



Exámen de muestra/practica 2013, preguntas y respuestas

Lexislación e Seguridade Informática (Universidade da Coruña)

LSI examen enero 2013/2014

1. LAG:

- a) Linux Access Grant
- b) Link Aggregation Channel**
- c) ..
- d) ..

2. Buffer Overflow:

- a) Modificación
- b) Interrupción**
- c) Generación
- d) ..

3. Idle Scan:

- a) Relacionado con Ip Spoofing, IP ID, control de estado entre otros.**
- b) No relacionado con Ip Spoofing pero sí con IP ID
- c) La a) es correcta pero sin Ip Spoofing
- d) Ninguna de las anteriores

4. Top 10 OWASP 2013:

- a) Cross-Site Scripting (XSS)
- b) Network Sniffing
- c) Injection**
- d) Broken Session Control Management

5. AES:

- a) Cifrado Simétrico**
- b) Cifrado Asimétrico
- c) Función Hash
- d) Función de codificación

6. modsecurity:

- a) ..
- b) ..
- c) Mod de Apache para evitar DDoS
- d) Firewall de aplicación web**

7. mangle en iptables:

- a) ..
- b) NAT
- c) Modificación de paquetes**
- d) ..

8. proxy transparente:

- a) Eres totalmente anonimo
- b) Totalmente desaconsejable si quieres ganar anonimidad.**
- c) ..
- d) ..

9. La ip de ntp 127.127.1.1 significa:

- a) Nivel superior
- b) Nivel inferior
- c) El reloj interno de la máquina**
- d) Ninguna de las anteriores

10. En los tipos de backups:

- a) ..
- b) El diferencial es más rápido que el incremental haciendo el backup.
- c) El diferencial es más sencillo que el incremental restaurando.**
- d) Todas las anteriores son ciertas

11. Diferencia entre tcp-wrappers e iptables:

- a) ..
- b) Los tcp-wrappers se aplican antes que las reglas de iptables.
- c) Los tcp-wrappers se aplican a nivel de sistema operativo y los iptables a nivel de aplicación.
- d) Ninguna de las anteriores.**

12. En cifrado asimétrico se cifra:

- a) Con la clave pública del receptor**
- b) Con la clave privada del emisor
- c) Con la clave pública del emisor
- d) Con la clave privada del receptor

13. La función:

- a) Sha3 es usada en los protocolos de seguridad actuales.
- b) Kekkan..? es el algoritmo que implementa Sha2
- c) ..
- d) Ninguna de las anteriores**

14. X509:

- a) PKI**
- b) ..
- c) ..
- d) Estandar de sensores de red

15. CVE-2003-5007:

- a) Clave de identificación única para vulnerabilidades.**
- b) "" de categorías.
- c) ..
- d) ..

16. Port-knocking:

- a) Un mecanismo para tirar host, coloquialmente hablando "knockear"
- b) Con esto ves a través de la cámara de tu profesor de LSI
- c) ..
- d) Técnica empleada para abrir servicios/puertos enviando una secuencia de paquetes a puertos determinados**

17. La manera más eficiente de comprobar si una máquina esta up:

- a) ICMP Echo Request (Ping)
- b) TCP SYN ← Creo**
- c) TCP ACK
- d) ARP Request

18. CAM Flooding:

- a) Rebentar el CAM del switch objetivo con el objetivo de que actúe como un Hub**
- b) No funciona utilizando ARP estático
- c) Es lo mismo que ARP Spoofing/Poisoning
- d) ..

19. En las redes Tipo TOR:

- a) Es infalible
- b) Hay tres tipos de entidades: Onion Router, Onion Proxy, y Anonymizers
- c) Es necesario un entry node, middle node, y exit node**
- d) El exit node va siempre cifrado a su destino.

20. El Reflective SYN FLOOD

- a) Empleo de botnets.
- b) ..
- c) Se le manda a la víctima un paquete con la dirección ip de origen su dirección de destino para que entre en un bucle infinito.
- d) Utiliza nodos intermedios para repetir.. (broadcast)**

21. El Common Name de un certificado digital es:

- a) El nombre y apellidos
- b) Un correo electrónico
- c) El nombre de dominio**
- d) El nombre de la CA

Protección y Seguridad de la Información (junio 2009)

1.- DVL

- a) Distribución GNU/Linux que aglutina las principales herramientas en ataque orientada a la realización de auditorías de seguridad
- b) Distribución GNU/Linux repleta de inseguridades orientada al aprendizaje**
- c) Distribución GNU/Linux que incluye los desarrollos LVS orientada a Alta Disponibilidad
- d) Ninguna de las anteriores

2.- La herramienta Xprobe está orientada a

- a) Backups en modo cliente-servidor
- b) Detección de sniffers en un segmento de red
- c) Cifrar sesiones de trabajo que no soporten SSL
- d) Identificación remota de sistemas operativos basada en ICMP**

3.- Un amigo está haciendo referencia al nmap y te habla de un idle scan

- a) Hace referencia a la decodificación de firmas para identificar el sistema operativo de un sistema remoto de forma pasiva
- b) Hace referencia a un escaneo de puertos
- c) Hace referencia a un escaneo suplantando otras IPs**
- d) Hace referencia a un escaneo mediante retardos

4.- Si enviamos un paquete FIN a un sistema generalmente nos responderá

- a) FIN ante un puerto cerrado y nada si está abierto
- b) RST|ACK ante un puerto abierto y nada si está cerrado
- c) RST|ACK ante un puerto cerrado y nada si está abierto**
- d) Ninguna de las anteriores

5.- El proceso de firma digital

- a) Cifra la huella con la clave pública del emisor
- b) Cifra la huella con la clave pública del receptor
- c) Cifra la huella con la clave privada del emisor**
- d) Ninguna de las anteriores es correcta

