

**PRIMER EJERCICIO DE LA FASE DE OPOSICIÓN PLAZA CIBERSEGURIDAD.
PREGUNTAS TIPO TEST.**

1. Cuál de los siguientes derechos es un derecho fundamental según la Constitución Española.
 - a) Asociación.
 - b) Propiedad privada
 - c) Trabajo.
 - d) Régimen de Seguridad Social

2. Indique la respuesta correcta relacionada con la Ley de Igualdad 3/2007, de 22 de marzo.
 - a) constituye acoso sexual cualquier comportamiento, verbal o físico, de naturaleza sexual que tenga el propósito o produzca el efecto de atentar contra la dignidad de una persona, en particular cuando se crea un entorno intimidatorio, degradante u ofensivo.
 - b) Las obligaciones establecidas en esta Ley serán de aplicación solo a las personas físicas que se encuentre o actúe en territorio español.
 - c) La igualdad de trato y de oportunidades entre mujeres y hombres no es un principio informador del ordenamiento jurídico.
 - d) No constituye discriminación directa por razón de sexo todo trato desfavorable a las mujeres relacionado con el embarazo o la maternidad.

3. ¿La Ley Orgánica de Universidades será de aplicación?
 - a) Solo a las universidades públicas españolas
 - b) Solo a las universidades privadas españolas
 - c) A las universidades públicas y privadas españolas
 - d) A las universidades públicas y privadas españolas, excepto a las universidades catalanas y vascas

4. ¿Cuál de las siguientes normas es básica para funcionarios públicos?
 - a) Texto Refundido del Estatuto Básico del Empleado Público
 - b) Convenio Colectivo de Personal Funcionario de la AGE
 - c) Ley de la Contrareforma de la Función Pública
 - d) Acuerdo intersectorial de los funcionarios públicos

5. ¿Qué tipo de concursos de provisión de puestos de trabajo pueden convocarse en el ámbito de los funcionarios públicos?
 - a) Concurso de méritos generales y méritos específicos
 - b) Solo concurso de méritos generales
 - c) Solo concurso de méritos específicos
 - d) Concurso-oposición

6. ¿Cuál de las siguientes situaciones administrativas es una excedencia en el ámbito de los funcionarios públicos?
- Excedencia por servicio en otras administraciones Públicas
 - Excedencia por servicios especiales
 - Excedencia por cuidado de familiares
 - Excedencia por servicio activo
7. ¿Cuál de los siguientes conceptos no es una retribución de los funcionarios públicos?
- Sueldo
 - Complemento de destino
 - Complemento de especialización
 - Complemento específico
8. Las personas que no posean ninguna titulación académica habilitante para acceder a la universidad por otras vías podrán acceder mediante la vía de acreditación de experiencia laboral o profesional en relación con una enseñanza, para lo cual:
- Deberán superar una prueba de acceso que constará de una fase general y una fase específica.
 - Deberán superar una prueba de acceso adaptada.
 - Se incluirá en todo caso la realización de una entrevista personal con el candidato.
 - Deberán cumplir o haber cumplido los 45 años de edad en el año natural de comienzo del curso académico.
9. Los planes de estudios de las enseñanzas universitarias oficiales:
- Serán elaborados por las universidades y verificados por la Conferencia General de Política Universitaria.
 - Serán elaborados por las universidades y verificados por el Consejo de Universidades.
 - Serán elaborados por las universidades y verificados por la Comunidad Autónoma correspondiente.
 - Serán elaborados por las universidades y verificados por el Gobierno mediante Real Decreto.
10. De acuerdo con el Real Decreto 822/2021 de 28 de septiembre, por el que se establece la organización de las enseñanzas universitarias y del procedimiento de aseguramiento de su calidad, todos los títulos universitarios oficiales de Grado y de Máster Universitario deberán adscribirse a:
- Una de las ramas del conocimiento relacionadas en el anexo I del mencionado Real Decreto.
 - Uno de los ámbitos del conocimiento relacionados en el anexo I del mencionado Real Decreto.
 - Una de las áreas del conocimiento relacionadas en el anexo I del mencionado Real Decreto.
 - Uno de los campos del conocimiento relacionados en el anexo I del mencionado Real Decreto.

