ANUNCIO DEL CUESTIONARIO Y DE LA PLANTILLA PROVISIONAL DE RESPUESTAS DEL EXAMEN TIPO TEST DEL PROCESO SELECTIVO PARA LA COBERTURA DE UNA PLAZA DE JEFE DE COMUNICACIONES DEL AYUNTAMIENTO DE ZAMORA

De conformidad con lo previsto en las bases de selección se publica el cuestionario tipo test y la PLANTILLA PROVISIONAL DE RESPUESTAS DEL EXAMEN TIPO TEST celebrado el día 24-09-2025, del proceso selectivo para el ingreso como funcionario de carrera, de una plaza de Jefe de Comunicaciones.

PRIMER EJERCICIO: CUESTIONARIO TEÓRICO TIPO TEST

1. ***Según la Guía de Análisis Forense en Sistemas de Control Industrial (INCIBE), en general, el orden de volatilidad de los componentes de un dispositivo informático se clasifica de la siguiente forma (del más al menos volátil):***
2.
   a. **Contenidos de la memoria caché y registros del sistema, Información de red, Memoria, Procesos del sistema, Sistema de ficheros temporal, Datos del disco duro, Datos sobre el registro de acceso remoto, Datos de medios extraíbles**.
   b. Información de red, Contenidos de la memoria caché y registros del sistema, Memoria, Procesos del sistema, Sistema de ficheros temporal, Datos del disco duro, Datos sobre el registro de acceso remoto, Datos de medios extraíbles.
   c. Información de red, contenidos de la memoria caché y registros del sistema, Memoria, Procesos del sistema, Sistema de ficheros temporal, Datos del disco duro, Datos de medios extraíbles, Datos sobre el registro de acceso remoto.
   d. Contenidos de la memoria caché y registros del sistema, Información de red, Memoria, Procesos del sistema, Datos del disco duro, Sistema de ficheros temporal, Datos sobre el registro de acceso remoto, Datos de medios extraíbles.

2. ***Según la Guía para la Gestión de un Inventario de Activos en Sistemas de Control Industrial (INCIBE), ¿Cuál de estas afirmaciones no es correcta?:***
   a. La forma de llevar a cabo un inventariado de activos define el tipo de implementación. Esta puede ser: manual, automática o mixta.
   b. Un inventario automático se elabora gracias al uso de herramientas que permiten agilizar las tareas de recopilación de datos de cada activo de manera automática, algo especialmente útil cuando el número de activos de una organización es muy elevado.
   c. Un inventario manual es aquel elaborado por una o varias personas designadas, con los conocimientos suficientes para recopilar los datos que aportarán valor a dicho inventario y sin la ayuda de software complementario.
   d. **La forma de llevar a cabo un inventariado de activos define el tipo de implementación. Esta puede ser: mecánica, automática o semiautomática.**

3. ***Según la Metodología Evaluación de Indicadores para la mejora de la Ciberresiliencia (INCIBE), a partir del marco conceptual, se ha diseñado un modelo de evaluación del nivel de ciberresiliencia de servicios esenciales. Dicho marco conceptual está formado por metas y dominios funcionales ¿Cuál de estas afirmaciones no es correcta?:***

a. **Formación en Ciberseguridad (FO) en una Meta.**
b. Política de Ciberseguridad (PC) es un Dominio.
c. Resistir (T) es una Meta.
d. Recuperar (R) es una Meta.

4. ***Según el Diccionario de Indicadores para mejora de la Ciberresiliencia (IMC) (INCIBE), no es un objetivo específico de una Política de ciberseguridad (PC):***

a. Establecer y comunicar a toda la organización su misión, objetivos y actividades prioritarias. Colaborar con otros organismos en materia de Ciberseguridad.
b. Establecer responsabilidades en materia de Ciberseguridad.
c. Identificar las funciones críticas de la organización y establecer los requisitos de Ciberresiliencia. Disponer de una estrategia de continuidad y recuperación.
d. **Aprobar la Política de Seguridad de la Información.**

5. ***Según la Defensa de Endpoints en Sistemas de Control Industrial (Guía INCIBE). A alto nivel, podemos definir diferentes acciones para realizar una mejora en cuanto a la seguridad de los Endpoints ¿Cuál de estas afirmaciones no es correcta?:***

a. **Implementar soluciones para monitorizar de forma continua y en tiempo real todos los servidores.**
b. Utilización de un inventario de activos bien actualizado, tanto a nivel de hardware como de software, para conocer que versiones y posibilidades existen para proteger al dispositivo.
c. Configurar correctamente, y siempre y cuando sea posible, la seguridad de los dispositivos finales.
d. Desarrollar y mejorar políticas y procedimientos sobre la seguridad de los dispositivos finales.