6.- Si ejecutamos el comando # ac

- a) Total de tiempo de cpu utilizado por los procesos de un usuario, en este caso del root
- b) Información de fecha, hora, etc., de las sesiones abiertas por un usuario, en este caso del root
- c) Relación de comandos ejecutados en el proceso de accounting, en este caso del root
- d) Total de horas de conexión de un usuario, en este caso del root**

7.- zabbix

- a) Herramienta de monitorización distribuida**
- b) Herramienta para backups distribuidos
- c) Herramienta de detección de interfaces en modo promisc
- d) Ninguna de las anteriores

8.- ISO27002

- a) Guía de buenas prácticas en seguridad
- b) Estándar que se centra en la gestión de la seguridad de la información (análisis de riesgos, planes de contingencia, etc.)**
- c) Guía de fases para “securizar” redes WIFI
- d) Estándar que define configuraciones seguras de plataformas de “backups”

9.- En una red de tomas de tierra, ¿qué es el TGB?

- a) Barra principal
- b) Barras secundarias**
- c) Backbone de la red de tomas de tierra
- d) Ninguna de las anteriores

11.- LTO4

- a) 400MB nativos
- b) 200GB nativos
- c) 400GB nativos
- d) 800GB nativos**

13.- ¿Qué entorno de trabajo es el característico del software Tivoli?

- a) Sniffers
- b) Gestión de almacenamiento y backups**
- c) DDoS
- d) Filtrado por tcpwrappers

14.- ¿Qué método de sniffing hace spoofing sobre los switches pensando en un entorno de medio conmutado?

- a) MAC Flooding**
- b) ARP Spoofing
- c) MAC Trusted
- d) MAC Duplicating

15.- Puerto 514

- a) ntp
- b) X509 – Autoridades Certificadoras
- c) syslog**
- d) Ninguno anteriores

16.- Atendiendo al nivel de importancia de los mensajes de log, ¿qué afirmación es correcta?

- a) EMERG menor importancia que CRIT
- b) ALERT menor importancia que CRIT**
- c) CRIT menor importancia que CRIT 9
- d) Ninguna de las anteriores

17.- Direcciones IPV6

- a) 32
- b) 64
- c) 128**
- d) 256

18.- /etc/nsswitch.conf

- a) Esquema de fuentes para hosts, dns, autenticación, etc.**
- b) Esquema de resolución del sistema y el dominio.
- c) Configuración de correspondencia entre máquinas y direcciones Ethernet
- d) Ninguna de las anteriores

19.- Port Security en CISCO

- a) enable switchport port-security
- b) port-security on
- c) switchport port-security**
- d) port-security active de una ... vez

20.- AES

- a) clásico
- b) flujo
- c) bloque**
- d) asimétrico

Junio 2001

1.- La modificación es una categoría de ataque contra

- a)Confidencialidad
- b)Disponibilidad
- c)Integridad**
- d)Austeridad

2.- Un ataque por repetición es de tipo

- a)activo**
- b)pasivo
- c)inverso
- d)mixto

3.- Que tecnica de “scanning de puertos” se conoce como escaneo de “media apertura”

- a)TCP SYN Scaning
- b)TCP connect() scanning
- c)TCP open() scanning
- d)TCP reserve ident scanning

Protección y Seguridad de la Información (junio 2009)

Nombre.:

Apellidos.:

1.- DVL

- a) Distribución GNU/Linux que aglutina las principales herramientas en ataque orientada a la realización de auditorías de seguridad
- b) Distribución GNU/Linux repleta de inseguridades orientada al aprendizaje
- c) Distribución GNU/Linux que incluye los desarrollos LVS orientada a Alta Disponibilidad
- d) Ninguna de las anteriores

2.- La herramienta Xprobe está orientada a

- a) Backups en modo cliente-servidor
- b) Detección de sniffers en un segmento de red
- c) Cifrar sesiones de trabajo que no soporten SSL
- d) Identificación remota de sistemas operativos basada en ICMP

3.- Un amigo está haciendo referencia al nmap y te habla de un idle scan

- a) Hace referencia a la decodificación de firmas para identificar el sistema operativo de un sistema remoto de forma pasiva
- b) Hace referencia a un escaneo de puertos
- c) Hace referencia a un escaneo suplantando otras IPs
- d) Hace referencia a un escaneo mediante retardos

4.- Si enviamos un paquete FIN a un sistema generalmente nos responderá

- a) FIN ante un puerto cerrado y nada si está abierto
- b) RST|ACK ante un puerto abierto y nada si está cerrado
- c) RST|ACK ante un puerto cerrado y nada si está abierto
- d) Ninguna de las anteriores

Nombre.:

Apellidos.:

5.- El proceso de firma digital

- a) Cifra la huella con la clave pública del emisor
- b) Cifra la huella con la clave pública del receptor
- c) Cifra la huella con la clave privada del emisor
- d) Ninguna de las anteriores es correcta

6.- Si ejecutamos el comando # ac

- a) Total de tiempo de cpu utilizado por los procesos de un usuario, en este caso del root
- b) Información de fecha, hora, etc., de las sesiones abiertas por un usuario, en este caso del root
- c) Relación de comandos ejecutados en el proceso de accounting, en este caso del root
- d) Total de horas de conexión de un usuario, en este caso del root

7.- zabbix

- a) Herramienta de monitorización distribuida
- b) Herramienta para backups distribuidos
- c) Herramienta de detección de interfaces en modo promisc
- d) Ninguna de las anteriores

8.- ISO27002

- a) Guía de buenas prácticas en seguridad
- b) Estándar que se centra en la gestión de la seguridad de la información (análisis de riesgos, planes de contingencia, etc.)
- c) Guía de fases para “securizar” redes WIFI
- d) Estándar que define configuraciones seguras de plataformas de “backups”

Nombre.:

Apellidos.:

9.- En una red de tomas de tierra, ¿qué es el TGB?