11. Según normativa de la Universidad Autónoma de Madrid, los requisitos para la permanencia en los estudios oficiales iniciados incluyen:
- Superar, cada curso académico, como mínimo el 25 % de los créditos matriculados en los estudios de grado o el 50 % en los estudios de máster.
 - Superar, cada curso académico, como mínimo el 25 % de los créditos matriculados en los estudios de grado o el 70 % en los estudios de máster.
 - Superar, cada curso académico, como mínimo el 20 % de los créditos matriculados en los estudios de grado o el 50 % en los estudios de máster.
 - Superar, cada curso académico, como mínimo el 20 % de los créditos matriculados en los estudios de grado o el 70 % en los estudios de máster.
12. De acuerdo con la Ley 47/2003, de 26 de noviembre, General Presupuestaria, podrán adquirirse compromisos de gastos plurianuales que hayan de extenderse a ejercicios posteriores a aquel en que se autoricen, siempre que su ejecución se inicie en el propio ejercicio y no se superen los límites y anualidades indicados en dicha ley. El gasto que se impute a cada uno de los ejercicios posteriores no podrá exceder de la cantidad que resulte de aplicar al crédito inicial a que corresponda la operación los siguientes porcentajes:
- En el ejercicio inmediato siguiente, el 70 por ciento, en el segundo ejercicio, el 60 por ciento, en el ejercicio tercero, el 50 por ciento y en cuarto, el 40 por ciento.
 - En el ejercicio inmediato siguiente, el 60 por ciento, en el segundo ejercicio, el 50 por ciento, en el ejercicio tercero, el 40 por ciento y en cuarto, el 30 por ciento.
 - En el ejercicio inmediato siguiente, el 75 por ciento, en el segundo ejercicio, el 50 por ciento, y en los ejercicios tercero y cuarto, el 25 por ciento.
 - En el ejercicio inmediato siguiente, el 70 por ciento, en el segundo ejercicio, el 60 por ciento, y en los ejercicios tercero y cuarto, el 50 por ciento.
13. De acuerdo con su clasificación económica, el capítulo 6 del presupuesto de gastos de la Universidad Autónoma de Madrid se denomina:
- Inversiones reales.
 - Gastos financieros.
 - Transferencias de capital.
 - Pasivos financieros.
14. Los traspasos que se producen entre partidas con distinto nivel de vinculación jurídica tendrán la consideración de:
- Transferencias de crédito.
 - Ampliaciones de crédito.
 - Incorporaciones de crédito.
 - Redistribuciones de crédito.

15. Un Sistema de Soporte a la Decisión (DSS):
- No es interactivo.
 - Está orientado principalmente a los líderes ejecutivos.
 - Requiere de conocimientos técnicos.
 - Almacena y recopila la información necesaria para que la administración tome las medidas adecuadas en el momento correcto.
16. ¿Cuál es el órgano máximo de Gobernanza TIC de la Administración General del Estado y sus Organismos Públicos?
- Comisión de Estrategia TIC.
 - Comisión Ministerial para la Administración Digital.
 - Secretaría General de Administración Digital.
 - Comité de Dirección de las Tecnologías de Información y Comunicaciones.
17. ¿Cuál de las siguientes funciones corresponde a un DBA?
- Actuar como punto único de contacto al usuario final.
 - Gestión de los usuarios de la red.
 - Establecer el diccionario de datos.
 - Monitorizar el correcto funcionamiento de los sistemas.
18. ¿Qué metodología o buenas prácticas debe utilizarse para la gestión de las licencias y el software que se utilizan en una empresa?
- Métrica.
 - ITIL.
 - CMMI.
 - SAM.
19. ¿Cuál de estas afirmaciones sobre un director de sistemas de la información NO es correcta?
- Debe tener capacidad de planear, hacer convivir y hacer evolucionar tecnologías de diferentes generaciones, lenguajes, conocimientos, etc.
 - Debe diseñar y adaptar los sistemas informáticos para mejorar el funcionamiento de la empresa.
 - Debe transformar la organización con el uso de la tecnología, reingeniería de procesos y gestión del cambio.
 - Debe asegurar y gestionar la aplicación de estándares dentro de la empresa y del sector.

20. El protocolo PXE utiliza los siguientes protocolos:
- BOOTP/DHCP, FTP y TCP/IP.
 - TFTP, TCP/IP y direccionamiento estático en los clientes.
 - TCP/IP, BOOTP/DHCP y TFTP.
 - FTP, TCP/IP y WoL en los clientes.
21. Si en un CPD se dispone de un equipo de climatización capaz de cubrir toda la necesidad de la sala. ¿Cuál sería el mínimo, según el estándar de The Uptime Institute, para poder disponer de redundancia?
- 2N.
 - N.
 - 2N+1.
 - 2(N+1).
22. ¿Qué tipo de herramienta debe utilizarse para la gestión centralizada de dispositivos móviles?
- Wrike.
 - MRTG.
 - BYOD.
 - MDM.
23. Una copia instantánea o punto de control en una máquina virtual:
- Es lenta de crear, pero muy segura.
 - Conserva el estado de la máquina y los datos en el momento en el que se crea dicha copia.
 - Es un buen sustituto a los sistemas de backup.
 - Te permite tener un histórico del servidor del que se hace la copia.
24. Si queremos conocer las librerías vinculadas a un determinado programa en un sistema Linux usaremos el comando:
- linked.
 - lk.
 - ln.
 - ldd.
25. La estructura de un Directorio Activo se basa en los siguientes conceptos:
- Directorios, Unidades físicas y Usuarios.
 - Dominio, Unidad Organizativa, Grupos y Objetos.
 - Unidades físicas, Unidades lógicas y Directorios.
 - Ficheros, Directorios, Particiones y Unidades.

