Ayuntamiento de Alcorcón
Concejalía de Seguridad, Organización Interna y Atención Ciudadana
Nuevas Tecnologías

PROCESO SELECTIVO PARA LA PROVISIÓN DE 1 PLAZA DE TÉCNICO DE SEGURIDAD INFORMÁTICA POR TURNO LIBRE
FASE DE OPOSICIÓN – 1ER EJERCICIO TIPO TEST

1. **La ley orgánica 3/2018, de 5 de diciembre, que en España regula en la actualidad el uso de la información para garantizar la intimidad y la protección de datos personales, atiende a las siglas:**
   - **a)** LOGSE
   - **b)** **LOPDGDD**
   - **c)** LOPMD
   - **d)** RGPD

2. **¿Cuál de las siguientes opciones NO es un formato de firma electrónica?**
   - **a)** CAdES
   - **b)** PAdES
   - **c)** **XmldES**
   - **d)** XAdES

3. **En el Esquema Nacional de Interoperabilidad, se establece que los sistemas y aplicaciones implicados en la provisión de un servicio público por vía electrónica se sincronizarán con la hora oficial de:**
   - **a)** El reloj de la Puerta del Sol
   - **b)** El Instituto Europeo de Medición Horaria
   - **c)** **El Real Instituto y Observatorio de la Armada**
   - **d)** La Agencia Española de Meteorología

4. **En un entorno con criptografía asimétrica, para enviar un mensaje cifrado que sólo ha de ver el receptor, se ha de cifrar con:**
   - **a)** La clave privada del emisor
   - **b)** La clave privada del receptor
   - **c)** La clave pública del emisor
   - **d)** **La clave pública del receptor**

5. **¿Qué comunidad internacional es la responsable de la especificación del lenguaje XML (Extensible Markup Language)?**
   - **a)** **The World Wide Web Consortium (W3C)**
   - **b)** European Telecommunications Satandards Insititute (ETSI)
   - **c)** European Committee for Standardization (GEN)
   - **d)** Massachusetts Institute of Technology (MIT)

6. **Respecto a la seguridad en redes, indique qué es un "Exploit":**
   - **a) Es un malware diseñado para aprovechar la vulnerabilidad de un software**
   - **b)** Persona que accede a datos no autorizados
   - **c)** Adware que modifica la página de inicio de los navegadores de Internet sin el consentimiento del usuario
   - **d)** Software utilizado para la suplantación de la identidad de un usuario de la red

7. **Con respecto a las tecnologías web:**
   - **a) IIS actúa como servidor web de Microsoft**
   - **b)** No se puede acceder a una base de datos Oracle desde un entorno Microsoft
   - **c)** Las páginas ASP solo pueden funcionar sobre servidores Apache
   - **d)** SQL Server solo puede estar asociado a la tecnología PHP

8. **¿Qué es un "honeypot"?**
   - **a)** Un ataque de phishing
   - **b)** Una técnica de encriptación
   - **c) Un sistema para atraer a los atacantes**
   - **d)** Una técnica de ocultación de archivos

9. **Las siglas SSL y TLS se refieren a:**
   - **a)** Diferentes estados lógicos del microprocesador
   - **b) Protocolos criptográficos para establecer conexiones seguras a través de una red**
   - **c)** Sistemas de localización geodésica para GPS
   - **d)** Diferentes tipos de memoria física

10. **Un programa que se aloja en el ordenador y permite el acceso a usuarios externos, con el fin de obtener información o controlar la máquina de forma remota, se denomina:**
    - **a) Troyano**
    - **b)** Gusano
    - **c)** Bot
    - **d)** chatBox

11. **La guía de normas, instrucciones y recomendaciones desarrolladas por el Centro Criptológico Nacional con el fin de mejorar el grado de ciberseguridad de las organizaciones, se denomina:**
    - **a) CCN-STIC**
    - **b)** CCN-SIEM
    - **c)** CCN-ENS
    - **d)** CCN-SOC

