## ***Tema 1***

### **Ejercicio 1.-**

**Ve al apartado del tema donde se ofrecen una serie de definiciones como integridad, confidencialidad, no repudio, …**

# Ponte de acuerdo con un compañero/a de clase.

# Uno de los/las dos deberá leer las definiciones pares y el otro las impares.

# Una vez hecho esto, cada uno deberá explicarle a la otra persona las definiciones que ha leído y tendrás que:

# Escribir lo que has entendido en el cuaderno de clase.

# Explicar una de ellas en clase, para ver que efectivamente lo has entendido.

* **La confidencialidad**: Hacer que sólo la persona que yo elija pueda ver los documentos.
* **Disponibilidad**: Que la información sea capaz de llegar a quien lo necesite.
* **Autorización**: Una vez ya autenticado, es la capacidad que tiene para modificar archivos...
* **Accounting**: Seguir los movimientos de una persona registrada
* **Vulnerabilidad**: Es el defecto de un sistema que se puede utilizar para atacarlo.
* **Impacto**: Cantidad de daño que se ha producido en un ataque.
* **Plan de contingencia**: Medidas de seguridad para prevenir que a un sistema le pueda afectar algún desastres, pero algunas veces ocurren esos desastres.
  + Cómo evaluar peligros.
  + Planificar actuaciones para recuperar datos perdidos.
  + Hacer simulacros.

### ***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.**

1.- Alguien al que vayan a despedir en la empresa y quiera borrar ciertos datos simplemente para molestar por rencor

2.- Gente del gobierno que quiera información de otro gobierno

3.- La policía para detectar ciertos casos como podría ser la pornografía infantil

4.- Una empresa para comprobar si sus sistemas son suficientemente seguros

5.- Hacerse pasar por una persona o entidad para obtener datos personales, como cuentas del banco, dni…

### ***Ejercicio 2.1.-***

**¿Crees que alguno de los compañeros de clase acabará siendo una persona a la que aplicar alguno de los términos anteriores?**

Probablemente alguno de clase acabe siendo programador de malware, alguno, pero lo veo menos probable, acabe siendo hacker, y yo, por ejemplo, iba para cracker pero de momento soy un newbie completamente.

### ***Ejercicio 3.-***

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

* 1. Ventilador de un equipo informático - Activo/Físico
  2. Detector de incendio - Pasivo/Físico
  3. Detector de movimientos - Activo/Físico
  4. Cámara de seguridad - Activo/Físico
  5. Cortafuegos - Activo/Lógico
  6. SAI - Activo y Pasivo/ Físico
  7. Control de acceso mediante el iris del ojo - Activo/Físico
  8. Contraseña para acceder a un equipo - Activo/Físico
  9. Control de acceso a un edificio - Activo/Físico

### ***Ejercicio 4.-***

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

* 1. Terremoto.
  2. Subida de tensión.
  3. Virus informático.
  4. Hacker.
  5. Incendio fortuito.
  6. Borrado de información importante.

### ***Ejercicio 5.-***

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

* 1. Antivirus - Activo y Pasivo
  2. Uso de contraseñas - Activo
  3. Copias de seguridad - Pasivo
  4. Climatizadores - Activo y Pasivo
  5. Uso de redundancia de discos - Activo
  6. Cámaras de seguridad - Activo
  7. Cortafuegos - Activo

### ***Ejercicio 6.-***

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

* 1. mesa - No segura, es una palabra de tan solo 4 letras
  2. caseta - No segura, es una palabra de tan solo 4 letras
  3. c8m4r2nes - No segura, tan sólo contiene números y letras
  4. tu primer apellido - No segura, es una tan sólo palabra
  5. pr0mer1s& - Segura, contiene caracteres especiales
  6. tu nombre - No segura, es una tan sólo palabra

### ***Ejercicio 7.-***

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

* 1. Claves con sólo números - 1
  2. Claves con números, letras mayúsculas y letras minúsculas - 3
  3. Claves con números, letras mayúsculas, letras minúsculas y otros caracteres - 4
  4. Claves con números y letras minúsculas - 2
  5. Claves con sólo letras minúsculas - 1

## 7 - Prácticas

### ***Ejercicio 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.***

* Alguien al que vayan a despedir en la empresa y quiera borrar ciertos datos simplemente para molestar por rencor
* Gente del gobierno que quiera información de otro gobierno
* La policía para detectar ciertos casos como podría ser la pornografía infantil
* Una empresa para comprobar si sus sistemas son suficientemente seguros
* Hacerse pasar por una persona o entidad para obtener datos personales, como cuentas del banco, dni…

### ***Ejercicio 2.-***

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

Lista de Control de Acceso. Una forma de determinar los permisos de acceso apropiados a un fichero específico

### ***Ejercicio 3.-***

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

Es un comprobador de archivos de sistema que ofrece al administrador la posibilidad de examinar los archivos protegidos.

### ***Ejercicio 4.-***

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

Lógica: Firewall, antivirus, la protección a sitios web prohibidos de la generalitat

Física: Ventiladores, ventanas, la puerta, extintor

### ***Ejercicio 5.-***

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

* Antivirus
* Fuente de alimentación
* La placa base contiene un pequeño módulo que controla los posibles picos de electricidad que pasen de la fuente de alimentación, en ese caso el ordenador se apaga
* Firewall
* Filtrado MAC

### ***Ejercicio 6.-***

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

No tengo SAI

### ***Ejercicio 7.-***

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

1. 123456
2. password
3. 12345678
4. qwerty
5. 12345

### ***Ejercicio 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 e importantes y como tal, se deben proteger.
* Tener varias copias de seguridad ayuda a evitar la pérdida de datos.
* Planear una forma rápida de volver a la normalidad, en caso de que sea un servicio en web, por ejemplo, si un servidor se cae, que empiece a trabajar otro servidor que sirve de colchón.

### ***Ejercicio 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.**

* Dejar claramente definidas las funciones de quienes deben entrar en acción cuando suceda el desastre, y que todos conozcan quienes son los que tienen dicha responsabilidad.
* Suelen ser cargos altos de la empresa, o personas dedicadas específicamente a ello.
  + Al recibir la información sobre el desastre, el encargado pone en marcha el protocolo de activación.
  + Si hay peligro para el personal se evacua el local
  + Cuando no haya peligro, se envía a un mínimo de personas al lugar del desastre, para comprobar el estado.
  + Valorar el tamaño del desastre.
  + Realizar un informe. Recomendable agregar fotografías del desastre.