26. ¿Cuál de las siguientes afirmaciones de seguridad sobre MacOS NO es incorrecta?
- Desde Catalina (MacOS 10.15), el sistema operativo se almacena en una partición del disco en modo sólo lectura.
 - Es seguro instalar MacOS en equipos PC que no sean Macintosh.
 - El acceso al código fuente del sistema operativo está restringido, permitiéndose sólo al personal autorizado de Apple.
 - Se puede cifrar el contenido del disco duro con el sistema de encriptación FileVault desde el menú de Preferencias del Sistema.
27. ¿Cuáles son las capas de la arquitectura de 3 niveles de IoT?
- Percepción, Red y Aplicación.
 - Red, Transporte y Niebla.
 - Percepción, Transporte y Negocios.
 - Red, Procesamiento y Negocios.
28. Indica cuál de las siguientes respuestas es INCORRECTA:
- Una de las utilidades de las funciones hash es la detección de malware.
 - Firmando un mensaje con una función hash aseguramos su no repudio.
 - Haciendo uso de funciones hash podemos hacer un control de archivos duplicados.
 - Las contraseñas pueden protegerse utilizando una función hash.
29. Indica la respuesta INCORRECTA. Una firma electrónica avanzada:
- está vinculada con los datos firmados por la misma de modo que cualquier modificación ulterior de los mismos sea detectable.
 - Está vinculada al firmante de manera única.
 - Permite la identificación del firmante.
 - Tiene mayor nivel de seguridad que la firma electrónica cualificada.
30. El protocolo OCSP, se utiliza en:
- La comprobación de la validez de una trama.
 - La comunicación entre sistemas abiertos.
 - La validación en tiempo real del certificado digital.
 - La validación de la dirección de origen de un equipo.
31. Una brecha de datos personales, que pueda constituir un riesgo a los derechos y libertades de las personas:
- Debe comunicarse a la Autoridad de Control en un plazo máximo de 48h.
 - Debe comunicarse siempre a las personas afectadas.
 - Debe comunicarse a la AEPD cuando el establecimiento principal de la empresa se encuentre en cualquier país de la Unión Europea, independientemente del país de los afectados.
 - Si se trata de ámbito público, debe comunicarse a la AEPD, en todas las Comunidades Autónomas españolas salvo Cataluña, País Vasco y Andalucía.

32. La especificación OVF es un:

- a. Formato abierto para gestores de bases de datos volátiles.
- b. Formato abierto para aplicaciones ofimáticas.
- c. Estándar abierto para empaquetar y distribuir software para ejecutar en máquinas virtuales.
- d. Estándar abierto para formatos de imagen admitido en la NTI de catálogo de estándares.

33. ¿Cuál de los siguientes tipos de datos según su estructura NO existe en el entorno de Big Data?

- a. Estructurados.
- b. Semiestructurados.
- c. Autoestructurados.
- d. No estructurados.

34. Lenguaje de marca que utiliza símbolos autodefinidos e ilimitados:

- a. HTML.
- b. XML.
- c. XHTML.
- d. W3C.

35. El protocolo OSPF:

- a) Es un protocolo de encaminamiento como el RIP
- b) Significa "Open Systems Protocol Family"
- c) No usa el algoritmo tipo de estados de enlaces (link-state) para encaminar los datagramas
- d) Se basa en un modelo mixto de rutas dinámicas y estáticas.

36. Las características fundamentales que se buscan con los sistemas abiertos son:

- a) Interoperabilidad, escalabilidad y portabilidad
- b) Sistemas multiproceso, multiusuario y multitarea compuestos por componentes de diversos fabricantes
- c) Poder pasar de un ordenador de sobremesa a un gran mainframe sin tener que cambiar de entorno de trabajo
- d) Interconexión de sistemas bajo un mismo sistema operativo, conectividad de periféricos, un entorno consistente en productos y tecnologías y un mejor posicionamiento desde el punto de vista económico

37. En redes conmutadas, se llama enlace trunk:

- a) Es un enlace lógico que agrega diferentes enlaces físicos para aumentar la tolerancia a fallos y el caudal disponible
- b) Es un enlace de interconexión entre routers que no extiende dominios de broadcast
- c) Es un enlace por el que se transmiten múltiples VLANs
- d) Es un enlace en el que conviven diferentes protocolos de nivel de acceso a la red

38. En un entorno de desarrollo Python ¿Qué es Django?
- a) Un entono de desarrollo integrado que permite editar, probar y ejecutar el código Python.
 - b) Es un framework de componentes Python (estructura, módulos y librerías, plantillas, formularios) que facilitan el desarrollo de nuevas aplicaciones.
 - c) Un gestor de paquetes para descarga e instalar módulos adicionales de Python.
 - d) Una base de datos específica para la programación de aplicaciones Python.
39. En una red local ¿Qué equipo de comunicaciones se utilizará para interconectar dos ordenadores situados en distinta VLAN?
- a) Un conmutador de nivel 2 (switch).
 - b) Un encaminador (router) con conexión en ambas VLAN.
 - c) Un concentrador (HUB)
 - d) Un sistema de gestión de red.
40. En un entorno de red con acceso autenticado 802.1X, ¿Qué tipo de autenticación EAP exige el uso de certificados de cliente y de servidor?
- a) EAP-TTLS
 - b) EAP-PEAP
 - c) EAP-LEAP
 - d) EAP-TLS
41. En backups, ¿qué indica el RTO?
- a) Nos indica la cantidad máxima de información que podemos perder.
 - b) Nos indica la cantidad máxima de información que podemos salvaguardar.
 - c) Nos indica el tiempo máximo de recuperación.
 - d) Nos indica el tiempo promedio en creación de backups.
42. ¿La gestión de claves en IPsec se realiza a través del protocolo:
- a) IKE
 - b) AH
 - c) ESP
 - d) A través de los protocolos AH y ESP.
43. En un sistema GIT ¿Cuál es el comando utilizado para listar los cambios (commits) que se han producido en el repositorio?
- a) git ls
 - b) git log
 - c) git dir
 - d) git pending