6. ***Según la Guía Nacional de Notificación y Gestión de Ciberincidentes (INCIBE), ¿Cuál de estas afirmaciones no es correcta?:***

a. Los organismos del Sector Público notificarán los incidentes según especifica la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad publicada en el BOE nº 95 de 18 de abril de 2018 y la Guía CCN-STIC 817 de Gestión de Ciberincidentes.
b. Se notificarán los incidentes de seguridad que tengan un impacto significativo en la seguridad de la información manejada o los servicios prestados en relación con la categoría del sistema, determinada de acuerdo con lo dispuesto en los artículos 43, 44 y Anexo I del Real Decreto 3/2010, de 8 de enero.
c. Las notificaciones efectuadas por las entidades del ámbito de aplicación de la citada Instrucción Técnica de Seguridad al Centro Criptológico Nacional (CCN) se realizará en los términos indicados en los artículos 36 y 37 del Real Decreto 3/2010, de 8 de enero.
d. **En todo caso, serán de obligatoria notificación al CCN en el momento en que se produzcan, los incidentes de seguridad que por su nivel de impacto potencial sean calificados con el nivel de CRÍTICO, MUY ALTO o ALTO, mediante el empleo de las herramientas desarrolladas al efecto de la notificación de incidentes (CLAUDIA).**

7. ***Según el Plan de Direccionamiento e Interconexión de Redes en la Administración, ¿Cuál de estas afirmaciones no es correcta?:***

a. **El Plan de direccionamiento e interconexión de redes en la Administración define un espacio de direccionamiento público común para los Centros de la Administración. Este Plan permite que cada entidad u organismo pueda establecer de manera independiente sus planes de numeración IP, en función de su infraestructura de red, o distribución orgánica o departamental, pero manteniendo una coordinación con el resto de Administraciones Públicas que evite el uso de direcciones duplicadas.**

b. La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en adelante LAECSP, en su artículo 43, establece que la Administración General del Estado, las Administraciones Autonómicas y las entidades que integran la Administración Local, así como los consorcios u otras entidades de cooperación constituidos a tales efectos por éstas, adoptarán las medidas necesarias e incorporarán en sus respectivos ámbitos las tecnologías precisas para posibilitar la interconexión de sus redes con el fin de crear una red de comunicaciones que interconecte los sistemas de información de las Administraciones Públicas españolas y permita el intercambio de información y servicios entre las mismas, así como la interconexión con las redes de las Instituciones de la Unión Europea y de otros Estados Miembros.

c. El Plan de direccionamiento e interconexión de redes en la Administración es necesario para la interconexión de las redes de las Administraciones Públicas y en particular a y a través de la Red SARA (Sistema de Aplicaciones y Redes para las Administraciones).

d. El Plan de direccionamiento e interconexión de redes en la Administración es necesario para la interconexión con redes de Administraciones de otros Estados miembros de la UE, el despliegue y acceso a los servicios públicos europeos de administración electrónica, a través de la Red SARA y de su enlace con la red transeuropea sTESTA, que tiene a su vez su propio plan de direccionamiento.

8. ***Según el Plan de Direccionamiento e Interconexión de Redes en la Administración, ¿Cuál de estas afirmaciones no es correcta?:***

a. Dotación de elementos de conectividad. –El MPTAP adquirirá, instalará, administrará, configurará y mantendrá los elementos de conectividad de cada PAS.

b. El soporte y la gestión de incidentes de la Red SARA se prestarán de manera conjunta entre el MPTAP y los PAS, a través de sus correspondientes equipos dedicados a estos servicios.

c. Para facilitar la actuación conjunta entre el MPTAP y los PAS, cada organización proporcionará los siguientes datos de sus servicios de soporte y de gestión de incidentes: Identificación, Responsable de la unidad, Responsable técnico, Horario de servicio, Localización, Horario y datos de contacto para incidentes, Observaciones.

d. Las organizaciones que se conecten a la Red SARA aplicarán el Plan de direccionamiento e Interconexión de Redes en la Administración establecido por la Dirección General para el Impulso de la Administración Electrónica (DGIAE) disponible en http://administracionelectronica.gob.es/ según lo dispuesto en artículo 14 del Real Decreto 3/2010, de 8 de enero.

9. ***Según la Norma y Guía Técnica de Interoperabilidad de Requisitos de Conexión a la Red de Comunicaciones de las Administraciones Públicas Españolas, ¿Cuál de estas afirmaciones no es correcta?:***

a. El MPTAP podrá hacer pública, en cualquier lista de referencia o en cualquier boletín de prensa publicado y sin autorización previa, la relación de organismos usuarios de la Red SARA.

b. **Los Proveedores de acceso a la Red SARA, garantizarán las condiciones adecuadas en la ubicación del AC (condiciones medioambientales, suministro eléctrico, cableado, etc.) con el fin de asegurar el mantenimiento del servicio.**

c. El Ministerio de Política Territorial y Administración Pública (El MPTAP), adoptará las medidas de seguridad necesarias para proteger debidamente la información transmitida, mediante el cifrado de las comunicaciones y la detección temprana de incidentes en colaboración con el CCN-CERT.

d. Los Órganos usuarios finales, aplicarán las condiciones particulares de servicios horizontales y verticales que utilizan a través de la Red SARA.

