lentos para que no puedan desempeñar su trabajo con regularidad, por motivo de que le hayan despedido
- Infectar ordenadores ajenos para hacer ataques DDoS a empresas
- Crear un programa de fuerza bruta para conseguir contraseñas de wifi y tenerlo gratis

Tema 1 práctica 2

Busca qué es una ACL, entiéndelo, y explícalo en clase.
(Lista de control de acceso) Es una lista que se usa generalmente para la separación de privilegios, esta lista determinará si el usuario puede hacer dicha tarea

Tema 1 práctica 3
Busca qué es sfc, entiéndelo, y explícalo en clase.
És un comando que se usa para la comprobación de archivos protegidos y verifica las versiones

Tema 1 práctica 4
Describe los medios de seguridad física y lógica que hay en el aula.
Física: ventana, extintor, caja del switch
Lógica: ACL

Tema 1 práctica 5
Evalúa qué medidas de seguridad activa y pasiva tienes en torno a tu ordenador personal.
Pasiva: SAI, antivirus
Activa: Contraseña, antivirus, zona ventilada

Tema 1 práctica 6
Analiza qué pautas de protección no cumple el sistema que tienes en tu casa.
yo creo que están bien

Tema 1 práctica 7
Busca en Internet las claves más comúnmente usadas.
1234,el nombre, el apellido, fecha de nacimiento, nombre de mascota.

Tema 1 práctica 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?
Son datos privados y muy importantes y se deben de proteger a toda costa porque sino te puedes hayar en un serio problema.
Proteger esos datos y no tenerlos en un solo lugar almacenados, tener varias copias de seguridad

Tema 1 práctica 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.

Es un proceso de recuperación que cubre los datos sobre el hardware y el software, se utiliza para que la empresa no pierda datos importantes y se vea comprometida.

-Tener un camino y unas pautas a seguir en caso de desastre natural y tener unos encargados que guiarán al grupo.

-Para ello la información debe estar almacenada en varios lugares, por si en un sitio se pierde poderla recuperar fácilmente.

-También es importante tener unos encargados de hacer las tareas de recuperación y almacenamiento.