12. **¿Cómo se denomina el protocolo encargado de intercambiar correos electrónicos entre dos servidores de correo?**
    - **a)** SPF
    - **b)** TCP
    - **c)** **SMTP**
    - **d)** FTP

13. **Señale cuál de los siguientes servicios de las administraciones públicas NO se presenta en modalidad WEB:**
    - **a)** **Autofirma**
    - **b)** Plataforma de Contratación del Sector Público
    - **c)** Punto General de Entrada de Facturas Electrónicas
    - **d)** Oficina de Registro de Ventanilla Electrónica (ORVE)

14. **Los sistemas de identificación permitidos en la plataforma Cl@ve son:**
    - **a)** **Claves concertadas (Cl@ve PIN 24H y Cl@ve permanente), y certificados electrónicos (incluyendo DNI electrónico)**
    - **b)** Claves concertadas (Cl@ve PIN 24H y Cl@ve permanente), y tarjeta de coordenadas.
    - **c)** Únicamente certificados electrónicos (incluyendo el DNI electrónico)
    - **d)** Únicamente claves concertadas (Cl@ve PIN 24 H y Cl@ve permanente)

15. **Cuando multitud de sistemas atacan un único sistema provocando su caída, estamos ante:**
    - **a)** **Un ataque distribuido de denegación de servicio (DDOS)**
    - **b)** Echelon, una red global de espías
    - **c)** Phishing, denegación por suplantación
    - **d)** Un ataque de ingeniería social

16. **Respecto al funcionamiento del registro electrónico:**
    - **a)** **La presentación en un día inhábil se entenderá realizada en la primera hora del primer día hábil siguiente salvo que una norma permita expresamente la recepción en día inhábil**
    - **b)** La presentación en día inhábil no está permitida
    - **c)** La presentación en un día inhábil se entenderá realizada en la última hora del primer día hábil siguiente, en cualquier caso
    - **d)** Ninguna de las respuestas anteriores es correcta

17. **¿Debe publicar la Administración del Ayuntamiento de Alcorcón un inventario de sus actividades de tratamiento de datos personales?:**
    - **a)** No, nunca
    - **b)** Sí, cuando se traten de datos a gran escala
    - **c)** **Sí, en cualquier caso**
    - **d)** No, aunque puede publicarlo si así lo estima conveniente

18. **¿Cuál es el órgano encargado de supervisar y ayudar a mejorar la accesibilidad de los portales web de la Administración?**
    - **a)** Ministerio de Nuevas Tecnologías y Transformación Digital
    - **b)** Ministerio de la Presidencia
    - **c)** INCIBE
    - **d)** **Observatorio de Accesibilidad Web**

19. **Cuando un atacante suplanta la identidad de un servidor DNS entregando direcciones IP falsas, estamos ante un ataque de tipo:**
    - **a)** DOS
    - **b)** HIJACKING
    - **c)** **SPOOFING**
    - **d)** Ninguna de las respuestas anteriores es correcta

20. **Un ataque Zero-day:**
    - **a)** Intercepta mensajes entre dos víctimas poniéndose el atacante en medio de la comunicación
    - **b)** Es el uso de la línea telefónica convencional y de la ingeniería social para engañar a personas y obtener información delicada como puede ser información financiera o información útil para el robo de identidad
    - **c)** **Aprovecha una vulnerabilidad de un software antes de que se publiquen y apliquen parches que lo corrigen**
    - **d)** Es un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza para manipularla y hacer que suministre datos personales

21. **De acuerdo a la ley de contratos de las Administraciones Públicas, los contratos menores no podrán tener una duración superior a:**
    - **a)** Cinco años
    - **b)** Seis meses
    - **c)** **Un año**
    - **d)** Ninguna de las respuestas anteriores es correcta

22. **De entre los siguientes RAID, ¿Cuál de ellos NO tiene tolerancia a fallos?**
    - **a)** **RAID 0**
    - **b)** RAID 1
    - **c)** RAID 5
    - **d)** RAID 6

