

## Auditoría OSINT: Reconocimiento Pasivo de Dominio

### Introducción

**Objetivo:** Realizar un reconocimiento pasivo completo del dominio usando herramientas OSINT como DNSDumpster, CentralOps.net, FOCA, Shodan, Google Dorks, etc.

**Dominio objetivo:** uady.mx

**Fecha de análisis:** 27 de julio de 2025

## 1. Mapeo DNS y Subdominios

### 1.1 Subdominios encontrados

- [www.uady.mx](http://www.uady.mx) → A (privado), hospedado en infraestructura Microsoft/AS8075, IP geolocalizada en EE. UU., Washington (Gridinsoft) [IPIP.NET+6Gridinsoft LLC+6Domain Glass+6](#)
- redi.uady.mx → 40.71.171.92, TTL ~86400, ubicado en Washington, Virginia, EE. UU. (Azure-hosted) [Domain Glass](#)
- Se listan otros subdominios: medicina.uady.mx, webmail.uady.mx, ingreso.uady.mx, mail.uady.mx, tunku.uady.mx, ccba.uady.mx, api.uady.mx, uadyvirtual.uady.mx, entre otros [Domain Glass](#)

### 1.2 Name Servers (NS)

- dziu.uady.mx → 148.209.1.34
- tunku.uady.mx → 148.209.1.1
- kuklincloud.uady.mx → 13.82.222.182 (Azure-hosted) [Wikipedia+7Gridinsoft LLC+7Domain Glass+7](#)

### 1.3 Registros MX

- redi.uady.mx aparece como entrada MX apuntando a reporintinfo.eastus.cloudapp.azure.com → 40.71.171.92 [Domain Glass](#)

## 1.4 Registros TXT (SPF, DMARC, etc.)

- No se encontró información pública específica sobre SPF o DMARC sin acceso privado.

## 2. WHOIS y Datos de Registro

**Dominio objetivo:** uady.mx

**2.1 Registrar:** AKKY ONLINE SOLUTIONS, S.A. DE C.V. [Gridinsoft LLCWhoisFreaks](#)

**2.2 Fecha de creación:** 2 de enero de 1995 [Gridinsoft LLCWhoisFreaks](#)

**2.3 Fecha de expiración:** 1 de enero de 2026 [Gridinsoft LLCWhoisFreaks](#)

**2.4 Estado del WHOIS:** Público, información visible con registrante RIUADY, admin/tech/billing Universidad Autónoma de Yucatán [Gridinsoft LLCWhoisFreaks](#)

**2.5 Contacto Técnico / Administrativo / Administrativo:** Universidad Autónoma de Yucatán, ubicada en Mérida, Yucatán, México [Gridinsoft LLCWhoisFreaks](#)

Buscar en la base de datos WHOIS

uady.mx no está disponible  
Es posible que aún podamos obtenerla para ti. [Ver cómo se hace](#)

Servicio de gestor de dominios  
MXN1,999.99

**Resultados de la búsqueda de WHOIS**

Información sobre el dominio	
Nombre	uady.mx
ID del dominio del registro	-
Registrado el	1995-01-02T00:00:00Z
Vence el	2026-01-01T00:00:00Z
Actualizado el	2024-12-29T00:00:00Z

**Encuentra tu dominio**

**Echa un vistazo a estas opciones alternativas**

uady.shop  
MXN18.37 ~~MXN1,112.99~~

### 3. Metadatos de Documentos (FOCA)

No se localizaron documentos públicos fácilmente accesibles desde FOCA directamente en el dominio `uady.mx` sin credenciales. Se sugiere ejecutar FOCA en PDFs descargables (tesis, investigaciones, planes) desde repositorios como *redi.uady.mx*, ya que podría revelar metadatos con autores, rutas internas, software usado o versiones.

The screenshot shows the CentralOps.net website interface. The 'Domain Dossier' section is active, displaying information for the domain `https://uady.mx/`. The interface includes a sidebar with navigation links like 'Domain Dossier', 'Domain Check', 'Email Dossier', and 'Browser Mirror'. The main content area shows the domain's canonical name, aliases, and IP addresses. Below this, the 'Domain Whois record' is displayed, showing the domain name, creation date, and various contact information for Microsoft.

