PERFIL 3: RESPONSABLE DE ÁREA ADMINISTRADOR DE SISTEMAS - COMUNICACIONES

REFERENCIA: 2024/T5B-TIC COMUNICACIONES

1. DESCRIPCIÓN DE LA PLAZA CONVOCADA

- Denominación: Grupo I, Técnico Nivel 5, Subnivel T5b.
- Grupo Profesional: Grupo I (Técnico).
- Número de plazas convocadas: 1.
- Departamento: Departamento TIC (Secretaría General).
- Convenio aplicable: Convenio Colectivo del Instituto para la Diversificación y Ahorro de la Energía BOCM Núm. 79 de 3/4/2009).
- Retribuciones brutas anuales: 49.613,82€, más un complemento salarial por cumplimiento de objetivos y en el puesto de trabajo regulado en el Art. 60 del Convenio Colectivo de IDAE, de hasta 6.546,62 €.
- Tipo de jornada: Jornada según artículos 40 y siguientes del Convenio Colectivo de IDAE.
- Lugar de trabajo: Madrid.

2. REQUISITOS ESPECÍFICOS EXCLUYENTES

- Titulación universitaria superior o media (nivel mínimo MECES 2). La titulación universitaria lo será en una disciplina acorde con las funciones del puesto.
- Experiencia profesional mínima de 10 años como Responsable de Comunicaciones, Arquitecto de Comunicaciones TIC, Jefe de Proyecto de Comunicaciones TIC o análogas, o trabajos análogos a las funciones descritas.

3. VALORACIÓN FASE II: CONCURSO DE MÉRITOS (máximo 40 puntos)

3.1. FORMACIÓN ACADÉMICA, IDIOMAS, FORMACIÓN COMPLEMENTARIA Y PONENCIAS	**Puntuación máxima**
1. Titulaciones universitarias oficiales en disciplinas acordes con las funciones de los puestos de trabajo ofertados. Sólo se considerarán en este apartado los títulos universitarios oficiales, bien sean de máster universitario, diploma de estudios avanzados de doctorado, etc.	2,00

Titulaciones nivel MECES 3	1,00
Titulaciones nivel MECES 4	2,00

<table>
<tr>
<td>2. Disponer de un nivel de inglés acreditado mediante título oficial La referencia para el nivel mínimo de inglés exigible será el correspondiente al Marco Común Europeo de Referencia para las Lenguas o título equivalente.
<table>
<tr><td>Nivel B2</td><td>0,50</td></tr>
<tr><td>Nivel C1</td><td>1,00</td></tr>
<tr><td>Nivel C2</td><td>2 ,00</td></tr>
</table>
</td>
<td>2,00</td>
</tr>
<tr>
<td>3. Cursos de perfeccionamiento, formaciones/certificaciones, siempre y cuando, a criterio del Órgano de Selección, estén vinculados con materias relacionadas, funciones y tareas del perfil del puesto.
- No darán derecho a puntuar los cursos relacionados con la informática de usuario y el inglés.
- Los cursos que darán derecho a puntuar como relacionados con las necesidades del puesto de trabajo a cubrir estarán relacionados con las funciones principales y tareas detallados en el apartado de funciones principales/ tareas a realizar
- Será potestad del Órgano de selección la determinación de los cursos que darán derecho a puntuar y que se consideren como relacionados con las necesidades del puesto de trabajo a cubrir.</td>
<td>2,00</td>
</tr>
<tr>
<td>4. Certificaciones relevantes del tipo siguiente o equivalentes que podrán tenerse en cuenta:
• CCNA (Cisco Certified Network Associate)
• CCNP (Cisco Certified Network Professional)
• Fortinet NSE (Network Security Expert)
• CompTIA Network+
• CISM (Certified Information Security Manager)
• CEH (Certified Ethical Hacker)
• CISSP (Certified Information Systems Security Professional)</td>
<td>3,00</td>
</tr>
</table>

3.2. EXPERIENCIA PROFESIONAL	**Puntuación máxima**
1. Experiencia profesional demostrable en la definición, implantación, desarrollo y mantenimiento de servicios internos y de infraestructura tales como: • Arquitectura de redes, incluyendo diseño y configuración de redes LAN, WAN, WLAN, MPLS, etc. • Gestión y administración de firewalls. • Tecnologías de enrutamiento y conmutación (Cisco, Juniper, etc.). • Configuración y mantenimiento de switches y cores de red. • Gestión de infraestructuras de la DMZ y servicios internet: FTP, SMTP, etc. • Herramientas de monitoreo y gestión de redes (Nagios, SolarWinds, etc.). • Configuración de servicios sobre VozIP, Gateway de voz, etc. • Experiencia con soluciones de autenticación multifactor (MFA), sistemas de prevención de pérdida de datos (DLP) y soluciones de seguridad en la nube. • Seguridad perimetral, incluyendo sistemas de detección y prevención de intrusiones (IDS/IPS) y VPNs. • Implementación o gestión de Web Application Firewalls (WAF) de los diferentes proveedores de soluciones tanto on-premise como soluciones nube (FortiWeb, F5 BIG-IP ASM, AWS WAF, Azure WAF, etc.)	10,00
2. Experiencia profesional demostrable en el diseño, implantación y mantenimiento en sistemas y servicios, en especial, los definidos a continuación: • Firewall Fortigate. • Fortianalyzer. • Fortimanager. • VPNs de usuario y Site to Site.	10,00