10. ***Según la Guía CCN-STIC 1421 Procedimiento de empleo seguro WatchGuard Fireware, en la fase de despliegue e instalación ¿Cuál de estas afirmaciones en la configuración por defecto no es correcta?:***

a. Interfaces: La interfaz 0 se encuentra habilitada como interfaz externa (WAN), actuando como cliente DHCP.

b. SSH: La interfaz de administración mediante SSH se encuentra habilitada a través del puerto 4118. Sin embargo, las conexiones a través del puerto SSH no están recomendadas para administrar el dispositivo, por lo que no se deberá acceder a través de esta interfaz para realizar ninguna operación de administración durante la fase de operación del producto.

c. **Web UI: Para conectarse a la interfaz de administración web, el usuario debe conectar un dispositivo actuando como cliente DHCP al puerto 1 del producto y acceder a la siguiente dirección: https://10.0.0.1:8080.**

d. Web UI: El puerto por defecto para establecer conexiones a través de la interfaz web es el puerto 8080.

11. ***Según la Guía CCN-STIC 140 Taxonomía de productos STIC, Anexo E.4: Sistemas de prevención de fuga de datos, ¿No es un requisito fundamental de seguridad (RFS)?:***

a. Requisitos criptográficos.

b. **Auditoría y registros de seguridad, gestión de ciber incidentes.**

c. Control de accesos, autenticación y privilegios.

d. Administración del producto, protección de datos de usuario.

12. ***Según la Guía CCN-STIC 140 Taxonomía de productos STIC, F.3-M: Protección de correo electrónico, ¿Los activos sensibles a proteger en un Análisis de Amenazas son?:***

a. **AC.Administración, AC.PSS, AC.PSC, AC.Actualizaciones, AC.Comunicaciones.**

b. A.NOAUT Acceso no autorizado de administrador, A.CRYPTO Mecanismos criptográficos débiles, A.COM Protocolos de comunicación no autorizados, A.ACT Actualización maliciosa.

c. A.NOAUTUSR Acceso no autorizado de usuario, A.CRE Compromiso de credenciales, A.SPM. Contenido externo potencialmente dañino.

d. A.AUD Actividades no detectadas, A.INT Compromiso de la integridad del software/firmware, A.PSC Compromiso de parámetros de seguridad críticos.

13. ***Según la Guía CCN-STIC 140 Taxonomía de productos STIC, Anexo F.8: Balanceadores de carga, ¿Las principales amenazas a las que el uso de esta familia de productos pretende hacer frente son?:***

a. **Información que atraviese el producto, que provenga de los equipos y dispositivos para los cuales se realiza la función de balanceador, en ambos sentidos. Interfaces de gestión del producto e información transmitida a través de ellas, en ambos sentidos. Datos de configuración del producto y de auditoría generados por éste. Actualizaciones del dispositivo susceptibles de afectar a su configuración y funcionalidad.**
b. Divulgación de información no autorizada, un atacante ya sea desde dentro de la red o desde fuera consigue enviar información no autorizada de la red interna al exterior a través del dispositivo (p.ej.: direccionamiento IP de la red protegida o mapa de dispositivos de la red). Acceso no autorizado, un atacante ya sea desde dentro de la red o desde fuera consigue acceder a información intercambiada a través del dispositivo para la que no estaba autorizado (p.ej.: recibir información transmitida a través del dispositivo, pero no destinada a él) o utilizar el dispositivo como mecanismo de acceso a la red protegida.
c. Envío de tráfico dañino, un atacante ya sea desde dentro de la red o desde fuera consigue eludir o inhabilitar las políticas de balanceo configuradas y/o enviar información no autorizada desde el exterior a la red interna a través del dispositivo (p.ej.: introducir información maliciosa de manera encubierta proveniente de la red externa). Cifrado débil, utilización en el dispositivo de algoritmos criptográficos débiles que permitan a un atacante comprometerlo, fundamentalmente mediante ataques de fuerza bruta.
d. Uso de canales de comunicación inseguros, mala implementación de protocolos estándar o utilización de protocolos no estandarizados que permiten a un atacante comprometer la integridad y confidencialidad de las comunicaciones del dispositivo. Compromiso de la funcionalidad del dispositivo, un atacante o un fallo en el dispositivo compromete la funcionalidad de seguridad, incluyendo el balanceo de carga y registro de actividad, permitiendo modificarla o desactivarla de manera no conforme a las políticas de seguridad (p.ej. instalación de actualizaciones maliciosas o administración no autorizada del dispositivo).