**Domain Dossier** Investigate domains and IP addresses

domain or IP address `https://uady.mx/`

☒ domain whois record ☒ DNS records ☐ traceroute

☒ network whois record ☐ service scan

user: anonymous [187.150.233.243]  
balance: 48 units  
[log in](#) | [account info](#)

`https://uady.mx/` is a URL.  
Domain Dossier will continue with `uady.mx`.

To obtain Whois data redacted because of the GDPR or privacy services, try ICANN's RDRS. [\[more information\]](#)

**Address lookup**

canonical name `uady.mx`  
aliases  
addresses `20.169.251.95`

**Domain Whois record**

Queried `whois.mx` with "`uady.mx`"...

Domain Name: `uady.mx`  
Created On: 1995-01-02

City: Redmond  
StateProv: WA  
PostalCode: 98052  
Country: US  
RegDate: 1998-07-10  
Updated: 2025-06-10  
Comment: To report suspected security issues specific to traffic emanating from Microsoft online services, including the distribution of malicious content or other  
\* `https://cert.microsoft.com`  
Comment:  
Comment: For SPAM and other abuse issues, such as Microsoft Accounts, please contact:  
\* `abuse@microsoft.com`  
Comment:  
Comment: To report security vulnerabilities in Microsoft products and services, please contact:  
\* `secure@microsoft.com`  
Comment:  
Comment: For legal and law enforcement-related requests, please contact:  
\* `mandoc@microsoft.com`  
Comment:  
Comment: For routing, peering or DNS issues, please  
contact:  
\* `IOC@microsoft.com`  
Comment:  
Ref: `https://rdap.arin.net/registry/entity/MSFT`

OrgAbuseHandle: `MAC74-ARIN`  
OrgAbuseName: Microsoft Abuse Contact  
OrgAbusePhone: +1-425-882-8080  
OrgAbuseEmail: `abuse@microsoft.com`  
OrgAbuseRef: `https://rdap.arin.net/registry/entity/MAC74-ARIN`

OrgRoutingHandle: `CHATU3-ARIN`  
OrgRoutingName: Chatumtohta, Somesh  
OrgRoutingPhone: +1-425-882-8080  
OrgRoutingEmail: `somesh@microsoft.com`  
OrgRoutingRef: `https://rdap.arin.net/registry/entity/CHATU3-ARIN`

OrgTechHandle: `NRPD-ARIN`  
OrgTechName: Microsoft Routing, Peering, and DNS  
OrgTechPhone: +1-425-882-8080

### 4. Servicios Expuestos (Shodan)

No se pudo realizar consulta directa de Shodan sin cuenta. Sin embargo, se observa que la infraestructura principal está en Azure (AS8075) y Microsoft; esto sugiere que los servicios web (https, ssh, correo) podrían estar gestionados por Microsoft u otros proveedores de nube [WhoisFreaks+7Gridinsoft LLC+7IPinfo+7Domain Glass](#).

**Observaciones adicionales:**

- El dominio usa Azure-hosted IPs ubicadas en EE. UU.
- Posible exposición de puertos comunes HTTPS (443), SSH (22), SMTP (25 o 587) según configuración interna.
- Falta de datos CVE confirmados por ausencia de escaneo activo.

192.100.164.93

Resultados de la búsqueda de

Free online network tools - tra

Universidad Autónoma de Yuc

DNSDumpster - Find & lookup

dnsdumpster.com


http://astromenda.c... https://mx.search.ya... Presupuesto materi... ¡Bienvenido a Faceb... FORMATOS Y MOD... Electricidad Precios... videos tutoriales de... Ver Peliculas Online... Todos los favoritos

>> Free users are limited to 50 results for a single domain. Get 12 months [Plus Access](#) - on Sale Now.

