

### III. ADMINISTRACIÓN LOCAL

#### AYUNTAMIENTO DE

**58****ALCORCÓN**

## OFERTAS DE EMPLEO

En el BOLETÍN OFICIAL DE LA COMUNIDAD DE MADRID número 233, de 30 de septiembre de 2022, se publica anuncio con número de inserción 02/18.249/22, referente a la provisión, mediante concurso-oposición libre, de una plaza de técnico superior, puesto de trabajo de Técnico/a de Seguridad Informática; habiéndose detectado error al no haberse publicado los anexos I, IV, V y VI, se inserta a continuación los mencionados anexos.

## ANEXO I

## TEMARIO

*Parte general*

1. La Constitución española de 1978: derechos fundamentales y libertades públicas. Instituciones del Estado.
2. La organización del Estado en la Constitución. La Corona. Funciones constitucionales del Rey. Sucesión y regencia. El referendo. Las Cortes Generales.
3. La organización territorial del Estado en la Constitución. Las Comunidades Autónomas. La Administración Local. El Estado de las Autonomías. Antecedentes. Modelo seguido por la Constitución española. Caracteres del derecho a la autonomía. Competencias.
4. Principios constitucionales de la Administración Local. El principio de autonomía: significado y alcance.
5. Las Comunidades Autónomas. Los estatutos de autonomía. Estatuto de Autonomía de la Comunidad de Madrid.
6. El Derecho Administrativo. Concepto. Fuentes del Derecho administrativo. La actividad organizativa de la Administración: principios jurídicos.
7. El acto administrativo. Concepto, clases y elementos. Su motivación y notificación. Eficacia y validez de los actos administrativos.
8. El procedimiento administrativo: principios generales y fases. El acto administrativo: eficacia y validez.
9. El administrado: concepto y clases. Actos jurídicos del administrado. Colaboración y participación de los ciudadanos en las funciones administrativas.
10. Los contratos del Sector Público. Clases. El expediente de contratación y su tramitación. Procedimientos y criterios de adjudicación. Ejecución y modificación de los contratos.
11. La Administración Local. Concepto y evolución en España. El Régimen Local. Regulación jurídica. La Administración Local. Entidades que comprende. Régimen de los municipios con población inferior a 5.000 habitantes.
12. La organización política y administrativa del Ayuntamiento de Alcorcón (I): el Gobierno municipal. El Pleno. El Alcalde. Los Tenientes de Alcalde. La Junta de Gobierno.
13. La organización política y administrativa del Ayuntamiento de Alcorcón (II): Niveles esenciales de Administración y gestión. Asesoría jurídica. La Intervención General. Órganos de gestión económico-financiera.
14. El personal al servicio de las Administraciones Públicas: tipología. Derechos y deberes de los funcionarios públicos. Régimen disciplinario. Sistema retributivo.
15. Las situaciones administrativas de los funcionarios públicos. Las incompatibilidades de los funcionarios públicos.
16. El personal laboral al servicio de las Entidades Locales. Derechos, deberes e incompatibilidades. El contrato laboral.
17. Los bienes de las Entidades Locales. Haciendas Locales: concepto y regulación.
18. Ordenanzas y reglamentos de las Entidades Locales. Clases. Procedimiento de elaboración y aprobación.