14. ***Según la Guía CCN-STIC 140 Taxonomía de productos STIC, Anexo G: Servicios en la nube, ¿No es un requisito fundamental de seguridad (RFS)?:***

a. Certificación de conformidad con el ENS, requisitos criptográficos y gestión de claves.
b. Requisitos de transparencia, jurisdicción de los datos.
c. Certificaciones de producto, auditoría de pentesting.
d. **Nombramiento formal del Responsable de Seguridad y del Delegado de protección de Datos, si se tratan datos de carácter personal.**

15. ***Según la Guía CCN-STIC 140 Taxonomía de productos STIC, Anexo I.1-M: Cámaras IP, ¿No es un requisito fundamental de seguridad para cámaras IP?:***

a. Se deberá seleccionar al menos una opción de las indicadas en el RFS y se incluirá en la declaración de seguridad.
b. Se deberá especificar el listado de opciones que sean de aplicación al TOE.
c. **El TOE debe definir, al menos, el perfil de administrador y ser capaz de asociar usuarios a perfiles.**
d. El TOE deberá identificar y autenticar a cada usuario administrador y [asignación: otros usuarios del producto] antes de otorgar acceso.

16. ***Según la Guía de Seguridad de las TIC CCN-STIC 817 Gestión de ciberincidentes, ¿Cuál de las siguientes afirmaciones no es correcta?:***

a. **Si el Ciberincidente afecta apreciablemente a una infraestructura crítica, tiene un nivel alto de impacto potencial.**
b. Los Daños reputacionales apreciables, con eco mediático (amplia cobertura en los medios de comunicación), tiene un nivel medio de impacto potencial.
c. Afecta a más de 50 equipos con información cuya máxima categoría es BÁSICA, tiene un nivel alto de impacto potencial.
d. Afecta a más de 50 equipos con información cuya máxima categoría es MEDIA, tiene un nivel muy alto de impacto potencial.

17. ***Según la Guía de Seguridad de las TIC CCN-STIC 811 Interconexión en el ENS, ¿Cuál de las siguientes afirmaciones no es correcta?:***

a. **El concentrador de redes privadas virtuales (donde empiezan las VPN) debe instalarse preferentemente en la zona desmilitarizada (DMZ) y todos los flujos de información, entrantes y salientes, deben pasar por el intermediador (cortafuegos).**
b. Por seguridad nos referimos a garantías de confidencialidad, integridad y autenticidad, según se recoge en las medidas de seguridad [mp.com.2] protección de la confidencialidad y [mp.com.3] protección de la autenticidad y de la integridad del ENS. Estas garantías son en buena parte criptográficas y se ajustarán a lo previsto en la guía CCN-STIC 807 Criptología de Empleo en el Esquema Nacional de Seguridad.
c. Las características y requisitos de las redes privadas virtuales se tratan en detalle en la guía CCN-STIC 836 Seguridad en VPN en el marco del ENS.
d. Se debe estudiar la oportunidad de desplegar un cortafuegos entre la terminación VPN y el proxy, a fin de limitar los paquetes que pueden atravesar esta interfaz.

18. ***Según la Guía de Seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6, ¿Cuántas superficies principales de ataque existen en una red IP?***

a. Existen dos superficies principales de ataque en una red IP.
b. **Existen tres superficies principales de ataque en una red IP.**
c. Existen cuatro superficies principales de ataque en una red IP.
d. Existen cinco superficies principales de ataque en una red IP.

19. ***Según la Guía de aplicación de la Norma Técnica de Interoperabilidad de Documento Electrónico, con el objetivo de dar apoyo a la aplicación e implementación de lo dispuesto en la NTI, esta guía no desarrolla:***
20.

a. Estructura y componentes del documento electrónico en intercambios entre Administraciones públicas y con el ciudadano, definiendo las características básicas de sintaxis para la necesaria interoperabilidad en procesos de este tipo.
b. **Interoperabilidad semántica de los documentos electrónicos.**
c. Formatos de ficheros que conforman los documentos electrónicos.
d. Consideraciones sobre la firma del documento electrónico.

20. ***Según la Guía de aplicación de la Norma Técnica de Interoperabilidad de Expediente Electrónico, con el objetivo de dar apoyo a la aplicación e implementación de lo dispuesto en la NTI, esta guía desarrolla:***

a. Indicaciones para los servicios de disminución y puesta a disposición de expedientes electrónicos.
b. Consideraciones para la implementación y gestión del documento electrónico.
c. Conjunto de metadatos mínimos complementarios para el expediente electrónico.
d. **Concepto de expediente electrónico, requisitos y etapas asociadas a su ciclo de vida genérico, con especial atención al concepto de índice electrónico del expediente como elemento que garantiza la integridad del mismo.**

21. ***Según la Ley 11/2022, de 28 de junio, General de Telecomunicaciones, los operadores que suministren redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar:***

a. **El secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias.**
b. El secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas organizativas necesarias.
c. El secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas y organizativas necesarias.
d. El secreto de las comunicaciones de conformidad con los artículos 21.3 y 1.1 de la Constitución, debiendo adoptar las medidas técnicas y organizativas necesarias.

22. ***Conforme a la Guía de Seguridad de las TIC CCN-STIC 816 de Seguridad en Redes Inalámbricas dentro de las medidas de seguridad del ENS, señale cual forma parte de las medidas operacionales:***

a. Procedimientos.
b. **Autenticación.**
c. Segregación de redes.
d. Borrado y destrucción.

