Yosef Naabid Gutiérrez

Administrador de infraestructura Windows y Linux

yosefnaabid@gmail.com | yosefnaabid.com | github.com/yosefnaabid | www.linkedin.com/in/yosefnaabid | +34 602 47 31 24

(Almería, España)

RESUMEN

Administrador de sistemas e infraestructura, **único responsable técnico de un entorno de producción 24/7** y anteriormente, de los sistemas de una **red de clínicas y postgrados universitarios con 90 sedes**. Especializado en entornos Windows y Linux, virtualización, seguridad de red e identidad y automatización de infraestructuras con monitorización y copias de seguridad. Busca incorporarse a un proyecto estable a largo plazo.

COMPETENCIAS TÉCNICAS

Sistemas y virtualización: Windows Server, Linux (Debian, RHEL), VMware ESXi/vCenter, Proxmox VE, Hyper-V, Active Directory (LDAP, GPO), Entra ID, Microsoft 365, Intune, Exchange
Redes y seguridad: firewalls (Sophos XGS, OPNsense, nftables), Sophos Endpoint, MikroTik RouterOS, VPN (WireGuard, Sophos VPN), SELinux, CrowdSec, Nginx, Cloudflare, Let's Encrypt (HTTPS/TLS), VLAN, DHCP, DNS
Automatización y operaciones: Bash, PowerShell, Python (pytest), Ansible, Terraform, Docker, Kubernetes, Git, GitHub Actions, CI/CD, systemd, Zabbix, Prometheus, Alertmanager, Grafana, ServiceNow ITSM, Veeam Backup, PostgreSQL, RAID/NAS

EXPERIENCIA

Administrador de sistemas e infraestructura **Noviembre 2025 – Actualidad**
Meridia Softworks *Remoto*

- Consolidé **más de 20 servicios en un mismo servidor**, cada uno aislado en su contenedor con límites de CPU y memoria y arranque automático, para que el que se descontrola no arrastre a los demás
- Saqué la administración fuera de internet por completo; hoy la única entrada es un **túnel cifrado terminado en el propio router**, y los intentos de acceso se bloquean solos
- Mantengo un **tiempo máximo de recuperación de 10 minutos de la base de datos de producción**, verificado cada mes con una restauración completa en entorno aislado y procedimiento documentado
- Reduje la **detección de fallos a menos de 60 segundos en más de 20 servicios** y eliminé la intervención manual en la recuperación diseñando un sistema de alertas con reinicio automático del servicio y escalado
- Puse toda la infraestructura en código, de forma que el entorno **se reconstruye desde cero en 15 minutos**, sin ningún paso que dependa de conocimiento no documentado ni de una máquina concreta
- Mudé la producción a un servidor dedicado **sin que los clientes notaran ninguna interrupción**, levantando el nuevo host desde esa definición en código y haciendo el cambio en una sola ventana

Administrador de sistemas y redes **Agosto 2024 – Octubre 2025**
Grupo PgO UCAM (Universidad Católica de Murcia) y Clínicas DEA *Almería, España*

- **Migré 20 servidores físicos a 25 máquinas virtuales** repartidas entre el clúster del CPD y hosts en alta disponibilidad en sedes, haciendo que un host caído ya no parase el servicio
- Segmenté **más de 150 dispositivos en 6 zonas aisladas**, unidas entre sedes por túneles cifrados y con protección en cada puesto, dejando dos barreras entre un equipo infectado y los historiales clínicos
- Preparé la copia de los historiales clínicos para la **auditoría RGPD** con procedimiento documentado, restauraciones verificadas en más de 30 servidores y copias inmutables que no puede borrar un ransomware
- Monté la monitorización de **10 clínicas y 300 usuarios**, llevando la detección de una caída de la llamada del usuario a un aviso y un ticket en menos de 10 minutos, y atendí esas incidencias como N2-N3 con el equipo IT
- Reduje en **más de 5.000 € al año** el gasto en licencias de Microsoft 365, midiendo qué usaba de verdad cada puesto y bajando de plan o recuperando licencias sin uso o huérfanas durante años

PROYECTOS

Clúster Kubernetes en alta disponibilidad verificado con cuatro simulacros de desastre | *Clúster de tres nodos levantado desde código y gobernado desde Git, donde matar un nodo no corta el servicio y la pérdida completa del clúster se reconstruye sola, datos incluidos, en menos de 10 minutos*

Segmentación de red con reglas de firewall generadas como código | *Red de seis VLANs cuyas reglas de firewall se generan desde un único fichero, con pruebas automáticas que tumban cualquier cambio que deje expuesto un segmento aislado*

Dominio Windows Server 2025 endurecido con CIS Benchmark | *Dominio completo levantado y administrado desde la línea de comandos en lugar de la interfaz gráfica, con los controles de seguridad que exigen las auditorías en lugar de los que trae por defecto*

Monitorización con Zabbix definida como código | *Servidor Zabbix completo que se levanta con un solo comando, con hosts, triggers y alertas definidos en ficheros y aplicados por API en lugar de por la interfaz*

Backup y recuperación en Proxmox verificados con un desastre provocado | *Hipervisor y sus VMs administrados de punta a punta con Ansible, copias programadas con retención y un script que destruye una VM y verifica que la restauración devuelve IP, datos y servicio*

FORMACIÓN ACADÉMICA

Técnico Superior en ASIR *(Administración de Sistemas Informáticos en Red)* *IES Aguadulce, Almería*
Técnico en SMR *(Sistemas Microinformáticos y Redes)* *IES Puebla de Vícar, Almería*

CERTIFICACIONES E IDIOMAS

Certificaciones: CCNA 200-301, Azure AZ-104, ITIL Foundation, Google Cybersecurity, CompTIA Security+ (previsto 2026)
Idiomas: Español nativo, Inglés B2 (Certificado de Cambridge)