23. **Según la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los derechos digitales, los interesados han de estar informados de la posibilidad de ejercitar varios derechos sobre sus datos, señale la respuesta FALSA:**
    - **a)** Acceso
    - **b)** **Certificación**
    - **c)** Rectificación
    - **d)** Supresión

24. **De entre los siguientes mecanismos de seguridad en redes inalámbricas, señale el que actualmente ofrece mayor protección frente a ataques:**
    a) WEP
    b) **WPA3**
    c) WWW
    d) SSID

25. **¿Cuál de las siguientes opciones es un formato que se usa para la sindicación de contenidos?**
    a) SPARQL
    b) **RSS**
    c) CMS
    d) WEBQUEST

26. **Según define el estándar ISO 11801-2:2017, en un sistema de cableado general de entornos de oficinas, ¿Qué elementos interconecta el subsistema de cableado horizontal?**
    a) Las tomas de usuario entre sí
    b) **El distribuidor de planta con las tomas de usuario**
    c) Los distribuidores de edificios entre sí
    d) El distribuidor de campus con los distribuidores de edificio

27. **La Plataforma de Intermediación de Datos ofrece, entre otras funcionalidades:**
    a) Información al ciudadano sobre el estado de sus expedientes
    b) **Servicios web de verificación y consulta de datos**
    c) Gestión de apoderamientos
    d) Acceso del ciudadano a sus notificaciones pendientes y la posibilidad de comparecer en ellas

28. **El protocolo IP es un protocolo:**
    a) No orientado a conexión, Fiable
    b) **No orientado a conexión, No Fiable**
    c) Orientado a conexión, Fiable
    d) Orientado a conexión, No Fiable

29. **De acuerdo al Esquema Nacional de Seguridad, los sistemas de información se podrían clasificar según las siguientes categorías de seguridad:**
    a) Seguridad de Red, Seguridad de Software y Seguridad de Hardware
    b) **Básica, Media y Alta**
    c) Leve, Grave y Muy Grave
    d) El Esquema no identifica categorías de seguridad

30. **¿Cuál de las siguientes características de una web NO se ajusta a los principios de accesibilidad del consorcio W3C?**
    - **a)** **Sólo hay un camino para encontrar las páginas relevantes en un conjunto de páginas web**
    - **b)** El color no se utiliza como única forma de transmitir información o identificar el contenido
    - **c)** Toda la funcionalidad que está disponible con ratón también está disponible con teclado
    - **d)** Contiene breves descripciones del contenido no textual, como archivos de audio y video

31. **De entre los siguientes, el sistema de almacenamiento que realiza el acceso a nivel de bloque es:**
    - **a)** CRS (Cloud Remote Storage)
    - **b)** SAS (Storage Attached Service)
    - **c)** **SAN (Storage Area Network)**
    - **d)** MSN (Massive Storage Network)

32. **Una página o sitio web diseñado y construido para que sus contenidos y servicios estén disponibles para cualquier persona, con independencia de sus capacidades visuales, auditivas, cognitivas o motrices e independientemente de la tecnología que utilizan, es una página o sitio web**
    - **a)** SPA (Single Page Application)
    - **b)** HTML5
    - **c)** **Accesible**
    - **d)** Corporativa

33. **¿Qué Norma Técnica de Interoperabilidad tiene por objeto establecer las condiciones en las que cualquier órgano de una Administración, o Entidad de Derecho Público, accederá a la Red SARA?**
    - **a)** La Norma Técnica de Interoperabilidad de Política Firma y Sello Electrónicos y de Certificados de la Administración
    - **b)** La Norma Técnica de Interoperabilidad de Digitalización de Documentos
    - **c)** **La Norma Técnica de Interoperabilidad de Requisitos de conexión a la red de comunicaciones de las Administraciones Públicas españolas**
    - **d)** La Norma Técnica de Interoperabilidad de Relación de modelos de datos

34. **¿Cuál de los siguientes es un ejemplo adecuado de proceso de respuesta a un incidente de seguridad?**
    - **a)** **Detección, análisis, contención, erradicación y recuperación**
    - **b)** Autenticación, autorización y contabilidad de usuarios
    - **c)** Clasificación, etiquetado y manejo de datos
    - **d)** Inventario de activos, gestión de configuración y control de cambios