3. Experiencia profesional demostrable en comunicaciones y en Instrumentos para la cooperación entre Administraciones Públicas en materia de administración electrónica, infraestructuras y servicios comunes. Integración con los sistemas de la administración. • Electrónica de Red. • Switches LAN, Routers, Backbone. • Interoperabilidad entre sistemas: Red SARA, aplicaciones de terceros, aplicaciones internas, … • Conectividad a internet: túneles IPSEC, redes privadas, públicas, accesos remotos, etc.	5,00
4. Experiencia profesional demostrable en seguridad de redes, prevención, localización y reacción ante posibles incidentes de seguridad, aplicando buenas prácticas de seguridad en el ámbito de las comunicaciones. • Esquema Nacional de Seguridad, procedimientos y Normas. Guías Serie 800. • Herramientas y soluciones CCN-CERT. • Instrucciones Técnicas de Seguridad (ITS): Notificación de incidentes de seguridad, auditoria de seguridad de sistemas de información, de conformidad con el ENS. • Concienciación y cultura en seguridad de la información y ciberseguridad.	5,00
5. Experiencia profesional demostrable en la definición de pliegos técnicos e interlocución con proveedores de infraestructura, así como en la confección de normativa interna de uso, protección de datos y de recursos informáticos, propiedad del software y otros aspectos de seguridad informática, en base a la legislación vigente. En este apartado, se valorará la experiencia en la elaboración y mantenimiento del inventario del software, controlando la situación legal de los programas existentes y resolviendo las anomalías encontradas, así como la capacidad de análisis y propuesta de soluciones para la protección de los activos informáticos, estudiando los posibles riesgos y requerimientos de seguridad.	1,00

Quedarán excluidos los aspirantes que no alcancen un mínimo de 12 puntos en la fase II de concurso de méritos.

4. FUNCIONES PRINCIPALES/TAREAS A REALIZAR

En la actualidad el IDAE dispone de unos 275 usuarios en sus oficinas situadas en edificios de uso exclusivo ubicados en C/Madera 8 y C/Beneficencia 2 en Madrid. El equipamiento hardware y software es muy homogéneo para todos los usuarios, teniendo como base PC's con una antigüedad inferior a los 4 años y como componentes principales Sistema Operativo Windows 10, 11 y Microsoft 365 y Office 365 como herramientas de trabajo.

Dentro del área de sistemas, para los servidores y demás componentes que configuran la lógica de red, comunicaciones, almacenamiento y backup, existe un entorno muy homogéneo. La mayoría de los elementos son Fortinet (Chasis, Switches, etc.) además de algunos elementos NetApp y servidores HP.

Entorno de elementos físicos:

- Red local Ethernet 10/100/1000 Base-T.
- Conmutadores, Switches y electrónica de red Fortinet con Red a 40 GB y 10 GB.
- Red Wifi – Fortinet con 47 PA
- 15 servidores físicos Intel
- 60 máquinas Virtuales
- 290 puestos de ordenadores personales
- 300 portátiles
- 7 armarios de comunicaciones y servidores.
- Robots de cinta y almacenamiento SAN de discos
- Equipos multifunción (Impresora, escáner, fotocopiadora, …)
- Sondas de red del CCN
- Sede Electrónica

Entorno lógico:

- Puestos de trabajo: ordenadores personales y portátiles con sistemas operativos Windows 10/11
- Microsoft 365
- Sistema operativo de los servidores: Windows 2012/2019/2022, LINUX
- Clúster Microsoft
- Virtualización VMware ESXI/Hyper-v
- Directorio Activo de Microsoft, DNS, DHCP, WINS, WINSUS, DFS, etc.
- Segmentación. 10 redes lógicas virtuales
- Sistemas de base de datos: Oracle 11g y 19c, SQL Server y MySQL
- Servidor de correo Exchange 365
- Sistema de copias de los servidores: VEEAM y Veritas
- Sistemas de copias de seguridad y archivado en la nube de Barracuda
- Seguridad de correo en la nube Microsoft Defender

