

CICLO: SISTEMAS MICROINFORMÁTICOS Y REDES
MÓDULO: SEGURIDAD INFORMÁTICA (09/0226)
Prueba para la obtención del título Técnico de Formación Profesional
I.E.S. G.M. de JOVELLANOS. (2020/21)

TIEMPO: 60 minutos.

Rellenar en la hoja de respuestas sin tachaduras.

TEST - RESPUESTA ÚNICA. Elija una única respuesta.

Calificación de las preguntas del test:

- Respuesta correcta: + 0'2 puntos.
- Respuesta incorrecta: -0'1 puntos.
- Preguntas sin contestar ni suman ni restan.

ESTA NO ES LA HOJA DE RESPUESTAS (no marque aquí las respuestas).

1: Si una empresa proporciona equipos portátiles para algunos empleados, desde el punto de vista de la seguridad, la mejor opción es:

- a) Nunca salen de las oficinas. Los tienen para poder trabajar solo en las salas de reunión.
- b) Los usan fuera y el empleado tiene privilegios de administración por si necesita instalar algo.
- c) Los discos tienen cifrado de la información almacenada por si el portátil resulta extraviado.

2: En la propiedad de no repudio usamos la firma electrónica y su función es, ante un problema...

- a) Proteger al destinatario y al emisor.
- b) Proteger únicamente al emisor.
- c) Garantizar el control de acceso mediante la autenticación.

3: Teniendo en cuenta las propiedades de la información, indica en qué caso no se vería afectada la integridad:

- a) Una amenaza de interrupción.
- b) Una amenaza de modificación.
- c) Una amenaza de fabricación.

4: Definición de SPOF:

- a) Un test para valorar la vulnerabilidad de la red informática de una organización, así como la de todos los dispositivos a los que se puede acceder desde internet, como *routers*, *firewalls*, servidores...
- b) Componente que si falla cae todo el sistema. Puede ser *SW*, *HW* o eléctrico.
- c) Utilizar usuarios que no sean administradores.

5: La temperatura en un CPD (centro de cálculo o Data center) debe estar entre:

- a) Entre 15 y 25° C, que es la temperatura a la que el *hardware* es capaz de funcionar correctamente y es agradable para las personas.
- b) Oscilando muy poco en torno a los 22° C.
- c) Entre 10 y 32° C siempre que la humedad esté entre el 40 % y el 50 %.

6: La seguridad en un edificio, local o CPD es:

- a) Física y activa.
- b) Activa y pasiva.
- c) Física, activa y pasiva.

CICLO: SISTEMAS MICROINFORMÁTICOS Y REDES
MÓDULO: SEGURIDAD INFORMÁTICA (09/0226)
Prueba para la obtención del título Técnico de Formación Profesional
I.E.S. G.M. de JOVELLANOS. (2020/21)

7: ¿Qué activos se están protegiendo al cuidar de la seguridad física de un edificio?

- a) Las personas y el *hardware*.
- b) El *hardware* y la información.
- c) Las personas, el *hardware* y la información.

8: Entre las funciones de los vigilantes de seguridad están:

- a) Comprobación del estado y funcionamiento de las instalaciones generales (electricidad, etc.).
- b) Control de sistemas anti-incendios y de control ambiental.
- c) Identificación de personas y registros en indicios de comisión de actos delictivos.

9: ¿Qué lector no es biométrico?

- a) De tarjetas de proximidad.
- b) De la forma de la mano o de la huella palmar.
- c) De firma.

10: En cuanto a los *racks*:

- a) Tienen unas medidas estándar de 19 pulgadas de ancho.
- b) Tienen unas medidas estándar de una U de alto por cada armario.
- c) Tienen unas medidas estándar de 16 pulgadas de ancho y el alto no está normalizado.

11: Colocar todos los servidores en una sala:

- a) Es malo porque se genera más calor y se estropearán.
- b) Es bueno porque controlamos mejor el calor.
- c) No es bueno. Conviene mezclarlos con ordenadores de usuario, que se calientan menos.

12: Los SAI (UPS) tanto *off-line* como *on-line* se categorizan como elementos:

- a) Activos y físicos.
- b) Pasivos y físicos.
- c) Activos y lógicos.

13: En general, salvo alguna excepción, la copia de seguridad incremental:

- a) Ocupa más que la copia completa.
- b) Ocupa más que la copia diferencial.
- c) Ocupa menos que la copia diferencial.