44. ¿A qué capa del modelo OSI correspondería el protocolo TCP?
- a) Capa de red 3
 - b) Capa de sesión 5
 - c) Capa de presentación 6
 - d) Capa de transporte 4
45. ¿Qué es DevOps?
- a) Es un modelo de ciclo de vida del software que sigue las fases de Desarrollo (Dev) y Operación (Ops).
 - b) Es una herramienta para la gestión de proyectos ágiles.
 - c) Es una metodología de desarrollo en la que equipos aislados colaboran para lograr el desarrollo más eficiente.
 - d) Es una práctica de ingeniería de software que tiene como objetivo unificar el desarrollo de software (Dev) y la operación del software (Ops) en el ciclo de vida del producto.
46. ¿Qué estándar de Telefonía IP soporta la centralita open-source Asterisk?
- a) IAX
 - b) SIP
 - c) H.323
 - d) SIP y H.323
47. Gestión de documentos (DMS) y gestión de contenidos (CMS), indique la respuesta correcta:
- a) Son la misma cosa.
 - b) Sólo se diferencian en la tecnología utilizada, pero gestionan lo mismo.
 - c) En la gestión de documentos se suele presentar y gestionar el documento en su formato original, mientras que en la gestión de contenidos se orienta hacia la creación y edición dinámica de páginas web.
 - d) La gestión de contenidos es más reciente y suele estar enfocada hacia flujos de trabajo.
48. El mecanismo por el que el operador de una red evita que se produzca congestión descartando el tráfico que inyecta un usuario concreto que supere el caudal contratado se denomina:
- a) Traffic shapping
 - b) Traffic policing
 - c) Traffic admission
 - d) Traffic monitoruál
49. En el entorno de un sistema de monitorización y telemetría para una infraestructura TIC ¿Qué LOGS incluiría en las mediciones?
- a) Sólo los LOGS de funcionamiento de los servidores
 - b) Los LOGS de servidores, aplicaciones, red, etc que puedan afectar al desarrollo del negocio
 - c) Ninguno, los LOGS no formarían parte de un sistema de monitorización y telemetría.
 - d) Únicamente los relativos a las aplicaciones críticas del negocio

50. En un entorno de redes de ordenadores que es un conmutador (Switch L2)
- a) Es un dispositivo de red que sirve para interconectar diversos equipos pertenecientes a una misma red
 - b) Es un dispositivo que permite interconectar dos redes diferentes
 - c) Es un equipo que permite la monitorización de una red
 - d) Es un equipo que permite agregar diferentes redes en una única.
51. En un entorno de servicios web ¿que define el estándar "Web Service Description Language" (WSDL)?
- a) Es un lenguaje basado en XML donde se describe la interfaz pública de los servicios WEB
 - b) Es un protocolo estándar que define cómo dos objetos, en diferentes procesos, pueden comunicarse por medio de intercambio de datos XML
 - c) Es el registro de servicios web de una organización en el catálogo de negocios
 - d) Es una interfaz de programación de aplicaciones web
52. ¿Qué tipo de registro DNS asocia un nombre de alias con otro nombre de dominio auténtico?
- a) CNAME
 - b) AAAA
 - c) LOC
 - d) NS
53. ¿Cuál es el propósito de la gestión de configuración?
- a) Controlar el acceso al código por parte de los programadores
 - b) Mantener los parámetros de configuración de los sistemas y aplicaciones
 - c) Llevar un control del proyecto
 - d) Mantener un control exhaustivo de los cambios en los sistemas y aplicaciones
54. ¿A qué se corresponden las siglas IEEE 802.11i sobre redes inalámbricas?:
- a) A especificaciones de nivel físico.
 - b) A especificaciones sobre Calidad de Servicio QoS (Quality ofService).
 - c) A especificaciones de Seguridad.
 - d) A selección dinámica de frecuencias.
55. ¿Para que sirve el siguiente código PHP?
- ```
if (isset($variable)) {}
```
- a) Recorre un array de nombre \$variable
  - b) Crea una variable de nombre "\$variable"
  - c) Verifica si la variable "\$variable" está definida y tiene un valor no nulo
  - d) Verifica si la variable "\$variable" ha reservado espacio en memoria

56. Atendiendo a lo recogido en las medidas de protección del Anexo de Medidas de Seguridad del ENS, ¿Cuándo es necesario emplear sistemas de cortafuegos con dos o más equipos de diferente fabricante puestos en cascada?

- a) Sistemas de Categoría Básica o superior.
- b) Sistemas de Categoría Media o superior.
- c) Sistemas de Categoría Alta.
- d) La utilización de sistemas de cortafuegos de diferente fabricante puestos en cascada no es un requisito obligatorio dentro de las medidas de protección del ENS.

57. ¿Cuáles son los contenidos mínimos de la política de seguridad, de acuerdo con el Esquema Nacional de Seguridad?

- a) Los objetivos o misión de la organización y el marco legal y regulatorio en el que se desarrollarán las actividades.
- b) Los objetivos o misión de la organización, el marco legal y regulatorio en el que se desarrollarán las actividades y los roles o funciones de seguridad.
- c) Los objetivos o misión de la organización, el marco legal y regulatorio en el que se desarrollarán las actividades, los roles o funciones de seguridad, la estructura del comité o comités para la gestión y coordinación de la seguridad y las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.
- d) Los objetivos o misión de la organización, el marco legal y regulatorio en el que se desarrollarán las actividades, los roles o funciones de seguridad y la estructura del comité o comités para la gestión y coordinación de la seguridad.