23. ***El Plan de contingencia y continuidad de negocio del INCIBE está formado por el siguiente número de fases:***

a. Cuatro fases.
b. Cinco fases.
c. **Seis fases.**
d. Siete fases.

24. ***Señale la respuesta correcta respecto a las soluciones del Centro Criptológico Nacional:***

a. Gloria, gestión de eventos e información de seguridad.
b. Mónica, gestor de logs para responder ante incidentes y amenazas.
c. **Clara, auditoría de cumplimiento ENS/STIC en sistemas Windows y Linux.**
d. Carla, herramienta para la detección de amenazas complejas en el puesto de usuario.

25. ***Dentro de las soluciones del Centro Criptológico Nacional, el informe de estado de seguridad en el ENS se denomina:***

a. **Ines**.
b. Elena.
c. Enma.
d. Iris.

26. ***Señale la respuesta incorrecta. Entre las medidas de la línea de acción 1 reforzar las capacidades ante las amenazas provenientes del ciberespacio, de la Estrategia Nacional de Ciberseguridad están:***

a. Potenciar la colaboración de los centros de excelencia e investigación en la lucha contra las ciberamenazas.

b. Potenciar la creación, difusión y aplicación de mejores prácticas, y la adopción de estándares en materia de ciberseguridad.

c. Potenciar las capacidades de ciberdefensa y de ciberinteligencia.

d. **Potenciar, en el marco de sus competencias, la progresiva implicación y creación de infraestructuras de ciberseguridad en las Comunidades Autónomas, las Ciudades Autónomas, las Entidades Locales y en sus organismos vinculados o dependientes que cooperarán y se coordinarán con las estructuras nacionales en pro de la mejora de la ciberseguridad nacional**.

27. ***Señale la respuesta incorrecta. Según la Estrategia Nacional de Ciberseguridad, el ciberespacio:***

a. Es un espacio común global caracterizado por su apertura funcional y su dinamismo.

b. **Posibilita la conectividad universal y facilita el libre flujo de la economía y el comercio.**

c. Se configura como campo de batalla donde la información y la privacidad de los datos son activos de alto valor en un entorno de mayor competición geopolítica, reordenación del poder y empoderamiento del individuo.

d. Se sustenta en elementos físicos y lógicos.

28. ***Señale la respuesta correcta respecto a la política de seguridad según el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad***

a. **Cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente.**

b. En la Administración General del Estado, la política de seguridad estará centralizada en el Ministerio de Asuntos Económicos y Transformación Digital.

c. La Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital dispondrá de su propia política de seguridad, que será aprobada por el titular del Ministerio.

d. La política de seguridad se establecerá de acuerdo con los principios básicos señalados en el capítulo III del citado Real Decreto.

29. ***Conforme al Anexo II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, las medidas de seguridad se dividen en:***

a. Marco organizativo, marco operacional, monitorización del sistema.

b. Marco organizativo, medidas de protección, monitorización del sistema.

c. Marco operacional, medidas de protección, monitorización del sistema.

d. **Marco organizativo, marco operacional, medidas de protección.**

30. ***Respecto a los principios de la protección de datos, según la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal:***

a. Los datos de carácter personal se recogerán siempre para su tratamiento, así como someterlos a dicho tratamiento, independientemente de la finalidad para la que se ha obtenido.

b. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos resultando incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

c. Los datos de carácter personal serán exactos y se actualizarán anualmente.

d. **Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.**

31. ***De las siguientes afirmaciones respecto al derecho a sindicarse, ¿cuál es la correcta según lo contemplado en el artículo 28 de la Constitución Española?***

a. La ley podrá limitar o exceptuar el ejercicio de este derecho a los funcionarios públicos.

b. La ley regulará las peculiaridades de su ejercicio a las Fuerzas o Institutos armados o a los demás Cuerpos sometidos a disciplina militar.

c. **La libertad sindical comprende el derecho a fundar sindicatos y a afiliarse al de su elección.**

d. Todas las anteriores son correctas.

32. ***Según lo contemplado en el artículo 64 de la Constitución Española en relación con el refrendo de los actos del Rey, la propuesta y el nombramiento del Presidente del Gobierno, y la disolución propuesta en el artículo 99, serán refrendados por:***

a. **El Presidente del Congreso**.

b. El Presidente del Gobierno.

c. Los Ministros competentes.

d. Las respuestas b) y c) son correctas.

33. ***Según lo contemplado en el artículo 68 de la Constitución Española las elecciones tendrán lugar:***

a. Tendrán lugar entre los 25 días y 50 días desde la terminación del mandato.

b. **Tendrán lugar entre los 30 días y 60 días desde la terminación del mandato.**

c. Tendrán lugar entre los 30 días y 90 días desde la terminación del mandato.

d. Tendrán lugar entre los 25 días y 60 días desde la terminación del mandato.

34. ***Según lo contemplado en el artículo 35 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, el presidente de la Comisión de Transparencia y Buen Gobierno será:***

a. **El Presidente del Consejo de Transparencia y Buen Gobierno.**

b. El miembro de la Comisión de mayor edad.

c. El miembro de la Comisión que sea elegido según los Estatutos.

d. Ninguna de las anteriores es correcta.

