

Ejercicios:

Ejercicio 2:

- La integridad: Que no puedes cambiar sin que el autor te de permisos
- Autenticación: Es una característica, una persona o máquina decide ser quien es, no hay impostores
- cifrado: Mensaje ocultado mediante una clave haciendo ilegible a los que no la conocen la clave
- No repudio: Que la comunicación quede garantizada como que a existido
- Riesgo: Grado en el que estás expuesto a una amenaza
- Desastre: Cualquier acto accidental que interrumpe una operación o servicio de una organización
- Centro de proceso de datos: El lugar donde se almacenan y/o procesan los datos

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.

- Una interrupción para coger información de una empresa competidora
- Modificación para cambiar la información del programa para no tener que pagar por sus servicios
- Suplantación para coger información de alguien que quieras
- Intercepción para copiar información de la empresa enemiga o de alguien
- una interrupción para robar información de un enemigo

1. Piensa en los perfiles que se acaban de mencionar, ¿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.

Yo pienso que pero no para hacer el mal a nadie si no por diversión porque ahora mismo ya muestra interés por el tema y le gusta intentarlo y investigar

2. 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 incendio.: Pasiva y física
 - c. Detector de movimientos: Pasiva y física
 - d. Cámara de seguridad: Pasiva y física
 - e. Cortafuegos: Pasiva y lógica
 - f. SAI: Activa, 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
3. 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
4. Asocia las siguientes medidas de seguridad con la seguridad activa o pasiva.
- a. Antivirus.:Activa
 - b. Uso de contraseñas.: Activa
 - c. Copias de seguridad.: Pasiva
 - d. Climatizadores.:Activa
 - e. Uso de redundancia de discos.:Pasiva
 - f. Cámaras de seguridad.:Activa
 - g. Cortafuegos.Pasiva
5. De las siguientes contraseñas indica cuales se podrían considerar seguras y cuáles no y por qué:
- a. mesa: No es segura porque no tiene 8 caracteres mínimos
 - b. caseta: no es seguro porque no tiene 8 caracteres mínimo es insegura
 - c. c8m4r2nes: Es segura porque tiene más de 8 caracteres y mezcla números y letras
 - d. tu primer apellido: No es seguro poner tu nombre o fechas de algo importante como cumpleaños son muy predecibles, no es segura
 - e. pr0mer1s&:Es seguro porque mezcla números y letras y tienes más de ocho caracteres
 - f. tu nombre: no es seguro poner tu nombre ni apellidos en una contraseña no sería seguro
6. Ordena de mayor a menor seguridad los siguientes formatos de claves.
- a. Claves con sólo números.:1
 - b. Claves con números, letras mayúsculas y letras minúsculas.:4

- c. Claves con números, letras mayúsculas, letras minúsculas y otros caracteres.:5
- d. Claves con números y letras minúsculas.:3
- e. Claves con sólo letras minúsculas.:2

Prácticas:

7. 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. Robar información de la empresa en la que lo han despedido
 - b. Espiar un ordenador de alguien que quieras chantajear
 - c. Robar información para venderla a la competencia
 - d. Entrar en otro ordenador para conseguir contraseñas de cuentas bancarias
 - e. Entrar en otro ordenador para robar su identidad

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

Un listado donde pone los permisos que tiene cada usuario, en carpetas, archivos, usar ciertos comandos...

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

es un comando que comprueba que un archivo está sobrescrito lo repara

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

los ventiladores del aula y de los ordenadores como seguridad física

los proxy de conselleria como seguridad lógica

copias de seguridad de los sistemas como seguridad lógica

los extintores como medios físico

las contraseñas en los equipos

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

Los ventiladores del ordenador, las copias de seguridad que se hacen del sistema, las contraseñas para que solo tenga yo acceso.

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

No tengo copia de seguridad

13. Busca en Internet las claves más comúnmente usadas.

123456, password, 12345678, qwert y 12354

14. 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?

Que tienes que tener una base de datos, tenemos que tener en cuenta que es información confidencial de las personas y no podemos dejar que las roben, hay que tener una buena seguridad. También una copia de seguridad de toda la información. La información que tenemos no la podemos usar como queramos tiene que estar acorde con la ley. sería recomendable tener la información encriptada.

15. 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.

Actúan ambulancias, personal médico, policías y también vehículos para trasladar a los heridos . Siempre tiene que estar alguien de guardia. si hay algún fallecido no se puede mover. Los operarios tienen que ir con uniforme de vivos colores y tiras reflectantes para ser vistos a grandes distancias. Según las lesiones de los heridos se les clasifica por colores según la gravedad. Si es en una oficina tienen que ir a la calle o a algún lugar habilitado.