- a) Barra principal
- b) Barras secundarias
- c) Backbone de la red de tomas de tierra
- d) Ninguna de las anteriores

10.- ¿Qué hace un RAID01?

- a) RAID1 sobre dos RAID0
- b) RAID0 sobre dos RAID1
- c) RAID0 sobre dos RAID lineales
- d) No existen los RAID01. Únicamente existen los RAID10

11.- LTO4

- a) 400MB nativos
- b) 200GB nativos
- c) 400GB nativos
- d) 800GB nativos

12.- ¿Qué otro nombre se utiliza para designar un RAID-0?

- a) striking
- b) mirror
- c) stripping
- d) lineal

13.- ¿Qué entorno de trabajo es el característico del software Tivoli?

- a) Sniffers
- b) Gestión de almacenamiento y backups
- c) DDoS
- d) Filtrado por tcpwrappers

Nombre.:

Apellidos.:

14.- ¿Qué método de sniffing hace spoofing sobre los conmutadores pensando en un entorno de medio switched?

- a) MAC Flooding
- b) ARP Spoofing
- c) MAC Trusted
- d) MAC Duplicating

15.- Puerto 514

- a) ntp
- b) X509 – Autoridades Certificadoras
- c) syslog
- d) Ninguno anteriores

16.- Atendiendo al nivel de importancia de los mensajes de log, ¿qué afirmación es correcta?

- a) EMERG menor importancia que CRIT
- b) ALERT menor importancia que CRIT
- c) CRIT menor importancia que CRIT ☺
- d) Ninguna de las anteriores

17.- Direcciones IPV6

- a) 32
- b) 64
- c) 128
- d) 256

18.- /etc/nsswitch.conf

- a) Esquema de fuentes para hosts, dns, autenticación, etc.
- b) Esquema de resolución del sistema y el dominio.
- c) Configuración de correspondencia entre máquinas y direcciones Ethernet
- d) Ninguna de las anteriores

Nombre.:

Apellidos.:

19.- Port Security en CISCO

- a) enable switchport port-security
- b) port-security on
- c) switchport port-security
- d) port-security activate de una ... vez

20.- AES

- a) clásico
- b) flujo
- c) bloque
- d) asimétrico

Respuestas del examen:

1. b
2. d
3. c
4. c
5. c
6. d
7. a
8. b
9. b
10. a
11. d
12. c
13. b
14. a
15. c
16. b
17. c
18. a
19. c
20. c

PREGUNTAS TIPO TEST DE AUDITORÍA INFORMÁTICA (algunas de examen)

- 1. La Auditoría Interna se centra principalmente en:**
 - a. Salvaguarda de bienes
 - b. Integridad de datos
 - c. Aspectos de gestión
 - d. Todas las anteriores
- 2. Uno de los métodos empleados por Jerry Schneider fue:**
 - a. Masquerading
 - b. Browsing
 - c. Piggybacking
 - d. Spooling
- 3. Piggybacking o interceptación de comunicaciones consiste en:**
 - a. Acceso no autorizado suplantando a un usuario autorizado o al propio sistema
 - b. Usar el tiempo durante el cual un usuario autorizado está conectado e inactivo
 - c. El usuario interactúa con un programa que imita el procedimiento de conexión de un usuario con el sistema
 - d. Ninguna de las anteriores
- 4. ¿Cuál de los siguientes controles no forma parte del Marco de Control de la Gerencia?**
 - a. Gerencia de Programación
 - b. Gerencia de Desarrollo de Sistemas
 - c. Administración de Bases de Datos
 - d. Gerencia del Plan de Recuperación
- 5. La fase de revisión preliminar en una Auditoría Informática consiste en:**
 - a. Obtener un conocimiento detallado de los controles utilizados en la instalación
 - b. Comprobar que los controles internos funcionan como lo deben hacer
 - c. Obtener información sobre cómo llevar a cabo la auditoría
 - d. Obtener evidencias suficientes para tomar la decisión final
- 6. ¿Cuál es el mejor modo para paliar la pérdida de independencia de un auditor?**
 - a. Aumentar el conocimiento informático del auditor
 - b. Poner los mismos auditores en la Fase de Diseño y en la Post-Implementación
 - c. Auditorías con ordenador y sin ordenador
 - d. Todas las anteriores
- 7. Los controles batch son:**
 - a. Controles preventivos
 - b. Controles de detectores
 - c. Controles correctores
 - d. Ninguna de las anteriores
- 8. Si en una cadena en vez de 87942 ponemos 8792, se conoce como:**
 - a. Transcripción
 - b. Transposición
 - c. Truncamiento
 - d. Doble transposición