35. ***Según lo contemplado en el Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público, el ascenso en la estructura de puestos de trabajo por los procedimientos de provisión establecidos en el capítulo III del título V de este Estatuto, corresponde con:***

a. Promoción interna vertical.

b. Promoción interna horizontal.

c. **Carrera vertical.**

d. Carrera horizontal.

36. ***Según lo contemplado en el artículo 24 del Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público, la cuantía y estructura de las retribuciones complementarias de los funcionarios se establecerán por:***

a. El Gobierno.

b. **Las correspondientes leyes de cada Administración Pública.**

c. La Ley de Presupuestos Generales del Estado.
d. Los órganos de Gobierno de las Comunidades Autónomas.

37. ***Según lo contemplado en el artículo 9 de Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos,***

a. La titularidad de la sede electrónica corresponde al máximo Órgano responsable en materia de transformación digital de cada Administración Pública.
b. **La titularidad de la sede electrónica corresponde a una Administración Pública, o bien a uno o más organismo públicos o entidades de derecho público en el ámbito de sus competencias.**
c. La titularidad de la sede electrónica corresponde a una Administración Pública, y, en todo caso, a la Administración General del Estado.
d. Ninguna de las anteriores es correcta.

38. ***Señale la incorrecta de las siguientes afirmaciones en relación con la solución ORVE.***

a. Es un servicio gratuito en la nube para el intercambio electrónico de asientos registrales y su documentación adjunta entre administraciones integradas en el Sistema de Interconexión de Registros.
b. **Tiene como destinatarios la Administración General del Estado, la Administración Autonómica y Local.**
c. Para solicitar el Servicio ORVE es necesario firmar un acuerdo de Adhesión.
d. ORVE permite digitalizar la documentación en papel que presenta el ciudadano en las oficinas de registro, y enviarlo electrónicamente al destino competente siempre que esté integrado en SIR.

39. ***¿Qué puede ocurrir tras una revisión periódica de validez de un producto o servicio incluido en el CPSTIC?***

a. Puede actualizarse automáticamente sin necesidad de revisión adicional.
b. **Puede bajar el máximo nivel de clasificación autorizado y, en caso de incumplimiento, ser excluido del catálogo**.
c. Se mantiene siempre vigente sin cambios mientras exista un certificado original.
d. Puede cambiarse el fabricante sin notificación al CCN.

40. ***Atendiendo a la guía CCN-STIC-140, ¿qué productos se incluyen en la tercera parte llamada "Taxonomía de Productos y Servicios de Conformidad y Gobernanza de la Seguridad"?***

a. Productos que forman parte de la arquitectura de seguridad del sistema TIC.
b. Productos sin funcionalidades de seguridad.
c. **Productos que facilitan el cumplimiento normativo y servicios de auditoría o análisis de riesgos.**
d. Productos exclusivamente de hardware para cifrado.

41. ***¿Cómo está organizada la estructura de la taxonomía para clasificar productos cualificados en la Guía CCN-STIC-140?***

a. Por rangos de precios y fabricantes.
b. **Basada en las medidas de seguridad definidas en el Anexo II del Real Decreto 311/2022 (ENS).**
c. Por tipos de administración, General del Estado, Autonómica, atendiendo al territorio.
d. Según el tamaño de la organización que lo adquiere.

42. ***¿Cuál es el principal objetivo del CPSTIC?***
   a. Publicar una lista de fabricantes tecnológicos.
   b. **Facilitar la adquisición segura de productos y servicios TIC.**
   c. Listar todos los servicios de telecomunicaciones.
   d. Clasificar software libre.

43. ***¿Qué familias conforman la taxonomía de productos cualificados según CCN-STIC-140?***
   a. Productos de hardware, software, y servicios.
   b. **Control de acceso, seguridad en explotación, monitorización, protección de comunicaciones y protección de equipos**.
   c. Software libre, propietario y mixto.
   d. Auditoría, análisis y riesgos.

44. ***¿Cuál es la base legal que asigna al Centro Criptológico Nacional la responsabilidad de certificar productos y servicios TIC en España?***
   a. Ley Orgánica de Protección de Datos.
   b. **RD 421/2004 y RD 311/2022**.
   c. Directiva Europea de Seguridad Informática.
   d. Ley de Propiedad Intelectual.

45. ***Según la Guía CCN-STIC-140, ¿qué dimensiones de seguridad se incrementan mediante los productos incluidos en el CPSTIC?***
   a. Rendimiento, usabilidad y seguridad.
   b. **Disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.**
   c. Coste y escalabilidad.
   d. Movilidad y acceso remoto.

46. ***¿Cuál de las siguientes familias de productos está orientada a automatización, respuesta a incidentes y correlación avanzada de alertas?***
   a. Seguridad en explotación.
   b. Sistemas Honeypot.
   c. **Sistemas SOAR.**
   d. Herramientas de caché web.