*Parte específica*

19. Real Decreto 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.
20. Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
21. Estrategia nacional de Ciberseguridad 2019. Consejo nacional de Ciberseguridad.
22. El Esquema Nacional de Seguridad. Procedimientos y Normas. Guías Serie 800. Herramientas y soluciones CCN-CERT. Certificación de una Entidad Local. Instrucciones Técnicas de Seguridad (ITS): Notificación de incidentes de seguridad, de conformidad con el ENS. Concienciación y cultura en seguridad de la información y ciberseguridad.
23. Auditoría de seguridad de sistemas de información. Certificación y auditorías en el ámbito del ENS Normas Técnicas de seguridad. Serie ISO 27000. Certificación ISO 27001.
24. Resiliencia y continuidad de negocio. UNE-EN ISO 22301:2020. ISO/IEC 38500. La gestión de la continuidad del negocio. Planes de continuidad y contingencia del negocio.
25. Hacking ético, descubrimiento y explotación de vulnerabilidades de aplicaciones y de hardware y software de infraestructuras TIC. Pentesting. Bases de datos de vulnerabilidades. Metasploit. Soluciones de prevención, detección de amenazas y monitorización de eventos e información de seguridad.
26. Amenazas. Clasificación de los tipos de amenazas más comunes. APTs. Contra-medidas.
27. Protección del dato, especialmente datos personales. Análisis de riesgos. Evaluación del impacto. Metodología MAGERIT. Herramienta PILAR y sus diferentes versiones.
28. Técnicas y herramientas de seguridad perimetral. Cortafuegos de nivel de red, aplicación y NGFW.
29. Técnicas y herramientas de seguridad en el cliente final. Sistemas antivirus y EDR.
30. Técnicas y herramientas de detección y prevención de amenazas. Sistemas IDS e IPS.
31. Técnicas y herramientas de análisis y correlación de eventos SIEM, Sistemas de detección y respuesta (XDR y plataformas SOAR).
32. Informática forense. Conceptos básicos. Análisis forense. Recolección y conservación de evidencias digitales. Peritaje. Redacción de informes forenses. Herramientas de informática forense.
33. Gestión de incidentes. Planes de gestión de ciberincidentes de seguridad. Herramientas de gestión de incidentes. SAT-ICS, SAT-INET, SAT-SARA. LUCIA, CERTs, CSIRTs en España y en la Unión Europea.
34. Análisis de incidentes complejos de ciberseguridad, mitigación de incidentes. Planes de respuesta y recuperación.
35. Ciberinteligencia y cibervigilancia. OSINT, HUMINT, IMINT. Análisis de inteligencia.
36. Cifrado y criptografía. Algoritmos de Hashing. Sistemas de cifrado simétricos y asimétricos. Principales suites y algoritmos de cifrado. Principales estándares de cifrado.
37. Infraestructura de clave pública. PKI. Funcionamiento y buenas prácticas. Tipos de certificados según su uso.
38. Identificación y firma electrónica. Marco normativo. Prestación de servicios públicos y privados. DNI electrónico, mecanismos biométricos, Smart cards. Gestión de identidades.
39. Real Decreto 1112/2018 de accesibilidad, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público. Observatorio de la accesibilidad web.
40. Instrumentos para la cooperación entre Administraciones Públicas en materia de Administración Electrónica. Infraestructuras y servicios comunes. Integración con los sistemas de la administración local.
41. Sede electrónica para la tramitación online de servicios de los ciudadanos. Descripción, servicios, seguridad y legislación.
42. La contratación electrónica desde el punto de vista tecnológico. Elaboración de Pliegos técnicos. Criterios de valoración. Contratos de servicios y suministros TIC.
43. Soluciones de comercio electrónico, mecanismos de pago, pasarelas de pago y factura electrónica.
44. Esquema Nacional de Interoperabilidad y Normas técnicas (NTI). El documento electrónico, el expediente electrónico. Gestión del ciclo de vida del expediente y del documento.