14: Después de una copia completa, la 1ª copia incremental y la 1ª diferencial:

- a) Deben hacerse fuera del horario de oficina porque tardan mucho y paralizan.
- b) Deben hacerse en horario de oficina para incluir los cambios realizados en vivo.
- c) Ocupan lo mismo porque contienen la misma información.

15: Si tenemos 4 discos de 1 TB en RAID 0 y falla uno de ellos:

- a) El usuario todavía puede acceder a 3 TB de ficheros.
- b) El RAID se ha roto, pero reponiendo el disco podemos recuperarlo.
- c) Hemos perdido todo.

CICLO: SISTEMAS MICROINFORMÁTICOS Y REDES
MÓDULO: SEGURIDAD INFORMÁTICA (09/0226)
Prueba para la obtención del título Técnico de Formación Profesional
I.E.S. G.M. de JOVELLANOS. (2020/21)

16: Si ejecuto una herramienta S.M.A.R.T. para Windows, y luego sobre el mismo disco lo mismo en Linux. ¿Debería tener el mismo resultado?

- a) Sí, porque S.M.A.R.T es un estándar. Da igual bajo qué sistema operativo esté funcionando la herramienta porque obtiene la información de los sensores del *hardware*.
- b) No, los parámetros serán distintos en cada sistema operativo, cada uno tiene sus sensores.
- c) S.M.A.R.T. no se puede ejecutar desde un sistema operativo, se hace en el arranque del PC.

17: Los principales tipos de memoria secundaria son:

- a) Magnéticos, ópticos y los basados en memoria *flash*.
- b) RAM, ROM y BIOS.
- c) Cintas, que duran 5 años y discos, que duran 20 años.

18: ¿Qué protocolo(s) de traducción de direcciones en IPv4 supuso una medida de seguridad "involuntaria" para proteger las redes locales de intrusiones externas?

- a) NAT/PAT
- b) IPSec
- c) SSL/TLS

19: Localiza la única definición que no es correcta:

- a) SUPLANTACIÓN: El atacante se hace pasar por un tercero, para dar información falsa o fraudulenta (DNS Spoofing, ARP spoofing, email spoofing, etc.)
- b) INTERCEPTACIÓN: La información que viaja por la red es desviada hacia otro destino (con técnicas conocidas como "secuestro" (Hijacking))
- c) DENEGACIÓN DE SERVICIO: Alguien consigue "colarse" a través de la red y acceder a servicios que le permiten obtener información confidencial (archivos, mensajes, datos).

20: Las formas de actuar que tiene un "antivirus" común para detectar *MALWARE* como virus, gusanos o troyanos es (marque la única definición correcta):

- a) Al vuelo: Buscan *malware* por indicación del usuario en memoria secundaria
- b) A propósito: Mientras se ejecutan programas (y pasan de memoria secundaria a principal) o cuando se insertan dispositivos de memoria secundaria o en tráfico de red que pasa por la NIC.
- c) Durante el arranque: Cuando aún no ha cargado el S.O. busca *rootkits* y otro *malware*.

21. El envenenamiento ARP consiste en:

- a) Configurar los equipos para que utilicen tablas ARP estáticas.
- b) Desinstalar el protocolo ARP.
- c) Enviar respuestas ARP no solicitadas.

22: Contra un ataque por envenenamiento ARP:

- a) Podríamos bloquear el tráfico ARP en todos los *routers* de la red.
- b) Podríamos utilizar tablas ARP generadas estáticamente desde un *switch*.
- c) Podemos introducir un servidor o SW que identifique este comportamiento anómalo.

23: El AP spoofing consiste en:

- a) Colocar un punto de acceso falso y abierto en sitio público para hacer un MITM.
- b) Falsear la resolución de nombre, redirigiendo navegadores y clientes a direcciones falsas.
- c) Enviar paquetes *ping* (ICMP) y con las respuestas obtener datos básicos sobre el sistema.

CICLO: SISTEMAS MICROINFORMÁTICOS Y REDES
MÓDULO: SEGURIDAD INFORMÁTICA (09/0226)
Prueba para la obtención del título Técnico de Formación Profesional
I.E.S. G.M. de JOVELLANOS. (2020/21)

24: El ataque MITM puede realizarse mediante:

- a) *Hardware*: Atacante se interpone en algún tramo de la conexión física entre máquinas atacadas.
- b) *Software*: el atacante engaña a máquinas atacadas haciéndose pasar por alguna de ellas.
- c) Las respuestas a y b son correctas.