- Gestor documental Alfresco y SharePoint
- Registro de Entrada/Salida: GEISER
- Servidor VPN de Fortinet
- Servidor Aplicaciones: IIS, Apache Tomcat y WebLogic
- Administración entornos WampServer
- Clúster Firewall Fortigate de Fortinet
- Panda Adaptive Defense 360+Patch Management
- Protocolo de comunicaciones: TCP-IPv4.
- Sistemas Videoconferencia Modena, Webex y Teams
- Gestor de Incidencias Redmine
- SCCM

Funciones Principales:

Como Responsable de Área, será el encargado del desempeño de uno o varios conjuntos de actividades de trabajo y/o proyectos dentro del Departamento TIC de Comunicaciones. Entendiendo por proyecto un contenido de trabajo planificado, con asignación de tareas y responsabilidades, que utiliza recursos económicos y/o humanos, y es susceptible de alcanzar resultados evaluables. Las funciones principales del puesto de trabajo, relacionadas con el ámbito de actuación del departamento TIC-Comunicaciones, son las siguientes:

- Realizar estudios e informes para la implantación de nuevas funcionalidades y procedimientos para incrementar la seguridad y eficacia de los sistemas de comunicación y dar respuesta a las necesidades de la organización.
- Realizar, analizar, supervisar y controlar proyectos, y realizar la dirección de proyectos en las instalaciones de comunicaciones.
- Analizar y realizar el seguimiento de las instalaciones de comunicaciones asignadas, proponiendo, en su caso, medidas correctoras e identificar las necesidades de nuevas instalaciones o mejora de las existentes y desarrollarlas.
- Programar, coordinar, organizar y ejecutar el mantenimiento de las instalaciones de comunicaciones.
- Definir, aplicar y supervisar medidas y sistemas de ciberseguridad.
- Realizar y supervisar estudios, análisis e informes y emitir documentación técnica.
- Coordinar el proceso de gestión y evaluación de riesgos asociados a su ámbito.
- Elaborar, dirigir, coordinar y realizar la gestión técnica y económica de proyectos sobre sistemas, redes, infraestructuras y servicios de telecomunicaciones.
- Modelar, diseñar, implantar, gestionar, operar, administrar y mantener redes, servicios y contenidos.
- Realizar la planificación, toma de decisiones y empaquetamiento de redes, servicios y aplicaciones de telecomunicaciones considerando la calidad de servicio, los costes directos y de operación, el plan de implantación, supervisión, los procedimientos de seguridad, el escalado y el mantenimiento, así como gestionar y asegurar la calidad en el proceso de desarrollo.

- Integrar tecnologías y sistemas de la Ingeniería de Telecomunicación.
- Elaboración de informes periódicos de la utilización de los servicios de red, disponibilidad y capacidad de las redes.
- Coordinar el mantenimiento preventivo y correctivo de hardware de los dispositivos LAN, Wifi, Firewall, proxy, etc.…
- Redacción y valoración de los pliegos en el ámbito de la Dirección TIC, así como la supervisión en el cumplimiento de los pliegos y contratos.
- Dirigir y gestionar el equipo humano del departamento y el personal externo.
- Elaboración de documentación técnica y presentaciones directivas. Elaboración de documentación de formación.
- Validación tecnológica de plataformas y soporte a otras áreas de TIC.

Responsabilidades Técnicas:

- Soporte a usuarios en modo remoto y presencial, con aplicaciones ofimáticas, certificados, correo electrónico, firma electrónica, etc.
- Implementar y mantener dispositivos de seguridad perimetral, incluyendo firewalls, sistemas de detección y prevención de intrusiones (IDS/IPS), VPNs y Web Application Firewalls (WAF).
- Configurar y gestionar sistemas Fortinet, incluyendo FortiGate, FortiAnalyzer y FortiManager.
- Diseñar y optimizar la arquitectura de redes, abarcando redes LAN, WAN y WLAN.
- Configurar y mantener redes de comunicaciones internas utilizando switches y cores.
- Diagnosticar y resolver problemas de conectividad y rendimiento. Gestión y resolución de incidencias TIC.
- Colaborar con otros equipos para asegurar la integridad y seguridad de la red.
- Documentar procedimientos y configuraciones.
- Soporte a auditorías de seguridad y pruebas de penetración para identificar y mitigar vulnerabilidades.
- Monitorear y analizar el tráfico de red para detectar actividades sospechosas y responder a incidentes de seguridad.
- Desplegar y gestionar tecnologías de seguridad perimetral, incluyendo WAF, para proteger aplicaciones web contra amenazas como inyecciones SQL, cross-site scripting (XSS) y ataques DDoS.
- Mantenerse actualizado con las últimas tendencias y tecnologías en ciberseguridad y telecomunicaciones.
- Operación de plataformas de infraestructura basadas en Microsoft Windows Server.