- 9. Para el número 2148, el juego de pesos 5-4-3-2 y el módulo 10, el dígito de control sería:**
- a. 2
 - b. 8
 - c. 4
 - d. 6
- 10. Una contraseña debe:**
- a. tener longitud máxima
 - b. formadas por palabras que tengan significado
 - c. cambiarse obligatoriamente cada cierto tiempo
 - d. todas las anteriores
- 11. La Session Key (SK):**
- a. se genera automáticamente al comenzar cada sesión
 - b. se utiliza para encriptar todo el tráfico entre el terminal y el host durante la sesión
 - c. el host la envía al terminal
 - d. todas las anteriores
- 12. La fecha y hora en un informe estará presente en:**
- a. la página de título
 - b. la página de título y página de detalle
 - c. la página de detalle
 - d. Ninguna de las anteriores
- 13. ¿Cuál de los siguientes controles de calidad que no debe faltar?**
- a. QA de Migración
 - b. QA Interno
 - c. QA de Desarrollo
 - d. QA Independiente
- 14. ¿El personal de qué grupos compone el equipo de QA de Migración?**
- a. De Explotación
 - b. QA Independiente
 - c. Departamento del Usuario
 - d. Todas las anteriores
- 15. El control de versiones del software es un mecanismo que:**
- a. Mostrará el camino que deberá recorrer el software antes de su paso a Producción
 - b. Indicará los niveles de calidad que deberá atravesar
 - c. Determinará cuáles son los métodos de vuelta atrás en el caso de encontrarse fallos
 - d. Todas las anteriores
- 16. El coordinador de recuperación es el encargado de:**
- a. Realizar y mantener en el tiempo el plan de recuperación
 - b. Realizar copias de seguridad de los datos y las aplicaciones
 - c. Restaurar el sistema a una versión estable
 - d. Todas las anteriores
- 17. ¿En qué estrategia de protección de sistemas se contratan los servicios de una compañía externa que asegura la disponibilidad de los equipos utilizados por la empresa en caso de desastre?**

- a. Hardware redundante
- b. Cold site
- c. Hot site
- d. Suministro de equipos

18. En la revisión de Post-Implementación hay que:

- a. Realizar un backup de las Bases de Datos
- b. Documentar cualquier problema o solución no descubierta durante la fase de operación
- c. Realizar pruebas de trabajo real
- d. Todas las anteriores

19. En el diagrama de Ishikawa:

- a. La “cabeza del pez” representa una causa de un problema y las “espinas” posibles soluciones
- b. La “cabeza” representa un problema y las “espinas” sus posibles soluciones
- c. La “cabeza” representa un problema y las espinas” sus causas
- d. Ninguna de las anteriores

20. El diagrama de Pareto representa La relación existente entre:

- a. los fallos ocurridos y su frecuencia
- b. los fallos ocurridos y el tiempo en el que se produjo
- c. los fallos ocurridos y el tiempo en que se le dio solución
- d. Ninguna de las anteriores

21. Los datos de persona o de identificación personal:

- a. Son datos de dominio público
- b. Son un subconjunto de los datos de carácter personal
- c. No se consideran datos de carácter personal
- d. Ninguna de las anteriores

22. El derecho de oposición:

- a. Significa que nadie podrá ser obligado a declarar datos de ideología, religión o creencias
- b. Es un derecho gratuito
- c. Significa que toda persona física puede modificar sus datos personales en el caso de que presenten errores o incorrecciones
- d. Significa que toda persona física puede oponerse al tratamiento de sus datos personales si estos no se tratan correctamente en un fichero cifrado

23. Podrán acceder a donde se encuentren ubicados los sistemas de información con datos de carácter personal de nivel medio...:

- a. Los auditores internos
- b. El director del CPD
- c. Todos los que figuren en el Documento de Seguridad
- d. Todas las anteriores

24. ¿Qué características no forman parte del control interno en Auditoría Tradicional?

- a. Sistema de autorizaciones
- b. Acceso limitado a bienes
- c. Delegación clara de autoridad y responsabilidad
- d. Copias de seguridad y backup

- 25. La comprobación de que los controles internos funcionan correctamente se lleva a cabo en:**
- a. Revisión detallada
 - b. Pruebas de apoyo
 - c. Pruebas de comportamiento
 - d. Revisión preliminar
- 26. La descentralización de la función de AI es adecuada si:**
- a. Los grupos de AI son de diversa creación
 - b. Hay pocos expertos en AI
 - c. Los grupos tienen experiencia suficiente
 - d. Ninguna de las anteriores
- 27. En la escala de criticidad, aquellas funciones que pueden realizarse manualmente, aunque con dificultades durante un largo periodo de tiempo se dicen:**
- a. Críticas
 - b. Sensibles
 - c. No Sensibles
 - d. Ninguna de las anteriores
- 28. En la fase de definición de objetivos de recuperación:**
- a. Eliminar peligros evitables
 - b. Prevenir peligros evitables
 - c. Identificar los peligros que afectan a los sistemas
 - d. Todas las anteriores

Preguntas AXDI

1. Funciones del Derecho

- Organización de la vida social
 - Relaciones jurídico-públicas
 - Relaciones jurídico-privadas
- Resolución de conflictos
- Legitimación del poder social

2. Define brevemente: relación jurídica, sujeto de derecho, deber jurídico y derecho subjetivo

- Relación jurídica: relación que se establece entre dos o más sujetos en la que existe una parte titular de un derecho y otra titular del correspondiente deber.

- Sujeto de derecho: centro de imputación ideal de deberes y derechos; esto es, aquella unidad sobre la que la ley efectúa imputaciones directas, arrojándole derechos y obligaciones.

- Deber jurídico: surge de las condiciones de la relación jurídica. Sin deuda no hay derecho

- Derecho subjetivo: Es la facultad reconocida a la persona por la ley que le permite efectuar determinados actos, un poder otorgado a las personas por las normas jurídicas para la satisfacción de intereses que merecen la tutela del Derecho.

3. ¿Cómo se lleva a cabo la creación, modificación, extinción de relaciones jurídicas y de solución de controversias?

Mediante las normas, no aisladas, sino como parte de una regulación.

4. ¿Qué es la legislación?

Un cuerpo de leyes que regulan una determinada materia o al conjunto de leyes de un país.

5. ¿Qué es la jurisdicción?