35. **El Esquema Nacional de Seguridad que se rige por el RD. 311/2022 establece en el art. 31 que los sistemas han de ser objeto de una auditoría regular ordinaria al menos:**
    - **a)** Cada 6 meses
    - **b)** Cada año
    - **c)** **Cada 2 años**
    - **d)** El Esquema Nacional de Seguridad no especifica nada respecto a auditorías

36. **¿Qué nombre recibe el sistema de información que implementa la Dirección Electrónica Habilitada única?**
    - **a)** CL@Ve
    - **b)** NOTIFIC@
    - **c)** **DEHú**
    - **d)** HABILIT@

37. **¿Qué es un certificado digital?**
    - **a)** Es un conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad del mensaje
    - **b)** **Es un fichero digital emitido por una tercera parte de confianza que garantiza la vinculación entre la identidad de una persona o entidad y su clave pública**
    - **c)** Es una contraseña que se utiliza para acceder a documentos protegidos
    - **d)** Es un software que permite verificar la validez de una firma electrónica

38. **Las medidas de seguridad necesarias para restaurar el servicio de forma rápida, eficiente y con el menor costo y pérdidas posible se incluyen en el:**
    - **a)** Plan estratégico
    - **b)** Plan de sistemas
    - **c)** **Plan de Recuperación de Desastres**
    - **d)** Plan de inventario

39. **Cada uno de los equipos que, dentro de un servicio distribuido de detección de intrusión se instalan en los diferentes segmentos de red se llama:**
    - **a)** **Sonda**
    - **b)** Honeypot
    - **c)** Switch
    - **d)** Repetidor

40. **¿A qué hace referencia el concepto VDI?**
    - **a)** Virtualización dinámica integral
    - **b)** Desarrollo de integraciones virtuales
    - **c)** Voz descomprimida en Internet
    - **d)** **Infraestructura de escritorios virtuales**

41. **¿Respecto a la Seguridad Informática, qué es un "Plan de Continuidad de Negocio"?**
    - **a)** Un plan para gestionar las copias de seguridad de una organización
    - **b)** Un plan para proteger la información confidencial
    - **c)** **Un plan para mantener la operación de la organización en caso de un desastre o ciberataque**
    - **d)** Un plan para actualizar el software de seguridad en una red o sistema

42. **El método de infiltración que se vale de una vulnerabilidad informática a la hora de validar las entradas del usuario para realizar operaciones sobre una base de datos, se denomina:**
    - **a)** **Inyección de código SQL**
    - **b)** Troyano
    - **c)** Phishing
    - **d)** Ataque "*man in the middle*"

43. **¿A quién corresponde el soporte y coordinación para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad que tengan las Entidades Locales?**
    - **a)** **Al CCN-CERT**
    - **b)** Al Ministerio de Defensa
    - **c)** A la Agencia de Protección de Datos
    - **d)** A la Agencia de la Unión Europea para la Ciberseguridad (ENISA)

44. **¿Qué es MAGERIT?**
    - **a)** **Es una metodología de análisis y gestión de riesgos**
    - **b)** Es una metodología de inventario de activos
    - **c)** Es una metodología de gestión de proyectos
    - **d)** Ninguna de las respuestas anteriores es correcta

45. **¿Cuál de los siguientes servicios e infraestructuras comunes propuestos por la AGE hace referencia al Servicio Compartido de Gestión de Notificaciones?**
    - **a)** ALMACEN
    - **b)** SARA
    - **c)** Cl@ve
    - **d)** **NOTIFIC@**

46. **Qué es un "rootkit":**
    - **a)** Un tipo de virus informático para la encriptación de datos
    - **b)** **Un tipo de malware que se esconde en el sistema y permite el acceso no autorizado a un equipo o a otro software**
    - **c)** Un tipo de ataque de fuerza bruta
    - **d)** Ninguna de las respuestas anteriores es correcta

