SI 2.2.1

- ***Integridad:*** La integridad es el hecho de que los datos no puedan ser eliminados o modificados por otros usuarios no autorizados.

- ***Autenticación:*** Es la característica que identifica a cada usuario y comprueba que sea él mismo y no otro usuario no autorizado o uno que esté suplantando su identidad.

- ***Cifrado:*** El cifrado consiste en codificar un mensaje, escribirlo en clave de manera que nadie que no tenga acceso a la clave pueda leerlo o descifrarlo.

- ***No repudio:*** Garantiza que ha existido una comunicación entre el emisor y el receptor

- ***Riesgo:*** Es la probabilidad de que una amenaza cause daños.

- ***Desastres:*** Eventos que interrumpen una operación o servicio

- ***Centro de proceso de datos:*** Es un sitio centralizado donde se procesan o se almacenan los datos.

SI 2.3

Ejercicio 1

- 1 Suplantación de identidad de un ordenador para conseguir datos de la víctima
- 2 Ataque de fuerza bruta para averiguar un contraseña de un usuario y acceder a su cuenta.
- 3 Introducción de un programa malintencionado para que se cuele en el sistema y sacar los datos del usuario.
- 4 Buscar un agujero de seguridad para entrar al sistema
- 5 Realizar muchas solicitudes a un servidor para tumbarlo

SI 2.3.2

Ejercicio 2

Si que hay alguien que pueda responder porque tiene muchos conocimientos sobre la seguridad informática y tiene una mente capaz de hacerlo.

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 física
b. Detector de incendio. Pasivo física

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

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

j. Terremoto. Física
k. Subida de tensión. Física
l. Virus informático. Lógica
m. Hacker. Lógica
n. Incendio fortuito. Física
o. Borrado de información importante. Lógica

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

p. Antivirus. Activa
q. Uso de contraseñas. Activa
r. Copias de seguridad. Pasiva
s. Climatizadores. Activa
t. Uso de redundancia en discos. Pasiva
u. Cámaras de seguridad. Pasiva
v. Cortafuegos. Activa

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

w. mesa No segura
x. caseta No segura
y. c8m4r2nes Segura
z. tu primer apellido No segura
aa. pr0mer1s& Segura
bb. tu nombre No segura

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

cc. Claves con sólo números. 5
dd. Claves con números, letras mayúsculas y letras minúsculas. 2
ee. Claves con números, letras mayúsculas, letras minúsculas y otros caracteres. 1
ff. Claves con números y letras minúsculas. 3
gg. Claves con sólo letras minúsculas. 4

7 Prácticas

1.

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

ACL es una lista de control de acceso que permite controlar el flujo entre equipos y su principal objetivo es controlar el tráfico permitiéndolo o denegándolo

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

Es un comando que sirve para comprobar archivos en windows y repara los archivos si están dañados.

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

Alarma de incendios: Físico
Salida de emergencia: Físico
Restricción de páginas web: Lógico
Extintor: Físico
Ventiladores: Físico
Copia de seguridad: Lógico

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

Activas: antivirus, ventiladores Pasivas: antivirus, extintor

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

Revisar la lista de usuarios autorizados.

7. Busca en Internet las claves más comúnmente usadas.

La clave mas usada es 123456 o el nombre del usuario

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?

Afectan a la privacidad. Se tienen que tomar medidas como por ejemplo copias de seguridad, sistemas de discos RAID, etc.

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.

Realizar regularmente copias de seguridad y usar un sistema RAID

Seguir un protocolo de actuación en caso de descargas eléctricas y otro protocolo de actuación frente a sismos.