Es la potestad, derivada de la soberanía del Estado, de aplicar el Derecho en el caso concreto, resolviendo de modo definitivo e irrevocable una controversia, que es ejercida en forma exclusiva por los tribunales de justicia integrados por jueces autónomos e independientes.

6. ¿Qué se entiende por carácter institucional del Derecho?

El derecho representa una estructura de autoridad, pretende tener autoridad sobre sus destinatarios para decirles qué es lo que deben hacer.

7. ¿Qué se entiende por carácter normativo del Derecho?

El derecho pretende guiar la conducta, la acción humana (nota básica del sistema jurídico, pero no exclusiva de él)

8. ¿Qué se entiende por carácter coactivo del Derecho?

Significa que la obediencia a él y su aplicación se encuentran garantizadas en última instancia por el uso de la fuerza.

9. ¿Qué es el derecho informático?

Un conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación entre el Derecho y la informática.

10. ¿Qué es la informática jurídica? Clases

Es una disciplina de las ciencias de la información que tiene por objeto la aplicación de la informática en el Derecho. Difiere entonces del Derecho informático, que es la regulación jurídica de las nuevas tecnologías. Tiene como antecedente la jurimetría.

Clases:

- Informática jurídica documental.
- Informática jurídica de gestión.
- Informática jurídica decisional.

11. ¿Qué es la deontología? Definición

Se refiere a un conjunto ordenado de deberes y obligaciones morales que tienen los profesionales de una determinada materia

12. ¿Son obligatorias las normas deontológicas?

Expresan obligaciones de necesario cumplimiento.

13. Principios de un código tipo.

Dichos códigos hacen alusión a la política concreta de la empresa en cuanto a cómo llevará a cabo lo establecido por la ley, pero con el matiz de establecer en ellos un plus, o un esmero adicional a la hora de establecer dichas prácticas

14. ¿Qué es la protección de datos de carácter personal?

Se trata de la protección ético-jurídica de informaciones referidas a una persona física, identificada o identificable

15. ¿A qué obliga protección de datos de carácter personal?

Al control que a cada individuo le corresponde sobre la información que personalmente le concierne, sea íntima o no, para impedir que otros puedan conocerla y/o utilizarla de forma que les perjudique.

16. ¿Qué consecuencias puede tener su incumplimiento?

La aplicación de la LOPD, (Ley Orgánica de Protección de Datos).

17. ¿Qué son los datos de carácter personal?

Los datos referidos a lo íntimo, privado.

18. ¿Qué se entiende por persona identificable?

Se trata de una persona física.

19. ¿Cuáles son los datos especialmente protegidos?

Ideología, origen social, religión, salud, creencias, vida sexual.

20. ¿A qué datos no se aplica la ley y su reglamento?

A los datos de las administraciones públicas competentes

21. ¿Qué son los ficheros de datos personales?

Un fichero de datos personales es “todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica

22. ¿Puedo como empresario crear y mantener ficheros de datos personales?

Si, si se declaran a la agencia española de protección de datos informando a quien se soliciten los datos.

23. ¿Qué obligaciones asume una empresa por crear y mantener ficheros?

Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.

24. ¿Qué es el tratamiento de datos personales?

El tratamiento de datos es cualquier procedimiento técnico, automatizado o manual, que permita la recogida, grabación, conservación, elaboración, modificación, bloqueo, cancelación o cesión a terceros de los datos de carácter personal.

25. ¿Todos los tratamientos de datos están sometidos a la LOPD?

No, existen excepciones como cuando se trate de datos recogidos de fuentes accesibles al público.

26. ¿Qué diferentes personas intervienen en el tratamiento?

El responsable del fichero o del tratamiento, el encargado del tratamiento y el afectado o interesado.

27. ¿Quién es el responsable del tratamiento?

Es aquella persona física o jurídica, pública o privada, u órgano administrativo, que decide la creación de un fichero de datos personales, así como la finalidad, contenido y uso que haya de darse al mismo.

28. ¿Quién es el afectado o interesado?

Es la persona física (nunca una persona jurídica) que es titular de los datos de carácter personal que han sido incluidos en un fichero de datos y que son objeto de tratamiento

29. ¿Quién es el encargado del tratamiento?

Es aquella persona física o jurídica, autoridad pública, servicio u organismo que tiene acceso al fichero de datos personales y puede realizar un tratamiento de los datos contenidos en él por cuenta del responsable del fichero

30. ¿Cómo se lleva a cabo la relación entre responsable del fichero y el encargado del tratamiento?

Mediante un contrato.

31. Obligaciones del encargado del tratamiento

La celebración de un contrato en el que se especifiquen los datos a tratar, la finalidad del tratamiento, las medidas de seguridad a aplicar, la autorización o no para subcontratar servicios y, por ende, el tratamiento de datos personales, la destrucción y/o devolución de los datos una vez concluida la prestación del servicio, etc.

32. ¿Qué se entiende por procedencia de datos?

33. ¿Cuándo obtengo los datos directamente del interesado?

Cuando se precisa su consentimiento.

34. ¿A qué está la empresa obligada cuando pide los datos al interesado?

Sería preciso dejar al mismo la posibilidad de manifestarse a favor o en contra del tratamiento en el propio momento de la recogida

35. ¿Qué son las fuentes accesibles al público?

Hace referencia a aquellas fuentes de información que pueden ser utilizadas para obtener datos de carácter personal y tratarlos sin necesidad de disponer del consentimiento de la persona afectada.

36. ¿Qué fuentes accesibles al público hay?

Censo promocional, repertorios telefónicos. Diarios y boletines oficiales, medios de comunicación.

37. ¿A qué está obligada una empresa .cuando obtiene datos de fuentes accesibles?

Simplemente a asegurarse de que la fuente accesible se incluya en el artículo 3j.