25: Si el ataque MITM tiene éxito, a continuación:

- a) Podemos lanzar ataques de fabricación.
- b) Podemos lanzar ataques de interceptación, fabricación e interrupción.
- c) Podemos lanzar ataques de interceptación.

26: Elija la afirmación correcta:

- a) Los usuarios deben tener el menor nivel de permisos que permita trabajar.
- b) Debe programarse copias de seguridad para que, en caso de un ataque pasivo, pueda restaurarse el sistema a un estado anterior.
- c) Debe cambiarse en el BIOS el orden de los dispositivos de arranque para colocar en primer lugar el CD/DVD o una unidad portátil y después el disco duro principal.

27: La firma digital:

- a) Permite verificar la identidad y garantiza el no repudio.
- b) Sirve principalmente para garantizar la confidencialidad de la información.
- c) Garantiza la privacidad de las informaciones particulares.

28: En el cifrado simétrico:

- a) La clave debe ser conocida por emisor y receptor.
- b) La clave debe conocerla solo el que cifra la información.
- c) Se usa una clave para cifrar y otra para descifrar.

29: Un sistema de cifrado "híbrido" consiste en:

- a) Transportar la clave de un sistema simétrico mediante el uso de un sistema asimétrico.
- b) Transportar la clave de un sistema asimétrico mediante el uso de un sistema simétrico.
- c) Transportar las claves de un sistema asimétrico mediante el uso de un sistema híbrido.

30: Elija la afirmación correcta:

- a) AES y RSA son ejemplos de algoritmos simétricos.
- b) RSA y AES son ejemplos de algoritmos asimétricos.
- c) RSA es un ejemplo de algoritmo asimétrico y AES de algoritmo simétrico.

31: La principal diferencia entre IPSec y SSL/TLS es que:

- a) SSL usa un servidor RADIUS mientras que IPSec utiliza TKIP.
- b) IPSec actúa en el nivel de red por lo que se puede utilizar para cifrar datos de TCP y UDP.
- c) SSL/TLS actúa a nivel de red por lo que se puede utilizar para cifrar datos TCP y UDP.

32: Los certificados digitales con autoridades de certificación:

- a) Imposibilitan la duplicidad de claves y las protegen mediante un PIN.
- b) Jamás usan soportes físicos, siempre se almacenan en software (archivos .cer).
- c) Aunque se usan para firmar no tienen la misma validez que la firma manuscrita.

CICLO: SISTEMAS MICROINFORMÁTICOS Y REDES
MÓDULO: SEGURIDAD INFORMÁTICA (09/0226)
Prueba para la obtención del título Técnico de Formación Profesional
I.E.S. G.M. de JOVELLANOS. (2020/21)

33: Para que (A)lice envíe a (B)ob un texto cifrado asimétricamente:

- a) Alice necesita usar la clave pública de Bob.
- b) Alice necesita usar la clave privada de Bob.
- c) Alice necesita usar su propia clave privada.

34: Para que Alice envíe a Bob un texto firmado asimétricamente:

- a) Alice necesita usar su propia clave pública.
- b) Alice necesita usar su propia clave privada.
- c) Alice necesita usar la clave privada de Bob.

35: Para que Bob descifre un texto cifrado asimétricamente por Alice:

- a) Bob necesita usar la clave pública de Alice.
- b) Bob necesita usar su propia clave privada.
- c) Bob necesita usar la clave privada de Alice.

36: Para que Bob verifique la firma asimétrica de Alice en un texto:

- a) Bob necesita usar la clave pública de Alice.
- b) Bob necesita usar la clave privada de Alice.
- c) Bob necesita usar su propia clave privada.

37: Una medida de seguridad lógica y activa sería:

- a) Poner una contraseña en la BIOS del sistema.
- b) Poner unas bridas o un candado para evitar el robo/cambio de un disco duro.
- c) Activar auditoría de eventos para saber si alguien entra en la BIOS del sistema.