47. **¿Cuál de los siguientes protocolos es el más seguro para transferir archivos?**
    - **a)** **SCP**
    - **b)** TELNET
    - **c)** HTTP
    - **d)** FTP

48. **¿Qué es un "sniffer"?**
    - **a)** Un programa que registra las pulsaciones del teclado
    - **b)** Un programa que escanea los puertos de un sistema para identificar servicios y aplicaciones en ejecución
    - **c)** **Un programa que intercepta y registra el tráfico de red**
    - **d)** Un programa que analiza vulnerabilidades del SW que circula por la red

49. **La herramienta desarrollada por el Centro Criptológico Nacional que permite a las Administraciones Públicas realizar el análisis y la gestión de riesgos, así como el análisis del impacto y la continuidad de operaciones para las Administraciones Públicas se denomina:**
    - **a)** **PILAR**
    - **b)** LUCIA
    - **c)** FERNANDA
    - **d)** EMILIA

50. **Una red local ubicada entre la red interna de la organización y la red externa (generalmente internet), donde se ubican exclusivamente los recursos de la empresa que deben ser accesibles desde internet recibe el nombre de:**
    - **a)** SAT INET
    - **b)** **DMZ**
    - **c)** Intranet
    - **d)** Extranet

51. **¿Cuál de las siguientes opciones es una medida de control de acceso físico?**
    - **a)** **Tarjetas inteligentes**
    - **b)** Contraseñas fuertes
    - **c)** Auditoria de seguridad
    - **d)** Antivirus

52. **La inundación de un buzón de correo electrónico con un gran número de mensajes (e-mail spamming) afecta a:**
    - **a)** La dimensión de confidencialidad de la información
    - **b)** **La dimensión de la disponibilidad de la información**
    - **c)** La dimensión de integridad de la información
    - **d)** Ninguna de las respuestas anteriores es correcta

53. **¿Cuál de las siguientes respuestas NO es una estrategia para gestionar los riesgos?:**
    - **a)** Evitar el riesgo
    - **b)** Mitigar el riesgo
    - **c)** **Subestimar el riesgo**
    - **d)** Transferir el riesgo

54. **Las dimensiones de seguridad que contempla el Esquema Nacional de Seguridad son Disponibilidad, Autenticidad, Integridad, Confidencialidad y:**
    - **a)** Interoperabilidad
    - **b)** Transparencia
    - **c)** **Trazabilidad**
    - **d)** Legitimidad

55. **¿Qué es un ataque de ingeniería social?**
    - **a)** Es un ataque que explota una vulnerabilidad del software
    - **b)** Un ataque de fuerza bruta
    - **c)** **Un ataque que utiliza técnicas psicológicas para obtener información o acceso no autorizado**
    - **d)** Una fuga de datos confidenciales

56. **¿Qué es phishing?**
    - **a)** Un ataque de malware que roba información confidencial
    - **b)** **Un ataque que utiliza correos electrónicos fraudulentos para engañar a los usuarios y robar información confidencial**
    - **c)** Un ataque que utiliza fuerza bruta para acceder a sistemas sin autorización
    - **d)** Un ataque que aprovecha vulnerabilidades en el software de red para acceder a sistemas sin autorización

57. **Un Blockchain puede definirse como:**
    - **a)** Un libro mayor privado centralizado en el que se agregan registros que se almacenan en forma de bloques
    - **b)** **Un libro mayor público distribuido y descentralizado en el que se agregan registros que se almacenan en forma de bloques**
    - **c)** Un algoritmo de gestión de almacenamiento
    - **d)** Ninguna de las respuestas anteriores es correcta

58. **FACe – el Punto General de Entrada de Facturas Electrónicas de la AGE utiliza el formato de factura**
    - **a)** JSON
    - **b)** **FACTURAe**
    - **c)** FACT-Elect
    - **d)** RTF

59. **La gestión unificada de dispositivos móviles se conoce por el acrónimo de:**
    - **a)** UEM
    - **b)** **MDM**
    - **c)** EMM
    - **d)** GUDM