47. ***¿Qué indica un identificador como [mp.com.4] en la taxonomía CCN-STIC-140?***
   a. País de fabricación.
   b. **Una medida específica del Esquema Nacional de Seguridad relacionada con protección de comunicaciones.**
   c. Fecha de certificación.
   d. Una medida específica del Esquema Nacional de Seguridad relacionada con captura, monitorización y Análisis de tráfico.

48. ***¿El identificador ENS puede usarse para...?***
   a. Automatizar procesos de actualización.
   b. **Referenciar el cumplimiento en auditorías de seguridad.**
   c. Definir el rango de precio del sistema.
   d. Referenciar el producto.

49. ***¿Qué ocurre si una familia de productos en la taxonomía no tiene identificador ENS asociado?***
   a. Es certificado automáticamente.
   b. **No puede justificar su contribución a medidas específicas de seguridad ENS.**

c. Se aprueba para uso externo.
d. Se considera de uso exclusivamente interno.

50. ***¿Cómo organiza el esquema de la taxonomía la vinculación entre familias de productos cualificados y la normativa de seguridad?***

a. Por regiones geográficas.
b. **Por identificadores ENS y anexos de requisitos fundamentales.**
c. Por fecha de actualización.
d. Por mecanismos de cifrado.

PREGUNTAS DE RESERVA

51. ***Según lo contemplado en el artículo 10 de Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, el acto o resolución de creación o supresión de una sede electrónica o sede electrónica asociada será publicado en el caso de las entidades locales:***

a. **En el boletín oficial de la provincia al que pertenezca la entidad y también en el directorio del Punto de Acceso General Electrónico que corresponda**.
b. En el boletín oficial del Estado y también en el directorio del Punto de Acceso General Electrónico que corresponda.
c. En el boletín oficial de la provincia al que pertenezca la entidad o en el directorio del Punto de Acceso General Electrónico que corresponda.
d. En el boletín oficial del Estado o en el directorio del Punto de Acceso General Electrónico que corresponda.

52. ***Según lo contemplado en el artículo 87 de la Constitución Española la iniciativa legislativa corresponde a (Señale la incorrecta):***

a. El Gobierno.
b. El Congreso.
c. **El Consejo de Ministros.**
d. El Senado.

53. ***Según lo contemplado en el artículo 21 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, NO es una atribución del Alcalde:***

a. Aprobar la oferta de empleo público.
b. **La aprobación del reglamento orgánico y de las ordenanzas.**
c. Dictar bandos.
d. Ejercer la jefatura de la Policía Municipal.

54. ***Según lo contemplado en el artículo 49 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, la aprobación de las Ordenanzas locales se ajustará al siguiente procedimiento:***

a. Aprobación inicial por el Alcalde, información pública y audiencia a los interesados por el plazo mínimo de 30 días, resolución de todas las reclamaciones y sugerencias presentadas en plazo y aprobación definitiva por el Pleno.
b. **Aprobación inicial por el Pleno, información pública y audiencia a los interesados por el plazo mínimo de 30 días, resolución de todas las reclamaciones y sugerencias presentadas en plazo y aprobación definitiva por el Pleno.**

c. Aprobación inicial por el Alcalde, información pública y audiencia a los interesados por el plazo mínimo de 45 días, resolución de todas las reclamaciones y sugerencias presentadas en plazo y aprobación definitiva por el Pleno.

d. Aprobación inicial por el Pleno, información pública y audiencia a los interesados por el plazo mínimo de 45 días, resolución de todas las reclamaciones y sugerencias presentadas en plazo y aprobación definitiva por el Pleno.

55. ***Según Guía de Seguridad (CCN-STIC-801) Esquema Nacional de Seguridad Responsabilidades y Funciones, ¿Cuál de estas afirmaciones no es correcta?:***

a. En organismos de pequeña dimensión, los roles y responsabilidades identificadas en esta guía pueden reducirse a la siguiente estructura mínima reducida a 2 roles, dirección y operación.

b. En organismos de dimensión intermedia, los roles y responsabilidades identificadas en esta guía pueden reducirse a la siguiente estructura reducida a 3 roles, dirección, supervisión y operación.

c. **En organismos de gran dimensión, los roles y responsabilidades identificadas en esta guía pueden reducirse a la siguiente estructura reducida a 4 roles, dirección, supervisión, operación, responsable de Seguridad.**

d. En organismos de pequeña dimensión, una figura integrando las siguientes funciones en el rol de Dirección: responsable del fichero (si hay datos de carácter personal), responsable de la información, responsable del servicio, responsable de la seguridad.

