1- Diffie - Hellman (intercambio de claves asimétricas)
2- Tamaño del AES = variable (128 - 256)
3- Seguridad (integridad, confidencialidad, integridad)
4- Dirección IP pública (servidor -distinto- local) 192.168.1.0 es privada
5- Seguridad WIFI = WPA2
6- La Seguridad Informática es la disciplina que se ocupa de diseñar…
7- Información = activo más importante
8- Seguridad es un proceso, no un producto
9- Inyecciones SQL (Agregación ejecutable de instrucciones SQL en el servidor Web)
10- Envenenamiento de DNS (manipulación de IP)Pharming, false la info. de los servidores de nombres de dominio
11- Criptografía = La única que puede asegurar la privacidad
12- Asegurar la integridad en correo electrónico = Firma
13- Aspectos que aseguran la privacidad (Autenticación, confidencialidad, integridad,Norepudio, Trazabilidad,temporalidad)
14- Criptografía simétrica = El principal problema es hacer llegar la clave
15- Calidad del algoritmo cripta. = Potencia algoritmo y tamaño clave
16- Tamaño del RSA = fijo (512-4096)
17- Tamaño del resumen = fijo (256 - 512 bits)
18- ECB problemática al encriptar cada módulo del fichero con la misma clave
19- Man in the middle = problemática del modelo de clave asimétrica
20- RSA basado en la imposibilidad de factorial números enteros muy grandes
21- Sistemas horizontales = mismo nivel de confianza
22- Sistemas verticales = Claves públicas firmadas por la CA
23- Certificado digital = Clave pública del titular, identidad, operaciones, firma digital
24- Cookies = Se instalan en el navegador, se envían desde el servidor
25- VPN (Conexión en servidor seguro) cifra los paquetes de red (mantiene la cabecera)
26- S/MIME Es un estándar de codificación de información (te estructura el mensaje de correo en partes){Sistema vertical}
27- SSL -capa segura- es un estándar que permite la privacidad de las conexiones por internet (HTTPS lo tiene)
28- Aseguran la confidencialidad = clave simétrica
29- Que es el DAÑO= Relación entre la magnitud del riesgo y la probabilidad de que ocurra
30- Que es vulnerabilidad = Deficiencia de un sistema que puede que produzca un fallo (EXPLOIT)
31- Ataques de día 0 = Encontrar un EXPLOIT en un sistema que no haya sido descubierto
32- Rootkit = Sustituye programas del sistema operativo para pasar inadvertido
33- Bots = Se instalan en el equipo y ejecutan órdenes del atacante (disponen de rootkit los más sofisticados)
34- Phishing = Usa ingeniería social para crear una copia maliciosa y robar datos introducidos por el usuario

35- Cross-Site scripting = Explotación de vulnerabilidad de un servidor web, introduciendo código malicioso en el URL
35- DMZ =Porción de red interna del sistema que realiza la comunicación con el exterior (Firewall y monitorización)