58. En el marco de la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales, sobre el acceso por parte del empleador al contenido de un dispositivo digital respecto del que se haya permitido su uso con fines privados. ¿cuál de las siguientes afirmaciones es correcta?

- a) No se podrán utilizar dispositivos del empleador con fines privados
- b) Los trabajadores y los empleados públicos no tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador.
- c) Los empleadores deberán establecer criterios de utilización de los dispositivos digitales y en su elaboración deberán participar los representantes de los trabajadores.
- d) El acceso al contenido de un dispositivo digital propiedad del empleador, requiere de la autorización expresa del trabajador, que podrá denegar el permiso para dicho acceso.

59. En el marco de la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales, ¿Cuál es la edad a partir de la cual un menor puede otorgar el consentimiento?

- a) 13 años.
- b) 14 años.
- c) 15 años.
- d) 16 años.

60. Según el Reglamento General de Protección de Datos, ¿en cuál de las siguientes situaciones NO es obligatoria la realización de una Evaluación de Impacto relativa a la Protección de Datos?

- a) Tratamiento de datos a gran escala.
- b) Control de zonas de acceso de un Centro Comercial.
- c) Evaluación sistemática y exhaustiva de aspectos personales propios de personas físicas, basada en la elaboración de perfiles.
- d) Datos personales de pacientes, realizado por un solo médico u otro profesional de la salud.

61. ¿En qué circunstancias los prestadores de servicios de la sociedad de la información no son responsables por la información que proporcionen a los destinatarios de sus servicios?

- a) Cuando el proveedor de contenidos al que se enlace o cuya localización se facilite actúe bajo la dirección, autoridad o control del prestador que facilite la localización de esos contenidos.
- b) Siempre que tengan conocimiento de la ilicitud de la información o de que lesiona derechos o bienes de un tercero susceptible de indemnización y aleguen la imposibilidad de suprimir o inutilizar el enlace.
- c) Cuando el proveedor de contenidos al que se enlace o cuya localización se facilite desconozca el contenido ilícito de dicha información.
- d) Siempre que no tengan conocimiento efectivo de la ilicitud de la información o de que lesiona derechos o bienes de un tercero susceptible de indemnización o si lo tienen, actúen de forma diligente para suprimir o inutilizar el enlace.

62. La Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, en el artículo 45 detalla la prescripción para las sanciones e infracciones. Señale la respuesta correcta:

- a) Infracciones muy graves prescribirán a los 3 años, las graves al año y las leves a los 6 meses.
- b) Las sanciones impuestas por faltas muy graves prescribirán a los 3 años, las impuestas por faltas graves a los 2 años y las impuestas por faltas leves a los seis meses.
- c) Las infracciones muy graves prescribirán a los 5 años, las graves a los 3 años y las leves al año.
- d) Sanciones impuestas por faltas muy graves prescribirán a los 3 años, las impuestas por faltas graves a los 2 años y las impuestas por faltas leves al año.

63. En el marco del RD 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. ¿Cuál de las siguientes afirmaciones es correcta, respecto del ámbito de aplicación?

- a) Estarán sometidos a este decreto los servicios digitales que sean mercados en línea, motores de búsqueda en línea y servicios de computación en nube.
- b) Los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios electrónicos de confianza que no sean designados como operadores críticos en virtud de la Ley 8/2011, de 28 de abril.
- c) Los proveedores de servicios digitales cuando se trate de microempresas o pequeñas empresas, de acuerdo con las definiciones recogidas en la Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas.
- d) Cualquier empresa que preste servicio en España mediante la utilización de tecnologías de comunicaciones digitales, con independencia de su estructura o tamaño.

64. El RD 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. En el caso de los operadores esenciales, establece los contenidos mínimos de la política de seguridad de las redes y sistemas de información, atendiendo a los principios de:

- a) Gestión de riesgos y relación con CERTs de referencia.
- b) Seguridad integral y procedimiento de adquisición de productos de seguridad.
- c) Seguridad integral, gestión de riesgos, prevención, respuesta y recuperación, líneas de defensa, reevaluación periódica y segregación de tareas.
- d) Garantía de continuidad de operaciones.

65. En el marco de la Orden PCI 487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, ¿cuáles son sus principios rectores?

- a) Unidad de Acción, Anticipación, Eficiencia y Resiliencia.
- b) Gestión de Riesgos, Continuidad de Operaciones, Concienciación y Vigilancia.
- c) Formación y Prevención.
- d) Garantía de derechos y libertades, Impulso a la Industria y Liderazgo Tecnológico.

66. El contenido de la norma ISO 27001:2013, Sistemas de Gestión de la Seguridad de la Información. Requisitos. Se divide en secciones, ¿cuál de las siguientes NO se corresponde con una sección de esta?

- a) Mejora del SGSI.
- b) Auditorías internas.
- c) Responsabilidad de la dirección.
- d) Plan de seguridad.

