



IGNACIO GAITÁN

ADMINISTRADOR DE SISTEMAS

CONTACTO

+34-601725876

ignaciogtan@gmail.com

Mallorca (Islas Baleares)

github.com/nachogtan

[linkedin.com/ignaciogaitan](https://www.linkedin.com/in/ignaciogaitan)

FORMACIÓN COMPLEMENTARIA

- [Google Cybersecurity Professional Certificate V2](#)
- [Networking Devices and Initial Configuration](#)
- [AWS Cloud Quest: Cloud Practitioner - Training Badge](#)
- [Google Data Analytics Professional Certificate](#)
- [CCNA: Introduction to Networks](#)

IDIOMAS

- Español Nativo
- Inglés B2
- Italiano B2



SOBRE MÍ

Estudiante de Administración de Sistemas (ASIR) con especial interés en el despliegue de infraestructuras críticas y seguridad defensiva. Con experiencia práctica en la implementación de modelos Zero Trust, monitorización con SIEM (Splunk) y virtualización. Destaco por mi capacidad para automatizar procesos y mi mentalidad analítica orientada a la resolución de incidentes. Busco aportar mi proactividad y conocimientos técnicos en un entorno profesional desafiante.



HABILIDADES TÉCNICAS

Redes

- Protocolos y Servicios: Administración avanzada de TCP/IP, DNS, DHCP y Proxy.
- Análisis de Tráfico: Monitoreo y diagnóstico de red con Wireshark y tcpdump.
- Seguridad y Túneles: Implementación de VPNs (WireGuard, OpenVPN) y exposición segura con Cloudflare Tunnel.
- Balaneo: Gestión de alta disponibilidad mediante Nginx o HAProxy.

Sistemas

- Entornos: Administración avanzada de distribuciones Linux (Debian/Ubuntu/CentOS) y Windows Server.
- Identidad: Gestión de dominios, GPOs y usuarios en Active Directory.
- Administración remota: Control seguro de servidores vía SSH, RDP y protocolos de transferencia (SFTP).

Virtualización y contenedores

- Orquestación: Despliegue de microservicios con Docker y Docker Compose.
- Hipervisores: Gestión de entornos críticos en Proxmox VE (Tipo 1) y VMware Player/VirtualBox (Tipo 2).
- Emulación: Manejo de máquinas virtuales con KVM y QEMU (Virt-Manager).

Ciberseguridad

- Control de Acceso: Configuración de Firewalls (ufw, iptables, firewalld) y Listas de Control de Acceso (ACL).
- Cloud Security: Gestión de políticas IAM, grupos de seguridad y NACLs en entornos AWS.
- Arquitectura: Implementación de principios Zero Trust y bastionado de sistemas (Hardening).

Automatización

- Scripting: Automatización de tareas críticas en Bash (Linux) y PowerShell (Windows).
- IaC: Definición de infraestructura mediante archivos YAML para Docker Compose y despliegues automáticos vía GPO.
- Mantenimiento: Programación de backups automáticos con Cron o Task Scheduler.

Cloud

- Plataforma: Gestión de instancias y servicios en AWS (EC2, S3, VPC, Route53).
- Monitoreo: Seguimiento de recursos con herramientas nativas como CloudWatch.



PROYECTOS

Laboratorio de red segmentada con router/firewall en Debian

Implementación de infraestructura virtualizada con Debian como router/firewall central mediante iptables, NAT e IP forwarding. Segmentación de entornos críticos (Windows Server/Kali Linux) con control de tráfico y monitorización SIEM centralizada en Splunk (rsyslog/Universal Forwarder). Auditoría de eventos, resolución DNS y validación de conectividad. Stack: Debian, VirtualBox, Splunk, TCP/IP, Linux/Windows.

→ [Ver en GitHub](#)

Detección de ataques de fuerza bruta con Splunk (MITRE ATT&CK T1110)

Simulación de ataques RDP (Kali) hacia entornos Windows/Debian con pipeline de detección en Splunk. Ingesta de logs vía Sysmon y Universal Forwarder para análisis de EventCode 4625. Desarrollo de consultas SPL, dashboards y alertas automáticas para identificación de patrones anómalos. Mapeo a MITRE ATT&CK con enfoque en triage y respuesta a incidentes en contexto SOC. Stack: Splunk, SPL, Sysmon, Kali Linux.

→ [Ver en GitHub](#)

Administración de Active Directory y políticas GPO en Windows Server

IDespliegue de entorno Active Directory para gestión centralizada de usuarios, equipos y políticas de seguridad (GPO). Aplicación del principio de mínimo privilegio mediante restricción de herramientas críticas (PowerShell, CMD, Regedit) y control de dispositivos. Automatización de despliegue de software (MSI) y administración de recursos compartidos con permisos NTFS/UNC y SYSVOL. Hardening de contraseñas y firewall de dominio. Stack: Windows Server, AD, GPOs, PowerShell, NTFS.

→ [Ver en GitHub](#)



FORMACIÓN

Administración de Sistemas Informáticos en Red

2024 - Presente

DigitechFP

Formación en administración de sistemas, redes, ciberseguridad y automatización.

Bachiller de Ciencias Naturales

2001 - 2004

Instituto Secundario Bernardino Rivadavia



EXPERIENCIA LABORAL

Diseño Gráfico (autonomo)

2019 - Actualidad

Desarrollo de materiales visuales y contenido digital para clientes.

Jefe de Rango

2019 - 2025

Hotel Posada Terra Santa

Atención al cliente y apoyo en la coordinación del servicio en equipo.

Jefe de Rango

2017 - 2019

Hotel Sant Francesc

Responsable de turno en servicio, coordinando tareas y asegurando la calidad de la atención al cliente en entornos de alta exigencia.