

Ejercicios Seguridad física y lógica.

2.2 Definiciones

- Integridad: Solo posible editar una información con el permiso del autor.
- Autenticación: Demostrar o verificar que ese ordenador/persona es quien dice ser.
- Cifrado: Manera de codificar una información para que solo el que entienda ese código/idioma pueda leer la información.
- No repudio: Capacidad, que garantiza o demuestra que el emisor y el receptor han enviado o recibido una información.
- Riesgo: Probabilidad de que una amenaza se efectue.
- Desastres: Cualquier problema o circunstancia que interrumpe un proceso.
- Centro de proceso de datos: Lugar donde se procesan los datos.

2.3 Amenazas

1. Una empresa hace un “man in the middle” a la empresa que le hace competencia para espiar y robar información.
2. Un cracker tira los servidores de Playstation Network con el fin de hacer daño.
3. Una persona hace un “man in the middle” en un bar para conseguir toda la información personal de la gente que había conectada.
4. Una persona hace una página de phishing que imita la página de un banco, para robar el número de las tarjetas y sus claves de los clientes.
5. Un cracker crea un troyano e infecta a muchas personas para espiarlos y saber datos personales.

Apartado 6 Ejercicios

2. En esta clase yo pienso que podría haber algún cracker o hacker. Porque a día de hoy ya intentan cosas que hacen los hackers y los crackers.

3.

a.Ventilador de un equipo informático > Activo. Físico

b.Detector de incendio > Pasivo. Físico

c.Detector de movimientos > Activo. Físico

- d. Cámara de seguridad > Activo. Físico
- e. Cortafuegos > Pasivo. Lógico
- f. SAI > Pasivo. Físico
- g. Control de acceso mediante el iris del ojo > Activo. Físico
- h. Contraseña para acceder a un equipo > Activo. Lógico
- i. Control de acceso a un edificio > Activo. Físico

4.

- a. Terremoto > Seguridad física
- b. Subida de tensión. > Seguridad física
- c. Virus informático > Seguridad lógica
- d. Hacker > Seguridad lógica
- e. Incendio fortuito > Seguridad Física
- f. Borrado de información importante > Seguridad Lógica

5.

- a. Antivirus > Seguridad Activa
- b. Uso de contraseñas > Seguridad Activa
- c. Copias de seguridad > Seguridad pasiva
- d. Climatizadores > Seguridad Activa
- e. Uso de redundancia en discos > Seguridad pasiva
- f. Cámaras de seguridad > Seguridad Activa
- g. Cortafuegos > Seguridad activa

6.

- 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 menos seguridad.

- c. Claves con números, letras mayúsculas, letras minúsculas y otros caracteres.
- b. Claves con números, letras mayúsculas y letras minúsculas.
- d. Claves con números y letras minúsculas.
- e. Claves con letras minúsculas
- a. Claves con solo números.

7. PRÁCTICAS

1. Una empresa hace un “man in the middle” a la empresa que le hace competencia para espiar y robar información.
2. Un cracker tira los servidores de Playstation Network con el fin de hacer daño.
3. Una persona hace un “man in the middle” en un bar para conseguir toda la información personal de la gente que había conectada.
4. Una persona hace una página de phishing que imita la página de un banco, para robar el número de las tarjetas y sus claves de los clientes.
5. Un cracker crea un troyano e infecta a muchas personas para espiarlos y saber datos personales.

2. ACL: Es una lista en la que tu decides que permisos tiene cada usuario o persona que haya conectada.

3. sfc : “Comprobador de archivos de sistema”, lo que hace es comprobar que todos los archivos protegidos del sistema no hayan sido sobreescritos o cambiados, y si es así cambiarlos por los que venían originalmente.

4.

Puerta: seguridad física

Ventanas: seguridad física

Contraseñas de los ordenadores: seguridad lógica

Ventilador del ordenador: seguridad físico

Cortafuegos de los ordenadores: seguridad lógica

5.

Seguridad física: ventiladores del pc,

Seguridad lógica: Cortafuegos.

6. No tengo antivirus, no tengo contraseña en mi usuario del PC, no tengo copias de seguridad, no tengo SAI, no tengo el filtrado MAC activado en mi router.

7.

123456
password
123456789
nombre
qwertyuiop
abc1234

8. ¿En qué afecta estos datos a la formación de tu empresa? - Afecta en que tendrías que tener unos servidores de gran capacidad.

¿Qué medidas de seguridad tendrás que tomar cuando almacenamos esta información? Hacer copias de seguridad cada cierto tiempo para tener la información por si ocurre algún ataque.

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.