67. La declaración de aplicabilidad en la norma ISO 27001:2013, necesariamente debe incluir

- a) El plan de tratamiento de riesgos de seguridad de la información.
- b) Si los controles necesarios están implementados o no.
- c) seleccionar las opciones adecuadas de tratamiento de riesgos de seguridad de la información teniendo en cuenta los resultados de la apreciación de riesgos.
- d) El análisis de riesgos detallado de los sistemas de información de la organización.

68. La norma ISO 27002:2013 establece que la Política de Seguridad de la Información, debe ser aprobada por:

- a) El responsable de Seguridad de la Información (CISO) de la organización.
- b) El responsable Financiero de la organización.
- c) La dirección.
- d) El responsable de Tecnologías de la Información.

69. Atendiendo al estándar ISO 22301 en un Plan de Recuperación ante Desastres, el Objetivo de Punto de Recuperación (Recovery Point Objective RPO) es:

- a) El nivel de servicios a proporcionar en modo alterno hasta que se recupere la situación normal.
- b) El tiempo que la organización puede soportar desde que se produce el fallo hasta que se recuperan los servicios críticos.
- c) El tiempo máximo tolerable de interrupción.
- d) La pérdida máxima de datos tolerable en caso de interrupción.

70. En el marco del estándar ISO 22301, la dirección debe asegurarse que los objetivos deben:

- a) Ser establecidos por el director de Tecnologías de la Información.
- b) Ser monitorizados y actualizados como sea apropiado.
- c) Ser objetivos a largo plazo, sin horizonte temporal de ejecución.
- d) Ser independientes de las necesidades y requerimientos aplicables.

71. Respecto del alcance del Marco de Ciberseguridad del NIST, ¿Cuáles son las organizaciones que pueden utilizarlo?

- a) Esta dirigido exclusivamente a infraestructuras críticas y no tiene aplicación al resto de organizaciones.
- b) Está dirigido exclusivamente a organizaciones y empresas de Estados Unidos de América.
- c) Está dirigido a empresas, agencias gubernamentales, excepto para aquellas que se consideren infraestructura crítica.
- d) Está dirigido a infraestructuras críticas, pero puede utilizarlo cualquier organización.

72. ¿Cuál es la serie de las Guías CCN-STIC que aborda el Esquema Nacional de Seguridad?

- a) Serie 100.
- b) Serie 400.
- c) Serie 800.
- d) Serie 900.

73. Atendiendo a la guía CCN-STIC "ESQUEMA NACIONAL DE SEGURIDAD RESPONSABILIDADES Y FUNCIONES", en el caso de una Universidad, el Responsable de Seguridad de la Información:

- a) Deberá depender del director del Servicio de Tecnologías de la Información o similar.
- b) No deberá tener ninguna responsabilidad sobre la prestación de los servicios TIC.
- c) Deberá ser personal externo a la Universidad.
- d) Puede ser ocupado por personal funcionario, de los grupos A1 o A2.

74. De acuerdo con la guía CCN-STIC "ESQUEMA NACIONAL DE SEGURIDAD RESPONSABILIDADES Y FUNCIONES", ¿quién es el responsable de determinar los requisitos del servicio en materia de seguridad del sistema?

- a) Responsable de Seguridad.
- b) Responsable del Servicio.
- c) Delegado de Protección de Datos.
- d) Responsable del Sistema.

75. Desde el punto de vista ITIL, ¿cuál de las siguientes opciones es mejor modelo de "cambio de emergencia"?

- a) Publicación de una nueva versión menor de una aplicación software, planificada con antelación.
- b) Publicación de un parche de seguridad para una aplicación crítica.
- c) Publicación de una versión mayor de una aplicación software, planificada con antelación.
- d) Actualización de bajo riesgo que se implementa como una solicitud de servicio.

76. ¿Qué principio ITIL resalta la importancia de iniciar una acción, en lugar de invertir mucho tiempo en analizar diferentes opciones?

- a) Enfoque en valor.
- b) Mantenerlo simple y práctico.
- c) Progresar iterativamente con retroalimentación.
- d) Empezar donde se está.

77. ¿Cuál de las siguientes funciones no corresponde al Auditor de Sistemas de Información?

- a) Evaluar los controles implantados.
- b) Evaluar los riesgos.
- c) Realizar el análisis funcional.
- d) Evaluar la gestión eficaz de los recursos informáticos.

78. Señale la afirmación correcta sobre las pruebas de cumplimiento de Auditoría Informática:

- a) Verifican el grado de cumplimiento de lo revelado mediante el análisis de la muestra. Proporciona evidencias de que los controles claves existen y que son aplicables efectiva y uniformemente.
- b) Verifican el grado de confiabilidad del SI del organismo.
- c) Se suelen obtener mediante observación, cálculos, muestreos, entrevistas, técnicas de examen analítico, revisiones y conciliaciones.
- d) Verifican la exactitud, integridad y validez de la información.

79. En el marco de realización del Análisis de Riesgos empleando la metodología MAGERIT, ¿Qué se considera "activo esencial"?

- a) La información que se maneja y los servicios que se prestan.
- b) Los datos almacenados en los sistemas informáticos y las aplicaciones.
- c) El equipamiento informático y de comunicaciones.
- d) El equipamiento informático y de comunicaciones y las personas (usuarios y técnicos).

80. ¿Cuál es la herramienta del CCN-CERT para la realización del Análisis de Riesgos empleando la metodología MAGERIT?