45. Accesibilidad y usabilidad, Estándares W3C. Pautas de accesibilidad WCAG, UAAG, ATAG Diseño universal adaptativo.
46. Aplicaciones web. Lenguaje HTML. CSS. Lenguajes de script. Tecnologías de programación web: CGI, javaScript, applets, servlets, ASP, PHP, JSP. Servidores Web.
47. Web Services: estándares, protocolos asociados. Internacionalización y localización. UTF8. Unicode. Formatos de intercambio de datos (XML, JSON, etc.). Características. Esquemas, conceptos, fundamentos y tipos de datos.
48. Ingeniería inversa. Conceptos básicos. Principales herramientas. Descompiladores y desensambladores.
49. Sistemas y Tecnologías de Teletrabajo. Herramientas de trabajo en grupo. Sistemas de videoconferencia. Aplicaciones prácticas en la Administración local. Securitización en entornos de teletrabajo. La problemática del Shadow IT.
50. Virtualización del puesto de trabajo. Movilidad del puesto de trabajo. Sistemas VDI.
51. Tipos de sistemas de información multiusuario. Sistemas grandes, medios y pequeños. Virtualización de aplicaciones.
52. Equipos departamentales y estaciones gráficas de trabajo. Dispositivos personales: PC Portátil, Tablet, Smartphone y otros dispositivos. La conectividad de los dispositivos personales.
53. Paradigmas de computación distribuida y Servicios en Cloud. IaaS, PaaS, SaaS. Nubes privadas, públicas e híbridas. Securitización en entornos en la nube. La seguridad de los servicios cloud públicos.
54. Sistemas de almacenamiento para sistemas grandes y departamentales, SAN, NAS, Tecnologías de discos SATA, NL-SAS, SAS y SSD. Tiering. Topologías de almacenamiento de alta disponibilidad.
55. Sistemas de Backup. Políticas de gestión de copias de seguridad. Backup en cloud. Sistemas de recuperación de la información. Seguridad en las copias de seguridad, procedimientos y métodos para la conservación de la información.
56. Sistemas operativos (SO). Windows, Unix, Linux y otros SO de uso común. Administración de Sistemas operativos.
57. Bastionado SO Windows. Cifrado, GPOs...
58. Bastionado SO Linux. Cifrado, SELinux, servicios, políticas...
59. El procesamiento cooperativo y la arquitectura cliente-servidor. Clústeres y Sistemas de altas prestaciones.
60. Arquitectura de Sistemas de Información. Servidores de datos y de aplicaciones. Granjas de servidores.
61. Virtualización de servidores y SO. Tecnología de contenedores, microservicios, y serverless. Sistemas hiperconvergentes.
62. Los sistemas de gestión de bases de datos SGBD. Acceso y Control de Datos con Bases de Datos relacionales (ORACLE, MySQL, SQL SERVER... etc.). Administración de Bases de Datos.
63. Centro de Proceso de Datos: adecuación, características físicas. Seguridad física y lógica de un CPD. Control de acceso físico al CPD y a dispositivos. Niveles de Seguridad y acceso.
64. Tecnologías de Cadenas de bloques (Blockchain).
65. Técnicas de machine learning (aprendizaje automático), Inteligencia Artificial y Big Data.
66. Seguridad en el puesto de usuario. Formación, concienciación, auditoría, restricciones a aplicar.
67. Redes de área local. Arquitectura. Tipología. Medios de transmisión. Métodos de acceso. Dispositivos de interconexión. Gestión de dispositivos. Administración de redes. Gestión de usuarios. Monitorización y control de tráfico. Gestión SNMP. Configuración y gestión de redes virtuales (VLAN).
68. Securitización de redes LAN.
69. Arquitectura de las redes Intranet y Extranet. Concepto, estructura y características. Su implantación en las organizaciones.
70. Redes inalámbricas: el estándar IEEE 802.11. Características funcionales y técnicas. Sistemas de expansión del espectro. Sistemas de acceso. Autenticación. Modos de operación, Bluetooth. Seguridad. Normativa reguladora.
71. Seguridad de redes inalámbricas. Ataques conocidos, configuraciones de seguridad, medidas adicionales de seguridad.
72. Redes IP: arquitectura de redes, encaminamiento y calidad de servicio. Transición y convivencia IPv4-IPv6.

73. Seguridad de redes IP. Ataques y configuraciones de seguridad L3-L4.
74. Redes privadas virtuales. Topologías y escenarios de uso. Configuraciones de seguridad en escenarios Site-to-site y de acceso.
75. Ataques de Denegación de servicio. (DoS y DDoS) técnicas de ataque y contramedidas de protección.
76. Servicio DNS: Funcionamiento, arquitectura, configuración segura. Ataques. DNSSEC. Uso como herramienta de detección/bloqueo de amenazas.
77. Sistemas de compartición de ficheros: CIFS / NFS / FTP / Webdav/... Funcionamiento de los servicios, configuraciones de seguridad y ataques.
78. El correo electrónico. Funcionamiento, configuraciones y protocolos de seguridad SPF, DKIM, DMARC.
79. Seguridad en las comunicaciones de voz. Comunicaciones móviles, fijas y VoIP.
80. Protocolos de directorio basados en LDAP y X.500.
81. Active Directory. Arquitectura y seguridad.
82. La seguridad en el nivel de aplicación. Tipos de ataques y protección de servicios web, bases de datos e interfaces de usuario. WAF (validación de entrada, Gestión de cookies, Inyección de SQL, Cross-site scripting (XSS), Cross-site request forgery, Autenticación y gestión de sesión).
83. Metodologías de gestión de proyectos, (PMP, PMI, Agile, Scrum, etc.).
84. Gestión de riesgos de la cadena de suministros (SCRM) (Riesgos asociados al hardware, software y servicios. Monitorización de terceros. Requisitos mínimos de seguridad y acuerdos de nivel de servicio).
85. Gestión segura de los activos (Propiedad de la información y de los activos. Inventario de activos. Gestión de activos).
86. Políticas y ciclo de vida de las contraseñas y los certificados. Sistemas de autenticación múltiple.
87. Sistemas de autenticación (OIDC, Oauth, SAML, kerberos, RADIUS, TACACS+...).
88. Seguridad de dispositivos móviles. Seguridad en Android e IOS. Funcionalidades de soluciones MDM.
89. Seguridad en dispositivos IoT y entornos industriales.
90. Prevención de fuga de datos (DLP). Gestión de dispositivos móviles, almacenamiento removible. Medidas DLP en la red. Limpieza de metainformación en documentos. Borrado seguro de dispositivos. Control de impresión.

