# Sistemas Operativos
## Escuela de Ingeniería Informatica

## Preguntas de los kahoots del tema 7

- Cuándo es un sistema informático seguro?
  - **Cuando garantiza que un usuario legítimo pueda trabajar con él.**
  - **Cuando impide a un usuario ilegítimo trabajar con él.**
  - Cuando incluye un antivirus.
  - Cuando incluye un firewall.
- Cuáles son los objetivos clásicos de seguridad?
  - **Confidencialidad.**
  - **Intengridad.**
  - **Disponibilidad.**
  - Rendimiento.
- En seguridad informática, una amenaza es
  - Una técnica para atacar un sistema.
  - Una persona que puede dañar un sistema.
  - Una debilidad en la seguridad del sistema.
  - **Una daño que puede sufrir el sistema con una probabilidad significativa.**
- En seguridad informática, una vulnerabilidad es
  - Una técnica para atacar un sistema.
  - Una persona que puede dañar un sistema.
  - **Una debilidad en la seguridad del sistema.**
  - Una daño que puede sufrir el sistema con una probabilidad significativa.
- En seguridad informática, un exploit es
  - **Una técnica para atacar un sistema.**
  - Una persona que puede dañar un sistema.
  - Una debilidad en la seguridad del sistema.
  - Una daño que puede sufrir el sistema con una probabilidad significativa.
- Sniffing (o eavesdropping, o escucha ilegal) es una amenaza a
  - **La confidencialidad.**
  - La integridad.
  - La disponibilidad.
  - todos los anteriores.
- Man in the middle es una amenaza a
  - La confidencialidad.
  - **La integridad.**
  - La disponibilidad.
  - todos los anteriores.
- Un ataque DDOS (Denegación de servicio distribuido) es una amenaza a

  - La confidencialidad.
  - La integridad.
  - **La disponibilidad.**
  - todos los anteriores.
- La usurpación de identidad es una ataque a:
  - La confidencialidad.
  - La integridad.
  - La disponibilidad.
  - **todos los anteriores.**
- La usurpación de identidad es una ataque a:
  - La confidencialidad.
  - La integridad.
  - La disponibilidad.
  - **todos los anteriores.**
- Robar un disco duro es una ataque a:
  - La confidencialidad.
  - La integridad.
  - La disponibilidad.
  - **todos los anteriores.**
- Una medida fundamental para protegernos de los ataques de día cero es
  - Instalar un antivirus
  - Instalar un firewall
  - **Mantener el sistema actualizado**
  - **Instalar sólo el software que necesitemos**
- Qué medidas puede implementar el SO para hacerlo más seguro?
  - **Configurar límites para el uso de los recursos (procesos, memoria, ...)**
  - **Asignar los privilegios con cuidado.**
  - **Usar siempre comunicaciones cifradas.**
  - Restringir desde dónde se pueden realizar operaciones delicadas
- Qué medidas puede implementar el SO para hacerlo más seguro?
  - **Configurar límites para el uso de los recursos (procesos, memoria, ...)**
  - **Asignar los privilegios con cuidado.**
  - **Usar siempre comunicaciones cifradas.**
  - Restringir desde dónde se pueden realizar operaciones delicadas
- Para autenticar a un usuario la opción más segura es
  - Utilizar contraseñas.
  - Usar biométricos.
  - Usar elementos físicos (tarjetas, llaves, ....)
  - **Usar una combinación de las anteriores.**
- Para controlar el acceso a los recursos (como ficheros), el sistema operativo define
  - Dominios de protección
  - Permisos
  - Grupos
  - **Tanto dominios de protección como permisos.**
- Las listas de control de acceso
  - Almacenan permisos en una lista única.
  - asocia a cada usuario los permisos para acceder a cada recurso.

  - **asocia a cada recurso los permisos que tiene cada usuario o grupo**
  - Es una técnica para controlar el acceso al sistema.
- Los dominios de protección tradicionales son
  - Usuario, grupo, otros.
  - Usuarios individuales
  - Grupos
  - **Todos los anteriores**
- Los permisos de acceso típicos son
  - Leer, escribir, ejecutar.
  - Leer, escribir, borrar.
  - Leer, escribir, borrar, ejecutar y crear.
  - **Depende del sistema operativo.**