38. ¿Es Internet una fuente accesible al público?

No.

39. ¿Qué son los datos obtenidos de terceros? ¿Qué obligaciones hay al respecto?

En muchas ocasiones, las empresas contratan y subcontratan con otras empresas la prestación de servicios profesionales especializados, servicios que suponen un acceso a datos de carácter personal almacenados en nuestros ficheros para que sean tratados.

La obligación es formalizar por escrito de manera que acredite fehacientemente su celebración y contenido.

40. ¿Qué se entiende por cesión de datos?

Toda revelación de datos realizada por persona distinta del interesado.

41. ¿Qué es necesario para ceder datos?

- 1º.- Que sólo será posible la cesión de los datos para el cumplimiento de fines directamente relacionados con las funciones de cedente y cesionario.
- 2º.- El previo consentimiento informado del interesado.

42. La cesión de datos especialmente protegidos

43. ¿Qué se entiende por transferencia internacional de datos personales?

Aquel transporte de datos entre sistemas informáticos por cualquier medio de transmisión, así como el transporte de soportes de datos por correo o cualquier otro medio convencional.

44. ¿Qué es el consentimiento del afectado?

Al entender la Ley la necesidad del tratamiento, informatizado o no, de datos de carácter personal por parte de las empresas para poder desarrollar sus actividades propias, fija como contrapeso la necesidad de observar la voluntad del interesado

45. ¿De qué formas se puede obtener el consentimiento?

De manera tácita para la mayoría de los casos, en el caso de datos de salud debe existir un consentimiento expreso, así como para datos de ideología, creencias, etc.

46. ¿De qué debe informar el responsable del fichero?

Debe informarse al afectado de: el titular del fichero, las finalidades del tratamiento, el carácter obligatorio/facultativo de las respuestas, derechos que asisten al afectado y de las condiciones para ejercitar tales derechos.

47. ¿Quién debe probar que existe consentimiento del afectado?

El responsable del fichero.

48. ¿Se pueden obtener datos de menores de edad?

Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.

49. ¿Qué se entiende por calidad de los datos de carácter personal?

Los datos personales serán tratados de manera leal y lícita, y recogidos con fines determinados, explícitos y legítimos. Además, serán exactos y, cuando sea necesario, actualizados.

50. ¿Qué se entiende por la pertinencia de los datos?

La pertinencia de los datos refiere al almacenamiento únicamente de aquellos datos de carácter personal que resulten adecuado y necesarios para cumplir las finalidades para las que han sido recogidos y el deber que tiene de cancelarlos cuando dejan de serlo.

51. ¿Qué se entiende por adecuación del tratamiento?

La adecuación del tratamiento supone la aceptación y el compromiso de que los datos personales almacenados sólo serán tratados con la finalidad para la que hayan sido obtenidos.

52. ¿Qué se entiende por actualización de los datos?

Supone la modificación de los datos ya almacenados.

53. ¿Qué es la seguridad de los datos?

Se tratan de los procesos, recursos humanos y tecnología para asegurar la protección de los datos.

54. ¿Qué niveles de seguridad existen?

- Nivel básico: aplicable a todos los ficheros de datos personales.
- Nivel medio: aplicable a datos relativos a la comisión de infracciones administrativas o penales.
- Nivel alto: aplicable a datos especialmente protegidos.

55. Medidas de seguridad de nivel medio

1. Las medidas de seguridad de nivel bajo.
2. Responsable de seguridad.
3. Auditoría.
4. Gestión de soportes y documentos.
5. Identificación y autenticación (limitación del número de intentos).
6. Control de acceso físico.
7. Registro de incidencias.

56. Medidas de seguridad de nivel alto.

1. Medidas de seguridad de nivel bajo y medio.
2. Gestión y distribución de los soportes (cifrado).
3. Copias de respaldo y recuperación.
4. Registro de accesos.
5. Cifrado de datos en las telecomunicaciones.

57. ¿Qué es el documento de seguridad?

Creado por el responsable del fichero que contiene las medidas de índole técnicas y organizativas de obligado cumplimiento para el personal con acceso a los sistemas de información. Debe mantenerse actualizado y adecuado a las disposiciones vigentes en cada momento.

58. ¿Qué se entiende por responsable de Seguridad?

Son los encargados de coordinar y controlar las medidas definidas en el mismo.

59. ¿Qué es el deber de secreto y confidencialidad?

Obligación al secreto profesional respecto de los ficheros y al deber de guardarlos, obligaciones que sustituirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

60. ¿A quién se extiende?

Tanto el responsable del fichero, como el encargado de tratamiento, como cualquier persona que intervenga en cualquier fase del proceso.

61. ¿Cómo garantizar su cumplimiento?

Los responsables deberán adoptar las medidas de índole técnica y organizativa.

62. ¿A qué obligan al responsable del fichero los derechos de los interesados?

Obligan al deber general de respeto de la normativa de protección de datos, deber de seguridad, deber de secreto y cautelas en la cesión de datos.

63. El derecho de acceso

Permite al afectado preguntar al responsable del fichero si tiene datos personales suyos, cuáles, el origen de los mismos y la fuente.

64. El derecho de rectificación

Es el derecho que tiene el afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.

65. El derecho de cancelación

Es el derecho que da lugar a que se supriman los datos que resulten ser inadecuados o excesivos.

66. El derecho de oposición

El derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal se cese de dichos tratamientos.

67. La tutela de los derechos

68. ¿Para qué sirve la Agencia de Protección de Datos?

Vela por el cumplimiento de la normativa sobre protección de datos y garantiza y tutela el derecho fundamental a la protección de datos de carácter personal.

69. La facultad inspectora de la APD

Podrán solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados.