60. **En relación al borrado seguro de dispositivos**
    - **a)** Puede realizarse la destrucción física del dispositivo
    - **b)** Pueden sobrescribirse los sectores del disco duro con datos aleatorios
    - **c)** Puede usarse un software especializado para realizar un borrado seguro
    - **d)** **Todas las respuestas anteriores son correctas**

61. **Un dispositivo IoT está diseñado específicamente para realizar unas funciones básicas, indica la respuesta FALSA:**
    - **a)** **Analizar datos**
    - **b)** Capturar datos
    - **c)** Procesar datos
    - **d)** Comunicar datos

62. **Según MAGERIT un ACTIVO es:**
    - **a)** **Cualquier cosa que tenga un valor para la organización, ya sea tangible o intangible**
    - **b)** Solamente el hardware, dispositivos móviles y edificios
    - **c)** Las personas que trabajen en la organización únicamente
    - **d)** MAGERIT no gestiona ni identifica activos

63. **¿Cuál es la definición más adecuada para un WAF?**
    - **a)** Un dispositivo que bloquea el tráfico no autorizado a un servidor
    - **b)** **Un sistema que protege aplicaciones de servidores web**
    - **c)** Un programa de antivirus para proteger aplicaciones web
    - **d)** Un programa encargado de proteger el tráfico de datos entre dos servidores

64. **Si nos referimos a la recolección de información a través de personas, estamos refiriéndonos a:**
    - **a)** **HUMINT**
    - **b)** IDS
    - **c)** IPS
    - **d)** PHOTINT

65. **Entre los principios del Reglamento Europeo de Protección de Datos, NO se encuentra:**
    - **a)** **Reutilización**
    - **b)** Responsabilidad activa
    - **c)** Exactitud
    - **d)** Minimización

66. **¿Para qué sirven los IDS?**
    - **a)** Para impedir y denegar accesos no autorizados a una red
    - **b)** **Supervisar el tráfico de red en busca de actividades sospechosas**
    - **c)** Cifrar los datos en tránsito entre interfaces de servidores
    - **d)** Compactar los datos de una cabina de datos

67. **¿Para qué sirve una red privada virtual (VPN)?**
    - **a)** **Cifrar los datos en tránsito a través de un túnel virtual**
    - **b)** Impedir el acceso no autorizado a una red
    - **c)** Supervisar el tráfico de red para detectar actividades sospechosas
    - **d)** Proteger contra las infecciones de malware

68. **¿Qué es un "port scan"?**
    - **a)** Un ataque que utiliza correos electrónicos fraudulentos para engañar a los usuarios y robar información confidencial
    - **b)** Un ataque que aprovecha vulnerabilidades en el software de red para acceder a sistemas sin autorización
    - **c)** Un ataque que utiliza la fuerza bruta para acceder a sistemas sin autorización.
    - **d)** **Un proceso que escanea los puertos de un sistema para identificar servicios y aplicaciones en ejecución**

69. **¿Qué es el principio de "menor privilegio"?**
    - **a)** La idea de que los usuarios deben estructurarse de acuerdo a un organigrama para el desempeño de sus actividades.
    - **b)** **La idea de otorgar, exclusivamente, los permisos y derechos necesarios y suficientes a un usuario para desempeñar sus actividades.**
    - **c)** La idea de que el usuario administrador debe tener acceso a la información confidencial de una organización
    - **d)** La idea de que cada usuario básico sólo debe tener privilegios para instalar software

70. **¿Cuál NO es un derecho de las personas según la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales?**
    - **a)** Derecho de acceso
    - **b)** Derecho a la limitación del tratamiento
    - **c)** **Derecho a cobrar dinero por el tratamiento de sus datos**
    - **d)** Derecho de rectificación

71. **Indique qué tipos de entidades pueden conectarse a la Red SARA**
    - **a)** Entidades Locales
    - **b)** Administración General del Estado
    - **c)** Comunidades Autónomas
    - **d)** **Todas las respuestas anteriores son correctas**

72. **¿Cuál es la principal funcionalidad de un "Firewall"?**
    - **a)** Antivirus
    - **b)** Detección de vulnerabilidades
    - **c)** **Bloqueo de tráfico no autorizado**
    - **d)** Encriptación