- a) MONARCH.
- b) PIA.
- c) CLARA.
- d) PILAR.

81. ¿Cuál es la herramienta desarrollada por el CCN-CERT para la Gestión de Ciberincidentes en las entidades del ámbito de aplicación del Esquema Nacional de Seguridad?

- a) INES.
- b) CLARA.
- c) GLORIA.
- d) LUCIA.

82. Atendiendo a la taxonomía de referencia para la clasificación de Incidentes de Seguridad de INCIBE, ¿Cuál de los siguientes incidentes se clasificaría como "Intrusión"?

- a) Robo.
- b) Ingeniería social.
- c) Escaneo de redes (scanning).
- d) Análisis de paquetes (sniffing).

83. En ciclo Plan-Do-Check-Act de implantación de un Sistema de Gestión de Seguridad de la Información, ¿cuál de las siguientes actividades se corresponde con la fase Act?

- a) Implementar y gestionar el SGSI de acuerdo a su política, controles, procesos y procedimientos.
- b) Adoptar acciones correctivas y preventivas basadas en auditorías y revisiones internas con el objetivo de mejorar el SGSI.
- c) Establecer la política, objetivos, procesos y procedimientos relativos a la gestión del riesgo.
- d) Medir y revisar las prestaciones de los procesos del SGSI.

84. En el contexto de un SIEM, ¿qué se entiende por normalización?

- a) Ajustar los eventos recibidos a la curva normal, para detectar anomalías.
- b) Estructurar la base de datos del SIEM en tercera forma normal.
- c) Organización de los datos para que aparezcan de forma similar en todos los registros y campos.
- d) Eliminar los falsos positivos, para que sean tratados como eventos "normales".

85. ¿Señale la ventaja que ofrecen los EDR (Endpoint Detection and Response) frente a los antivirus?

- a) Interacción con otras herramientas de seguridad, como SIEM, IPS/IDS o herramientas antimalware.
- b) Detección de virus, gusanos y troyanos.
- c) Incorporan sistemas de mensajería instantánea.
- d) Son más sencillos de desplegar y configurar/administrar.

86. ¿Cuál es el objetivo de un equipo azul (Blue Team) de ciberseguridad?
- a) Realizar las pruebas de intrusión, documentarlas y recabar las evidencias de las vulnerabilidades.
  - b) Proteger los sistemas de la organización para evitar intrusiones.
  - c) Desplegar el SIEM y ajustar su configuración. Delegando en el equipo violeta, las restantes tareas de protección.
  - d) Realizar un reconocimiento de los sistemas de la organización y entregar dicha información al equipo violeta para que realice los test de intrusión de forma dirigida.
87. ¿Cuál de las siguientes evidencias digitales es más difícil de adquirir?
- a) El valor de las cookies del navegador.
  - b) El historial de navegación del perfil del usuario activo.
  - c) Los ficheros de la carpeta de Descargas del usuario activo.
  - d) La clave de sesión de una conexión HTTPS.
88. Señale la característica de un informe técnico forense
- a) Reproducible.
  - b) Basado en conjeturas.
  - c) Siempre tiene carácter probatorio.
  - d) Parte de la hipótesis para llegar a los hechos.
89. ¿Cuál de los siguientes programas tiene entre sus funcionalidades, recuperar un fichero borrado?
- a) Encase Forensic.
  - b) Autopsy.
  - c) Photorec.
  - d) Todos los anteriores permiten intentar recuperar ficheros borrados.
90. ¿Cuál de las siguientes técnicas se encuentra dentro de las tácticas de Movimiento Lateral en la matriz MITRE ATT&CK?
- a) Setuid and Setgid.
  - b) Port Knocking.
  - c) Winlogon Helper DLL.
  - d) SSH Hijacking.

91. En el OAuth 2.0 Authorization Framework (RFC 6749), ¿Qué entidad es la responsable de la creación del "Authorization Grant"?

- a) El cliente.
- b) El propietario del recurso.
- c) El servidor de autorización.
- d) El servidor del recurso.

92. ¿Cuál de las siguientes afirmaciones sobre la utilización de contenedores Docker es cierta?

- a) Ofrece mejor protección que sistemas de virtualización como XEN o VMWare.
- b) Requiere más recursos que los sistemas de virtualización como XEN o VMWare.
- c) Solo pueden desplegarse aplicaciones desarrolladas para Linux.
- d) Para desplegar aplicaciones Windows, es necesario que el sistema anfitrión sea Windows y tenga activada la funcionalidad de contenedores (Container feature).

93. ¿Cómo podría desplegarse un clúster para la ejecución de contenedores docker con varios equipos físicos?

- a) Kubernetes.
- b) Docker.
- c) Kubernetes o Docker en modo swarm.
- d) SeLinux.

94. ¿Cuáles son los flags TCP que activa el sondeo XMas de la herramienta NMap?

- a) SYN, FIN y ACK.
- b) SYN, FIN y URG.
- c) FIN, URG y PSH.
- d) ACK y SYN.

95. ¿Qué funcionalidad de BGP puede ser empleada para comunicar reglas de filtrado de nivel 4 entre encaminadores?

- a) Route Advertisement.
- b) Path Builder.
- c) FlowSpec.
- d) Nearest Neighbour.