56. ***Según la Guía de Acceso Seguro a los Dispositivos de Campo (INCIBE): ¿Cuál de estas afirmaciones no es correcta?:***

a. El uso del mecanismo de doble factor permitiría que, en el caso de que se produjera el robo de las credenciales del usuario, el atacante no pudiera acceder al sistema, ya que necesitaría aportar también el segundo factor para poder autenticarse.

b. **Un sistema de prevención de ataques (IPA, Intrusion Prevention Attacks) funciona a grandes rasgos de manera similar a un IDS, sin embargo, una vez detectada el posible ataque, también es capaz de actuar y bloquearlo.**

c. El despliegue de una arquitectura RADIUS en la red permite la gestión de una manera centralizada de la autenticación de los usuarios, así como de la asignación de los recursos a los que tiene acceso y sus permisos.

d. El mecanismo de doble factor de autenticación es utilizado para reforzar la seguridad en el proceso de autenticación de los usuarios. Su funcionamiento consiste en añadir un elemento extra al, mecanismo habitual de usuario y contraseña. Este elemento extra, puede ser “algo que tenemos”, como un token USB o tarjeta inteligente, o “algo que somos”, como una huella dactilar. El mecanismo de doble factor más extendido es el uso de un código aleatorio generado mediante un token hardware o software.

57. ***Según el Real Decreto 203/2021, de acuerdo con lo previsto en el artículo 42 de la Ley 40/2015, de 1 de octubre, en la tramitación administrativa automatizada de los procedimientos, cada Administración Pública podrá determinar los supuestos de utilización de los siguientes sistemas de firma electrónica:***

a. Certificado de Empleado Público, órgano, organismo público o entidad de derecho público, a que se refiere el artículo 19 de este Reglamento, basado en certificado electrónico cualificado que reúna los requisitos exigidos por la legislación de firma electrónica.

b. **Código seguro de verificación vinculado a la Administración Pública, órgano, organismo público o entidad de derecho público, en los términos y condiciones establecidos, permitiéndose en todo caso la comprobación de la**

integridad del documento mediante el acceso a la sede electrónica correspondiente.

c. Certificado de Empleado Público con seudónimo, órgano, organismo público o entidad de derecho público, a que se refiere el artículo 19 de este Reglamento, basado en certificado electrónico cualificado que reúna los requisitos exigidos por la legislación de firma electrónica.

d. Certificado de terceros, órgano, organismo privado o entidad de derecho privada, a que se refiere el artículo 19 de este Reglamento, basado en certificado electrónico cualificado que reúna los requisitos exigidos por la legislación de firma electrónica.

58. ***El órgano científico técnico especializado de la Administración General del Estado que tiene como misión el análisis y estudio de las condiciones de seguridad y salud en el trabajo, así como la promoción y apoyo a la mejora de las mismas es:***

a. La Inspección de Trabajo y Seguridad Social.

b. La Comisión Nacional de Seguridad y Salud en el Trabajo.

c. **El Instituto Nacional de Seguridad e Higiene en el Trabajo.**

d. La Comisión Nacional de Seguridad e Higiene en el Trabajo.

59. ***Señale la respuesta correcta. Los delegados de Prevención en función del número de trabajadores son:***

a. De 50 a 100 trabajadores: 1 Delegado de Prevención.

b. **De 101 a 500 trabajadores: 3 Delegados de Prevención**.

c. De 501 a 1.000 trabajadores: 5 Delegados de Prevención.

d. En una empresa de veinte trabajadores el Delegado de Prevención será elegido entre los Delegados de Personal.

60. ***Las Administraciones públicas, en el ámbito de sus respectivas competencias y en aplicación del principio de igualdad entre mujeres y hombres, deberán:***

a. Implantar la conciliación de la vida personal, familiar y laboral, sin menoscabo de la promoción profesional.

b. Implantar la formación en igualdad, tanto en el acceso al empleo público como a lo largo de la carrera profesional.

c. **Promover la presencia equilibrada de mujeres y hombres en los órganos de selección y valoración.**

d. Facilitar medidas efectivas para eliminar cualquier discriminación retributiva, directa o indirecta, por razón de sexo.

PLANTILLA PROVISIONAL DE RESPUESTAS

Nº PREGUNTA	RESPUESTA	Nº PREGUNTA	RESPUESTA
1	a	**26**	d
2	d	**27**	b
3	a	**28**	a
4	d	**29**	d
5	a	**30**	d
6	d	**31**	c
7	a	**32**	a
8	d	**33**	b
9	b	**34**	a
10	c	**35**	c
11	b	**36**	b
12	a	**37**	b
13	a	**38**	b
14	d	**39**	b
15	c	**40**	c
16	a	**41**	b
17	a	**42**	b
18	b	**43**	b
19	b	**44**	b
20	d	**45**	b
21	a	**46**	c
22	b	**47**	b
23	c	**48**	b
24	c	**49**	b
25	a	**50**	b

PREGUNTAS RESERVA			
51	a	**56**	b
52	c	**57**	b
53	b	**58**	c
54	b	**59**	b
55	c	**60**	c

El Tribunal del proceso selectivo para la provisión como funcionario/a de carrera de una plaza de Jefe de Comunicaciones, conforme a las bases específicas del proceso selectivo, CONCEDE a las personas interesadas, un plazo de TRES DÍAS NATURALES, contados desde el día siguiente a la publicación del presente anuncio, para plantear las reclamaciones que estimen oportunas o convenientes.

ZAMORA
AYUNTAMIENTO

DOCUMENTO FIRMADO ELECTRÓNICAMENTE