## ANEXO IV

**ACEPTACIÓN EXPRESA PARA SOMETERSE A LAS PRUEBAS MÉDICAS  
QUE SEAN NECESARIAS PARA ACREDITAR LA CAPACIDAD FUNCIONAL  
PARA EL DESEMPEÑO DE LAS TAREAS Y FUNCIONES DEL PUESTO**D./D<sup>a</sup>. .....

con D.N.I. número ..... acepto expresamente someterme a las pruebas  
médicas que sean necesarias para acreditar mi capacidad funcional para el desempeño de las  
tareas y funciones del Puesto de Trabajo.

En Alcorcón, a ..... de ..... de .....

Fdo. ....

## ANEXO V

**DECLARACIÓN RESPONSABLE  
DE NO HABER SIDO SEPARADO DEL SERVICIO NI HALLARSE INHABILITADO**D./D<sup>a</sup>. .....

con D.N.I. número ....., declaro:

- que no he sido separado/a mediante expediente disciplinario del servicio de cualquiera de las administraciones públicas o de los órganos constitucionales o estatutarios de las comunidades autónomas,
- que no me hallo en inhabilitación absoluta o especial para empleos o cargos públicos por resolución judicial, para el acceso al cuerpo o escala de funcionarios, o para ejercer funciones similares a las que desempeñaban en el caso de personal laboral, en el que hubiese sido separado o inhabilitado.
- En el caso de ser nacional de otro Estado, no me hallo inhabilitado o en situación equivalente ni he sido sometido a sanción disciplinaria o equivalente que impida, en mi Estado, en los mismos términos el acceso al empleo público.

En Alcorcón, a ..... de ..... de .....

Fdo. ....

## ANEXO VI

**DECLARACIÓN RESPONSABLE EN RELACIÓN CON LA EXENCIÓN  
DEL PAGO DE TASAS DE EXAMEN**D./D<sup>a</sup>. .....

con D.N.I. número ....., declaro:

- 
- Que tengo reconocida una discapacidad igual o superior al 33%

Debe aportarse certificado en el que figure el grado de discapacidad

- 
- Que soy demandante de empleo durante el plazo, al menos, de un mes anterior a la fecha de esta convocatoria, y que, además, no he rechazado oferta de empleo adecuado ni me he negado a participar en acciones de promoción, formación o reconversiones profesionales, y carezco de rentas superiores en cómputo mensual, al salario mínimo interprofesional.

Deben aportarse los siguientes documentos:

- Demanda de empleo o informe de situación administrativa
  - Informe negativo de rechazos
  - Resolución con el importe de la prestación concedida o certificado de no percibir ninguna prestación
- 
- Que todos los miembros de mi unidad familiar nos encontramos en situación de desempleo.

Deben aportarse los siguientes documentos:

- Libro de familia
- Demanda de empleo o informe de situación administrativa de todos y cada uno de los miembros de la unidad familiar mayores de edad

En Alcorcón, a ..... de ..... de .....

Fdo. ....”

Los anexos II (solicitud) y III (autobaremo) podrán descargarse en la página web municipal.

Madrid, a 30 de septiembre de 2022.

(01/19.016/22)

