Plan de formación. Contrato formativo para la obtención de la práctica profesional.

Titulación: Técnico Superior en Administración de Sistemas Informáticos en Red (ASIR).

Puesto de trabajo: Técnico de Sistemas para el Centro de Proceso de Datos (CPD)

Área funcional: Infraestructuras

1.- Finalidad y Objetivo

Dotar de la experiencia práctica a la persona contratada en aspectos relevantes propios de un Centro de Proceso de Datos:

Operatividad: Garantizar la disponibilidad, rendimiento y continuidad de los servidores, almacenamiento e infraestructura de red del CPD.
Mantenimiento: Ejecutar tanto tareas preventivas (revisión de logs, climatización, cableado) como correctivas (sustitución de hardware dañado).
Monitorización: Controlar alertas de los sistemas y servicios críticos las 24 horas del día.
Soporte: Ofrecer soporte técnico de segundo nivel ante incidentes y escalados.

2.- Competencias profesionales a desarrollar

Gestión de Infraestructura Física y de Red

- Cableado estructurado: Conectorización y organización de fibra óptica y par de cobre en los racks.
- Arquitectura de red: Configuración de VLANs, switches, routers y políticas básicas de firewall.
- Sistemas de soporte: Comprensión y seguimiento de los sistemas de alimentación ininterrumpida (SAI/UPS) y climatización ambiental.

Administración de Sistemas y Servidores

- Sistemas Operativos: Despliegue, configuración y securización de servidores en entornos Windows Server y distribuciones Linux (como Enterprise Linux o Debian).

• Virtualización: Gestión básica de hipervisores (VMware vSphere, Proxmox o Hyper-V) y aprovisionamiento de máquinas virtuales.
• Almacenamiento: Monitorización de cabinas de discos (SAN/NAS) y aprovisionamiento de volúmenes.

Monitorización y Copias de Seguridad
• Herramientas de monitorización: Uso diario de plataformas de alertas (como Zabbix, Nagios o Grafana) para supervisar CPU, RAM, espacio y tráfico de red.
• Políticas de Backup: Configuración y verificación de tareas de copia de seguridad (Veeam Backup, Bacula, etc.) y pruebas periódicas de restauración de datos.

Seguridad y Resolución de Incidencias

• Gestión de incidencias: Uso de herramientas de ticketing (como Jira Service Management o GLPI) siguiendo marcos metodológicos (ITIL).
• Ciberseguridad aplicada: Gestión de accesos, políticas de contraseñas, bastionado de sistemas y aplicación de parches de seguridad críticos.

3.-Actividades y tareas a realizar por la persona trabajadora durante el contrato formativo. Relación con los objetivos formativos

Bloque 1: Monitorización y Gestión de Alertas del CPD
• Actividades y tareas específicas:
o Supervisar de forma continua las consolas de monitorización del CPD (ej. Zabbix, Nagios, Grafana) para detectar anomalías en servidores, almacenamiento o red.
o Realizar el triaje y clasificación inicial de las alertas generadas por los sistemas automatizados.
o Documentar y registrar los incidentes en la plataforma de ticketing de la empresa (ej. Jira, GLPI) siguiendo los procedimientos internos.
o Verificar diariamente los parámetros ambientales del CPD (temperatura, humedad) y el estado de los sistemas de alimentación ininterrumpida (SAI/UPS).
• Relación con los objetivos formativos:
o Desarrollar la capacidad de anticipación ante fallos del sistema, aprender a priorizar incidencias según su impacto en el negocio y familiarizarse con la infraestructura crítica de hardware y climatización de un entorno de alta disponibilidad.

Bloque 2: Operaciones de Almacenamiento y Copias de Seguridad (Backup)

- Actividades y tareas específicas:
  - Revisar los logs diarios de ejecución de los planes de respaldo (ej. Veeam Backup, Bacula) para asegurar que todas las copias se han realizado correctamente.
  - Ejecutar tareas programadas de mantenimiento de almacenamiento, como la verificación de espacio libre en cabinas SAN/NAS.
  - Colaborar bajo supervisión en pruebas periódicas de restauración de datos en entornos de laboratorio para validar la integridad de las copias.
  - Gestionar el ciclo de vida de los soportes de almacenamiento físico si el CPD requiere custodia o rotación de cintas/discos.
- Relación con los objetivos formativos:
  - Comprender la importancia crítica de la política de salvaguarda de la información, asimilar los conceptos de RTO (Recovery Time Objective) y RPO (Recovery Point Objective), y dominar herramientas profesionales de continuidad de negocio.

Bloque 3: Administración y Mantenimiento de Servidores y Sistemas Operativos

- Actividades y tareas específicas:
  - Apoyar en el aprovisionamiento, instalación y actualización de parches de seguridad en servidores físicos y virtuales (Windows Server y entornos Linux).
  - Realizar tareas de administración de identidades y accesos (ej. creación de usuarios, asignación de permisos en Active Directory o LDAP) siguiendo el principio de mínimo privilegio.
  - Ejecutar el despliegue de máquinas virtuales a partir de plantillas preconfiguradas en el hipervisor (ej. VMware vSphere, Proxmox).
  - Colaborar en el montaje físico de servidores en los racks, conexionado de cableado estructurado y etiquetado normativo de la infraestructura.
- Relación con los objetivos formativos:
  - Afianzar de forma práctica los conocimientos de sistemas operativos de red y virtualización empresarial, adquiriendo destreza tanto en la gestión lógica (consola y comandos) como en el despliegue físico de hardware en salas técnicas.

Bloque 4: Gestión de Redes y Seguridad Perimetral del CPD

- Actividades y tareas específicas:
  - Comprobar la conectividad de los equipos de comunicaciones (switches, routers, firewalls) y monitorizar el consumo de ancho de banda de los enlaces.
  - Asistir en la configuración de puertos de red, asignación de direcciones IP estáticas y segmentación básica de redes mediante VLANs bajo el esquema del CPD.

o Colaborar en la aplicación de políticas de bastionado (hardening) de sistemas y en la revisión de logs de seguridad para detectar accesos no autorizados.
• Relación con los objetivos formativos:
o Trasladar los modelos teóricos de red (OSI y TCP/IP) a una infraestructura real y compleja, asimilando la criticidad de la seguridad perimetral y el aislamiento de redes en un CPD.

4.- Duración del contrato formativo. Horario previsto

35 horas a la semana. Aplica la instrucción de horario del personal de la Fundación.
De 08:00 a 15:00 horas de lunes a viernes (presencia obligatoria de 9:00 a 14:00) y una tarde de 2,5 horas al menos, entre el lunes y el jueves.
Duración del contrato: 6 meses, con posible prórroga por 6 más.

5.- Tutor/a y responsable/s de la formación

José Manuel Cuena Ramos, director del Área de Infraestructuras y CPD de la Fundación Universidad de Valladolid M.P.

6.-Sistema de evaluación de la formación
Métodos para valorar el progreso del trabajador
Frecuencia de reuniones de seguimiento

Reuniones quincenales para evaluar el progreso.
Permanente trabajo en equipo

Fdo. Tutor

Normativa	Este documento tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de original (art. 27 Ley 39/2015).	Estado	Fecha y hora	
Firmado por	Jose Manuel Cuena Ramos - Director Área Infraestructuras Fundación Uva	Firmado	22/09/2026 10:37:09	
URL de verificación	https://sede.uva.es/validador-documentos?code=5DRLMSCwjYf7nXxtAEq1Ig%3D%3D			