73. **¿Cuál de los siguientes técnicas o dispositivos se utiliza para detectar amenazas potenciales y generar alertas de actividades maliciosas?**
    - **a)** **IDS**
    - **b)** Proxy
    - **c)** Switch
    - **d)** Amplificador

74. **Un sistema criptográfico que utiliza pares de claves (pública y privada) para cifrar y descifrar información se denomina:**
    - **a)** Simétrico
    - **b)** **Asimétrico**
    - **c)** Paralelo
    - **d)** Ninguna de las respuestas anteriores es correcta

75. **Entre las características de Big Data se encuentra:**
    - **a)** Gran volumen de información
    - **b)** Gran variedad de datos
    - **c)** Se analizan datos a gran velocidad
    - **d)** **Todas las respuestas anteriores son correctas**

76. **Tienen la consideración de Administraciones Públicas:**
    - **a)** La Administración General del Estado
    - **b)** Las Administraciones de las Comunidades Autónomas
    - **c)** Las Entidades que integran la Administración Local
    - **d)** **Todas las respuestas anteriores son correctas**

77. **Según la Ley 9/2017, de Contratos del Sector Público, la adquisición de un ordenador tiene la categoría:**
    - **a)** Contrato de servicios
    - **b)** **Contrato de suministro**
    - **c)** Contrato de "leasing"
    - **d)** Contrato de obra

78. **¿Cuál de los siguientes se considera empleado público?**
    - **a)** Funcionario de carrera
    - **b)** Funcionario interino
    - **c)** Personal laboral, ya sea fijo, por tiempo indefinido o temporal
    - **d)** **Todas las respuestas anteriores son correctas**

79. **De acuerdo al art.50 de la Ley 7/2007, los funcionarios públicos tendrán derecho a disfrutar, durante cada año natural, de unas vacaciones retribuidas de:**
    - **a) Veintidós días hábiles**
    - **b)** Veintidós días hábiles y nueve días de libre disposición
    - **c)** Veinte días hábiles, nueve días de libre disposición
    - **d)** Un mes natural

80. **El número de miembros del Congreso de los Diputados, según la Constitución:**
    - **a)** Podrá ser superior a 300 sin límite máximo
    - **b) Será de un mínimo de 300 y un máximo de 400**
    - **c)** No podrá superar los 200
    - **d)** Será superior a 500

PREGUNTAS DE RESERVA (ESTAS PREGUNTAS NO COMPUTARAN A NO SER QUE SE ANULE ALGUNA DE LAS PREGUNTAS ANTERIORES)

81. **Indicar entre las siguientes normas del IEEE la que trata sobre redes inalámbricas:**
    - **a)** 802.1g
    - **b) 802.11**
    - **c)** 802.12
    - **d)** 802.13

82. **En Alcorcón, la máxima representación del municipio la ostenta**
    - **a) El Alcalde o Alcaldesa**
    - **b)** El Pleno
    - **c)** La Junta de Gobierno Local
    - **d)** La Junta de Representatividad y Protocolo

83. **Los actos del Rey serán refrendados por:**
    - **a)** El Presidente del Gobierno
    - **b)** Los Ministros competentes
    - **c)** El Príncipe heredero
    - **d) El Presidente del Gobierno, y en su caso los Ministros competentes**

84. **La comunicación, publicación y ejecución de los acuerdos plenarios, en el Ayuntamiento de Alcorcón corresponde a:**
    - **a)** El Concejal competente
    - **b)** La Alcaldesa Presidenta
    - **c)** El Titular de la Asesoría Jurídica Municipal
    - **d) El Secretario General del Pleno**

85. **¿Qué es “pharming”?**
    - **a)** Un tipo de ataque de fuerza bruta que usa técnicas de spoofing
    - **b) Un tipo de ataque para el robo de información confidencial**
    - **c)** Un ataque de inyección SQL
    - **d)** Un tipo de ataque de DDoS para atacar granjas de servidores