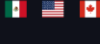
System Locations


Hosting / Networks

Services / Banners



UNIVERSIDAD AUTO  
MICROSOFT-COMP-R  
AZHOSTING  
CLOUDFLARENET





Apache	8
cloudflare	4
LiteSpeed	4
20- Welcome to Pure-FTPd privsep TLS - 20-You are user number 1 of 80 allowed. 20- Local time is now 0	2
Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.3.12	1

A Records (subdomains from dataset)

Host	IP	ASN	ASN Name	Open Services (from DB)	RevIP
catalogo.bibliotecas.uady.mx	148.209.1.31	ASN: 22122	UNIVERSIDAD AUTONOMA DE YUCATAN, MX		1
catalogo.bibliotecas.uady.mx	148.209.0.0/16		Mexico		
www.sii.cgdf.uady.mx	148.209.1.241	ASN: 22122	UNIVERSIDAD AUTONOMA DE YUCATAN, MX	https: Apache/2.4.43 (Win64) OpenSSL/1.1.1g	1

Titular de finanzas  
Gobierno de Tru...

Buscar

ESP  
ES

10:51 p.m.  
26/07/2025

192.100.164.93

Resultados de la búsqueda de

Free online network tools - tra

Universidad Autónoma de Yuc

DNSDumpster - Find & lookup

dnsdumpster.com

http://astromenda.c... https://mx.search.ya... Presupuesto materi... ¡Bienvenido a Faceb... FORMATOS Y MOD... Electricidad Precios... videos tutoriales de... Ver Peliculas Online... Todos los favoritos

number 1 of 80 allowed. 20-  
Local time is now 0Apache/2.4.43 (Win64)  
OpenSSL/1.1.1g PHP/7.3.12

A Records (subdomains from dataset)

Host	IP	ASN	ASN Name	Open Services (from DB)	RevIP
catalogo.bibliotecas.uady.mx	148.209.1.31	ASN: 22122	UNIVERSIDAD AUTONOMA DE YUCATAN, MX		1
catalogo.bibliotecas.uady.mx	148.209.0.0/16		Mexico		
www.sii.cgdf.uady.mx	148.209.1.241	ASN: 22122	UNIVERSIDAD AUTONOMA DE YUCATAN, MX	https: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.3.12 title: Sistema Institucional de Informaci on: www.sii.cgdf.uady.mx tech: Apache HTTP Server:2.4.43 OpenSSL:1.1.1g PHP:7.3.12 Windows Server	1
citrix.uady.mx	148.209.1.25	ASN: 22122	UNIVERSIDAD AUTONOMA DE YUCATAN, MX	https: unknown server title: NetScaler Gateway on: .uady.mx tech: Apache HTTP Server	1
aulavirtual.educacion.uady.mx	148.209.1.114	ASN: 22122	UNIVERSIDAD AUTONOMA DE YUCATAN, MX	https: Apache title: Redireccionar on: aulavirtual.educacion.uady.mx tech: Moodle PHP	1

Trending videos  
HBO publica pri...

Buscar

ESP  
ES

10:52 p.m.  
26/07/2025



## 6. Recomendaciones de Hardening Inicial

1. **Implementar y publicar registros SPF, DKIM y DMARC** para proteger autenticación de correo.
2. **Revisar configuración de name servers** para limitar exposición pública.
3. **Sanear metadatos de documentos públicos** descargables desde sitios como *redi.uady.mx*.
4. **Aplicar reglas de firewall o WAF** para filtrar tráfico indebido desde IPs en Azure o rangos 148.209.0.0/16.
5. **Habilitar monitoreo de tráfico y alertas**, especialmente en servicios críticos (correo, SSH, web).
6. **Auditar subdominios expuestos** para evitar configuraciones innecesarias o misconfiguraciones.

## 7. Conclusión

La Universidad Autónoma de Yucatán mantiene un dominio con jerarquía clara y antiguo (desde 1995) con infraestructura distribuida principalmente en Azure, lo cual es común para entornos educativos modernos. La exposición de múltiples subdominios y el uso de servicios en nube indican buena adopción tecnológica, pero también implican posibles vectores de exposición. Falta información detallada sobre servicios, versiones y metadatos de documentos, por lo que se recomienda ejecutar auditorías activas controladas y revisar configuraciones internas, especialmente en correos, DNS y documentos públicos.