38: Para el control de acceso a un sistema se utiliza (elija la correcta):

- a) Por ejemplo, una contraseña (poseer algo).
- b) Por ejemplo, la retina (biometría).
- c) Por ejemplo, una tarjeta de acceso con RFID (biometría).

39: Para que un control de acceso en biometría sea fiable debe ser:

- a) Único: Ha de ser distinto en cada persona.
- b) Caduco: Debe cambiar a menudo, ser reemplazado a corto plazo por seguridad.
- c) Cualificado: Debe poder ser descrito en lenguaje natural o analógico.

40: Los sistemas biométricos son:

- a) Infalibles: La huella dactilar no da lugar a dudas o fallos.
- b) Falibles: Por ello, el sistema puede dar lugar a falsas aceptaciones y falsos rechazos.
- c) Las respuestas a y b son correctas.

41: Una lista de control de acceso o ACL es:

- a) Una lista de usuarios autorizados en un sistema que se hace con el sistema RFID.
- b) Una serie de medidas de seguridad que tiene un sistema (Firewall, antivirus, etc.)
- c) Una forma de determinar los permisos de acceso apropiados a un determinado objeto.

CICLO: SISTEMAS MICROINFORMÁTICOS Y REDES
MÓDULO: SEGURIDAD INFORMÁTICA (09/0226)
Prueba para la obtención del título Técnico de Formación Profesional
I.E.S. G.M. de JOVELLANOS. (2020/21)

42: Elija la respuesta verdadera y correcta:

- a) Si no implantamos cuotas de disco limitadas nos podemos encontrar con problemas de DoS.
- b) Las auditorías del sistema operativo son una medida de seguridad activa.
- c) Principio básico: todo lo que no está prohibido debe estar permitido de manera irrevocable.

43: ¿Qué es un FIREWALL?

- a) Es un dispositivo físico que inspecciona y filtra el tráfico entre redes.
- b) Es un *software* sobre un sistema operativo que inspecciona y filtra el tráfico entre redes.
- c) Ambas son correctas.

44: Las reglas de un FIREWALL...

- a) Filtran en función de parámetros de nivel de red.
- b) Filtran en función de parámetros de nivel de transporte.
- c) Ambas son correctas.

45: Acciones posibles en IPTABLES son (marque la correcta):

- a) DROP: El FIREWALL deniega el paso de los paquetes que configuremos con esta opción.
- b) DENIED: El FIREWALL deniega el paso de los paquetes que configuremos con esta opción.
- c) EJECT: El FIREWALL devuelve al emisor los paquetes que configuremos con esta opción.

46: El esquema de FIREWALL muy usado es el que el que este sistema...

- a) Se ubica entre red local e Internet (para proteger una red local conectada a internet).
- b) Se ubica entre Internet y la DMZ para bloquear el tráfico de la red local al servidor DMZ.
- c) En ningún caso podemos tener más de un FIREWALL porque tendríamos reglas inestables.

47: Para permitir a la máquina IP 192.168.3.10 conectarse por SSH...

- a) iptables -A INPUT -s 192.168.3.10 -p 22 -j ACCEPT
- b) iptables -A INPUT -s 192.168.3.10 -p tcp --dport 22 -j ACCEPT
- c) iptables ACCEPT -j 192.168.3.10 -p tcp --dport 23

48: ¿Puedo nombrar a una empresa externa para que sea mi Delegado de Protección de Datos (DPD) cuyas funciones son entre otras informar, asesorar y supervisar el cumplimiento del RGPD?

- a) Sí. El DPD podrá ser interno o externo, persona física o jurídica.
- b) No. Debe ser un trabajador de la empresa con estudios de derecho o jurídicos.
- c) No. Debe ser el jefe/dueño de la empresa que cuente con 5 o más años de antigüedad.

49: ¿Qué se entiende por datos de carácter personal?

- a) Cualquier información que da una persona como sus gustos, opinión religiosa, sexo, etc.
- b) Cualquier información sobre el carácter personal: afable, simpático, alegre, paciente, etc.
- c) Información que identifique o permita identificar a una persona o que puede establecerse obteniendo otros datos adicionales.

50: ¿Quién tiene la obligación de adecuarse a la RGPD?

- a) Solo las empresas que tienen una tienda *on-line*.
- b) Cualquier persona física y/o jurídica que trate con datos de carácter personal.
- c) Las compañías que hacen encuestas online, aunque no recojan datos personales.