70. La potestad sancionadora de la APD

El Título VIII referenciado por el artículo 37. g) que recibe el nombre de “Infracciones y Sanciones”, concreta hasta dónde pueden llegar las sanciones que la APD puede imponer y por qué motivos. Las infracciones como es habitual quedan divididas en tres grandes grupos leves (art. 44.2), graves (44.3) y muy graves (44.4).

71. ¿Qué se entiende por inscripción, modificación y supresión de ficheros?

Se debe inscribir en el Registro General de Protección de Datos todos los ficheros que contengan datos de carácter personal. Para cualquier modificación o supresión debe comunicarse al Registro General de Protección de Datos.

72. ¿Qué es la propiedad intelectual?

El conjunto de derechos que corresponden a los autores y a otros titulares respecto de las obras y prestaciones fruto de su creación.

73. ¿Quién es el sujeto de la propiedad intelectual y qué características tiene?

Es la persona natural creadora de la obra. Podrán beneficiarse personas jurídicas.

74. ¿Qué y cuáles son los derechos morales de la propiedad intelectual?

Son un conjunto de derechos inherentes a la persona del autor, que tienen carácter de irrenunciables e inalienables. Son los derecho(s):

1. Sobre la divulgación de la obra,
2. de paternidad,
3. a la integridad de la obra,
4. de modificar y retirar la obra del comercio, y
5. de acceso al ejemplar de la obra.

75. ¿Qué características tienen los derechos morales de la propiedad intelectual?

1. Carácter perpetuo,
2. irrenunciabilidad, y
3. inalienabilidad.

76. ¿Qué son y cuáles son los derechos patrimoniales de la propiedad intelectual?

Conjunto de derechos que atribuyen a su titular facultades de explotación y disfrute económico derivadas de la utilización de la obra. Son los derechos:

1. exclusivos y
2. de simple remuneración.

77. ¿Qué son y cuáles son los derechos exclusivos patrimoniales?

Poder jurídico de autorizar formas de explotación de la obra. Son los derechos de:

1. reproducción,
2. distribución,
3. comunicación pública y,
4. transformación.

78. ¿Qué son y cuáles son los derechos de simple remuneración?

Facultan al autor al cobro de determinadas cantidades por utilización de la obra. Son los derechos de:

1. participación y,
2. remuneración por copia privada.

79. ¿Qué se entiende por copia privada?

No es un derecho. Es un límite al derecho de reproducción que ostentan los titulares de los derechos de propiedad intelectual de las obras y prestaciones protegidas.

80. He creado un videojuego, ¿qué tengo que hacer para protegerlo? ¿Qué derechos tengo? Si quiero utilizar unas imágenes ajenas, ¿cómo puedo hacerlo sin atentar contra los derechos de autor de otros?

Está protegido desde el momento en el que se desarrolla. Tienes todos los derechos sobre él.

Debes contar con el consentimiento del autor.

81. ¿Cuáles son los derechos de propiedad afectados por el intercambio de obras a través de los sistemas P2P?

1. *Uploading*, va precedido de la reproducción de la obra para fijarla en el disco duro. La obra es “subida” al sistema de intercambio: comunicación pública.
2. *Downloading*, constituye una reproducción de la obra.

82. ¿Se encuentran amparadas las reproducciones que se producen cuando se utiliza un sistema P2P por el límite de copia privada?

La copia realizada por el *downloader* no goza de la cobertura del límite de copia privada. Si se hace de la copia un uso colectivo deja de ser privada y se convierte en un “ejemplar ilícito”. Si se hace una utilización lucrativa, es un delito sancionado en el Código Penal.

83. ¿Cuál es la duración de los derechos de autor?

Toda la vida del autor más 70 años después de muerto o declaración de fallecimiento. Se calcula a partir del 1 de enero del año siguiente.

84. ¿Qué reproducciones totales están permitidas sin la autorización del autor?

1. Reproducción para uso privado,
2. para seguridad pública y procesos públicos,
3. copias privadas para personas con discapacidad,
4. reproducciones destinadas a centros de documentación o de investigación, y
5. reproducción de obras difundidas por los medios de comunicación.

85. ¿Qué es necesario para recurrir a la jurisdicción penal para la protección de la propiedad intelectual?

1. Dolosa: intención expresa de infringir el derecho de propiedad intelectual ajeno.
2. Con animo de lucro.
3. En perjuicio de tercero. La acción ha de ser idónea para producir un perjuicio. No se exige que efectivamente se le cause.
4. Sin autorización del titular.

86. ¿Es necesario registrar una obra artística para protegerla? ¿Qué ventajas tiene hacerlo?

No, la obra se protege por el sólo hecho de su creación. Proporciona una prueba cualificada de que los derechos inscritos existen y pertenecen a su titular y da publicidad a los derechos inscritos.

87. ¿Cuáles son los requisitos para proteger un programa de

ordenador? ¿Qué se protege y qué no se protege?

Se requiere originalidad, que no equivale a novedad, es decir, creación intelectual propia del autor.

Se protege: Cualquier forma de expresión del programa o de cualesquiera de sus versiones sucesivas y programas derivados.

NO se protege: Programas que creen virus informáticos e ideas y principios en los que se basan los elementos de un programa de ordenador.

88. ¿Quién es el autor de un programa de ordenador y qué reglas particulares existen?

A la persona o grupo de personas naturales que lo hayan creado, o la persona jurídica que sea contemplada como titular de los derechos de autor.

89. ¿Cuáles son los límites de los derechos de explotación de los programas de ordenador?

1. Actos necesarios para la utilización del programa,
2. realización de copias de seguridad,
3. estudio de programa para extraer principios o ideas implícitas, y
4. el autor no podrá oponerse a que cesionario realice versiones nuevas.