96. Un auditor que ha participado en el desarrollo de un sistema podría haber perdido su independencia si:

- a) Realiza una auditoría de otro sistema similar.
- b) Recomienda medidas de mejora.
- c) Realiza una evaluación independiente de la aplicación después de su puesta en producción.
- d) Participa activamente en el diseño e implementación del sistema de aplicación.

97. Señale la afirmación verdadera sobre las pruebas de cumplimiento:

- a) Son aquellas que se aplican para detectar la presencia o ausencia de errores en los procesos o controles, basándose en muestreos estadísticos o buscando específicamente las operaciones de mayor riesgo.
- b) Son aquellas orientadas a comprobar que se cumplen determinados procedimientos de control o procesos establecidos.
- c) Son aquellas dedicadas exclusivamente a probar la existencia de controles.
- d) Son aquellas que se aplican para verificar cumplimiento normativo e incluyen pruebas sustantivas.

98. ¿Como se denomina al documento formal que recoge como primer resultado de la fase de Planificación de una auditoría, la enunciación de los objetivos y alcance de la auditoría?

- a) Plan de auditoría.
- b) Informe de auditoría.
- c) Plan estratégico.
- d) Plan de sistemas.

99. Señale la afirmación incorrecta sobre los factores críticos de éxito de un SGSI

- a) Empezar solo las tareas necesarias y evitar el control excesivo y el desperdicio de recursos valiosos.
- b) Basarse en la formación y sensibilización continua del personal y evitar el uso de medidas disciplinarias y prácticas "policiales" o "militares".
- c) Gestionarse de forma centralizada, sobre la base de una estrategia y una política comunes en toda la organización.
- d) Ser un proceso acotado en el tiempo.

100. ISACA hace referencia a:

- a) A una asociación que promueve un estándar de auditoría y control de los sistemas de información.
- b) A un organismo de certificación de ámbito internacional.
- c) Un protocolo de acceso remoto a datos a través de Internet.
- d) Un organismo internacional de estandarización de sistemas de virtualización de infraestructuras.

**PREGUNTAS DE RESERVA (CONTESTAR CON LOS MISMOS CRITERIOS Y VALORACIÓN QUE LAS ANTERIORES, AUNQUE SOLO SERÁN VALORADAS EN EL CASO DE ANULACIÓN DE ALGUNA/S PREGUNTAS EN EL MISMO ORDEN QUE FIGURAN)**

101. La auditoría informática tiene entre sus normas generales:

- a. Exigencia de evidencia.
- b. Hacer partícipe al usuario.
- c. Formar parte de la empresa auditada.
- d. Informar a las autoridades judiciales.

102. ¿Qué es la Planificación Estratégica?:

- a. Es un proceso puntual.
- b. Es un proceso holístico.
- c. Es un proceso continuo.
- d. Es un proceso objetivo.

103. ¿Qué es la Red SARA?:

- a) Una red pública de interconexión de proveedores de internet.
- b) Un sistema de interconexión e intercambio de información automático entre de redes avanzadas.
- c) Un sistema de interconexión e intercambio de información entre administradores de redes avanzadas.
- d) Un sistema de interconexión e intercambio de información entre redes de Administraciones Públicas Españolas y Europeas, a través de la red s-TESTA.

104. En el prefijo de subred 2001:720:41C::/47, ¿Cuántos bits quedan libres para direccionamiento interno?
- a) 13
  - b) 17
  - c) 23
  - d) 18
105. La norma ISO 27002:2013 se estructura en:
- a) 35 categorías de controles y 114 controles.
  - b) 14 categorías de controles y 97 controles.
  - c) 5 categorías de controles y 230 controles.
  - d) 10 categorías de controles y no tiene establecido un número determinado de controles.
106. ¿Cuáles son las áreas en las que se divide el Marco de Ciberseguridad del NIST?
- a) Planificación, Ejecución, Comprobación y Actuación.
  - b) Identificación, Protección, Detección, Respuesta y Recuperación.
  - c) Planificación, Implementación y Auditoría.
  - d) Análisis, Diseño e Implementación.
107. Un Sistema de Gestión de Seguridad de la Información con certificación vigente en la norma ISO/IEC 27001 implica directamente cumplimiento del Esquema Nacional de Seguridad
- a) Si, siempre.
  - b) No.
  - c) Si, pero habría que comprobar que la Política de Seguridad incluye los aspectos requeridos por el ENS.
  - d) Si, siempre y cuando la organización esté certificada en ISO 22301.
108. ¿En qué fase de un ataque informático se enmarcan los ataques de phishing?
- a) Reconocimiento.
  - b) Entrega.
  - c) Instalación.
  - d) Explotación.

109. ¿Cuál es el plazo para interponer un recurso potestativo de reposición?

- a) Quince días si el acto fuera expreso
- b) Un mes si el acto fuera expreso
- c) Tres meses si el acto fuera expreso
- d) Veinte días si el acto fuera expreso

110. En la clasificación económica del presupuesto:

- a) Los artículos se desglosarán en capítulos y estos, a su vez, en conceptos que podrán dividirse en subconceptos.
- b) Los conceptos se desglosarán en subconceptos y estos, a su vez, en capítulos que se dividirán en artículos.
- c) Los conceptos se desglosarán en subconceptos y estos, a su vez, en artículos que se dividirán en capítulos.
- d) Los capítulos se desglosarán en artículos y estos, a su vez, en conceptos que podrán dividirse en subconceptos.