90. ¿Quiénes son los infractores de los derechos de propiedad de los programas de ordenador?

1. Pongan en circulación copias ilegítimas,
2. poseer copias ilegítimas con fines comerciales, y
3. pongan en circulación/posean instrumentos para suprimir o neutralizar dispositivos de protección de programa.

91. ¿Cuáles son las libertades que un software debe cumplir para que sea libre, según la *Free Software Foundation*?

1. La libertad de usar el programa, con cualquier propósito.
2. libertad de estudiar cómo funciona el programa, y adaptarlo a las necesidades de cada usuario,
3. la libertad de distribuir copias, para poder ayudar a la comunidad de programadores, y
4. la libertad de mejorar el programa y hacer públicas las mejoras a los demás, de modo que toda la comunidad se beneficie de ellas.

92. ¿Cuáles son los criterios que un software debe cumplir para que se considere de “fuentes abiertas”, según la *Open Source Initiative*?

1. Libre redistribución.
2. Código fuente.
3. Trabajo derivado.
4. Integridad del código fuente del autor.
5. No discriminación contra personas o grupos.
6. No discriminación contra campos de actividad.
7. Distribución de la licencia.
8. La licencia no debe ser específica al producto.
9. La licencia no debe restringir otro software.
10. La licencia debe ser tecnológicamente neutral.

93. ¿Qué se entiende por copyleft?

Se considera que una licencia es copyleft cuando además de otorgar permisos de copia, modificación y redistribución de la obra protegida, contiene una cláusula que impone la misma licencia a las copias y a las obras derivadas.

94. ¿Qué se entiende por licencia privativa o no libre?

Es cualquier cosa en el que el usuario tiene limitaciones para usarlo, modificarlo o redistribuirlo (esto último con o sin modificaciones).

95. ¿Qué se entiende por licencia permisiva?

Es una licencia de software libre flexible respecto a la distribución, de modo que el software pueda ser redistribuido como software libre o software propietario, siendo libre la licencia original del autor.

96. ¿Qué se entiende por copyleft fuerte?

El copyleft que rige un trabajo se considera “más fuerte” cuanto mayor es la eficiencia con la que hace cumplir las condiciones de la licencia a todos los tipos de trabajos derivados. Ejemplo, GPL.

97. ¿Qué se entiende por copyleft suave?

El “copyleft débil” hace referencia a las licencias que no se heredan a todos los trabajos derivados, dependiendo a menudo de la manera en que éstos se hayan derivado. Ejemplos, BSD o MIT.

98. ¿Qué se entiende por compatibilidad de licencias?

Significa que distintas licencias son compatibles entre ellas; puedes combinar código publicado bajo una licencia con código publicado bajo otra.

99. Desde el punto de vista jurídico, ¿qué objetivos deben tener los proyectos de creación de Software de fuentes abiertas?

100. ¿Qué es una patente, ¿Es obligatorio su inscripción? ¿Cuánto dura el derecho de exclusividad de una patente?

Título que reconoce el derecho de explotar en exclusiva la invención patentada, impidiendo a otros su fabricación, venta o utilización sin consentimiento del titular. Dura 20 años.

101. ¿Cuáles son los requisitos de patentabilidad?

Requisitos positivos:

1. Novedad,
2. ha de implicar una actividad inventiva, y
3. debe ser susceptible de aplicación industrial.

Requisitos negativos:

1. innovaciones consideradas no patentables: los descubrimientos, teorías o métodos matemáticos. Los programas de ordenador, y
2. las que se oponen al orden público o a las buenas costumbres. Clonación de seres humanos, procedimientos de modificación de la identidad genética del ser humano, etc.

102. ¿Cuál es el contenido del derecho de una patente?

1. Derecho de monopolio sobre el objeto de la patente.
2. Derecho a impedir que terceros exploten, comercialicen o importen el

objeto de la patente sin autorización.

3. Explotación de la patente.

4. Pago de tasas anuales para el mantenimiento de su vida legal.

103. ¿Puede caducar una patente?

Sí, debido al vencimiento de plazo de protección, renuncia del titular, falta de pago de las anualidades o por su no explotación.

104. Riesgos de la patente en el software.

Esto quiere decir que una misma patente puede afectar a un número indeterminado de programas. El coste de desarrollar un software básico sería muy alto, ya que utilizaría multitud de “ideas”.

105. ¿Cuál es el contenido del derecho de marca? ¿Pueden existir dos marcas idénticas?

Derecho exclusivo de la marca para identificar y comercializar un producto/servicio en el mercado. Puede oponerse a que otro la utilice sin su autorización.

Pueden coexistir dos marcas idénticas en un mismo país siempre que los productos o servicios amparados por ellas sean distintos, de forma que no se produzca confusión.

106. ¿Por qué pueden surgir problemas con los nombres de dominio?

1. Es imposible que existan dos nombres de dominio de 2o nivel idénticos bajo el mismo DNS de primer nivel.

2. Piratería en sentido amplio.

3. Conflicto entre marcas y nombres de dominio idénticos o similares, cuando pretenden ser efectivamente usados.

107. ¿Cuándo puede prosperar una demanda debido a un conflicto de nombres de dominio?

Cuando el nombre de dominio en conflicto haya sido registrado de forma especulativa o abusiva.

108. ¿Qué es un secreto industrial?

Es toda información que:

1. No sea generalmente conocida ni fácilmente accesible para personas introducidas en los círculos en que normalmente se utiliza dicha información.

2. Tenga un valor comercial por secreta.

3. Sea objetivo de medidas razonables para mantenerla secreta.

Son conocimientos técnicos o industriales que atesora el empresario, no están patentados y no son conocidos por terceros.