

Octubre 2025

Investigación a través de herramientas OSINT

(Inteligencia de Fuentes Abiertas)



PRESENTADO POR EQUIPO SQUIRTLE





Índice

- 1. Resumen ejecutivo**
- 2. Introducción y alcance**
- 3. Metodología y herramientas utilizadas**
- 4. Perfiles de la organización y huella del personal**
- 5. Infraestructura y terceros críticos (dominios, IPs, proveedores)**
- 6. Perfilado técnico resumido (DNS, correo, certificados, web)**
- 7. Contenido público y endpoints visibles (robots.txt, sitemap, PDFs)**
- 8. Exposición en índices y servicios detectados .**
- 9. Correlación y visualizaciones (Maltego / SpiderFoot)**
- 10. Hallazgos principales y priorización de riesgos.**
- 11. Recomendaciones prioritarias y roadmap resumido**
- 12. Anexos esenciales y glosario ejecutivo**



INTRODUCCIÓN

Objetivo del trabajo

El objetivo de este trabajo es identificar, desde una perspectiva externa, qué tipo de datos podrían ser aprovechados por actores malintencionados para comprometer la seguridad digital de la empresa. Todo el análisis se basa en información accesible sin necesidad de permisos especiales ni técnicas **invasivas/activas**.

El propósito final de esta investigación es contribuir al fortalecimiento de la seguridad de la empresa, ofreciendo una visión objetiva que permita detectar posibles áreas de mejora y anticiparse a riesgos que podrían ser explotados por **ciberdelincuentes**.

Metodología

La metodología utilizada en esta investigación se basa en diversas técnicas de **OSINT (Inteligencia de Fuentes Abiertas)**, las cuales consisten en recopilar y analizar información pública disponible en internet, sin necesidad de acceder directamente a los sistemas internos de la empresa. Para ello, se utilizaron diferentes herramientas especializadas que permiten identificar datos expuestos los cuales podrían representar un riesgo. Entre ellas se encuentran buscadores técnicos como **Shodan** y **Censys**; servicios que muestran registros públicos de dominios y certificados digitales (***DNS/CT**); herramientas para revisar detalles visibles de páginas web, como encabezados, archivos de navegación (robots.txt, sitemap.xml) y metadatos; así como **Subfinder**, que permite detectar subdominios relacionados con la organización. También se analizaron redes sociales y se emplearon plataformas como **FOCA, Hunter, Maltego** y **SpiderFoot**, que ayudan a visualizar conexiones entre datos públicos. Todo el proceso se realizó sin modificar ni intervenir en los sistemas, limitándose únicamente a observar lo que ya está expuesto en línea.



Alcance

Se ha realizado una investigación OSINT centrada en el perfil tecnológico de la empresa Slclab, dedicada al desarrollo de soluciones LIMS (Laboratory Information Management System) para laboratorios clínicos.

El objetivo fue identificar los activos tecnológicos visibles públicamente, analizar su infraestructura web y evaluar posibles riesgos asociados a su exposición digital.

La investigación se ha llevado a cabo siguiendo una metodología OSINT estándar, combinando técnicas de reconocimiento pasivo y análisis de huella digital.

Estructura Asociada

Servidores Principales y Aplicaciones

Dominio/Host	Dirección IP	Proveedor/Hosting	Servicios Destacados
slclab.com	93.189.91.160	CLOUDING, ES (ASN 49635)	HTTP/S (IIS 10), FTP (Microsoft FTP Service)
zendolims.com	46.183.114.177	CLOUDING, ES (ASN 49635)	FTP, HTTP, HTTPS
clouding.zendolims.com	185.253.153.148	CLOUDING, ES (ASN 49635)	FTP, HTTP, HTTPS
interno.slclab.com	80.24.200.197	TELEFONICA_DE_ESPAÑA (ASN 3352)	HTTP/HTTPS: Microsoft-IIS/10.0

Servicios de correo y DNS

Host/Servicio	Dirección IP	Proveedor/Ubicación
slclab-com.mail.protection.outlook.com	52.101.73.30	Microsoft (Correo Electrónico)
shades07.rzone.de	185.132.34.134	IONOS-AS (ASN 8560)
docks09.rzone.de	217.160.80.136	IONOS-AS (ASN 8560)
smtp.rzone.de	81.169.145.98	STRATO AG (ASN 6724)
ns1.dondominio.com	87.117.96.2	SCIP-AS (ASN 57910)
ns2.dondominio.com	87.117.96.3	SCIP-AS (ASN 57910)



Perfiles de la organización

SLCLAB Informática desarrolla, comercializa y da soporte a software de gestión de laboratorios. Su producto principal es Zendo LIMS; también comercializa Alfa21(para laboratorios de análisis de agua) y Alfa21 VET (para laboratorios veterinarios) Fundada en 2007. Empiezan instalando su software en laboratorios por toda España . En 2010 empiezan a expandirse internacionalmente incluyendo laboratorios de latinoamérica.

Razón Social: SLCLAB Informática S.L.

Fecha de creación: 03/05/2007

Cif: B 37460938

C. de Velázquez nº6 1ºC 37005 Salamanca, España

Teléfono contacto: (+34) 923 720 700, **tel:**(+34) 923 600 282

Correo contacto: info@zendolims.com / informatica@slclab.com

Web: <http://www.zendolims.com> | SLCLAB INFORMATICA | Software de Gestión para Laboratorios | LIMS en la nube



Calle de Velázquez nº6 1ºC 37005 Salamanca, España



Sectores: Veterinario Patología Clínico Salud Pública Químico Hospitales Agua Alimentación Medioambiente Manufactura Forense Petroquímico Toxicología Molecular Ciencias Biológicas Enología Minería y Construcción

Clientes por todo el mundo especialmente Europa y Latinoamérica



Tamaño de la empresa: 11 empleados

El Equipo Zendo



JOSÉ NAVAO
Zendo team



JULIO RODRÍGUEZ
Zendo team



PEDRO MARCOS
Zendo team



SANTOS GÓMEZ
Zendo team



JUAN CARLOS VEGAS
Zendo team



ÁNGEL DELGADO
Zendo team



SUSANA MARTÍN
Zendo team



SARA MARTÍN
Zendo team



DIEGO GONZÁLEZ HERNÁNDEZ
Zendo team



JORGE MARTÍN RODRÍGUEZ
Zendo team

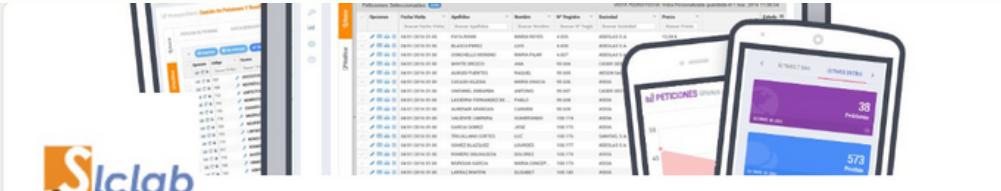


ADRIÁN CLAVERO CORTÉS
Zendo team



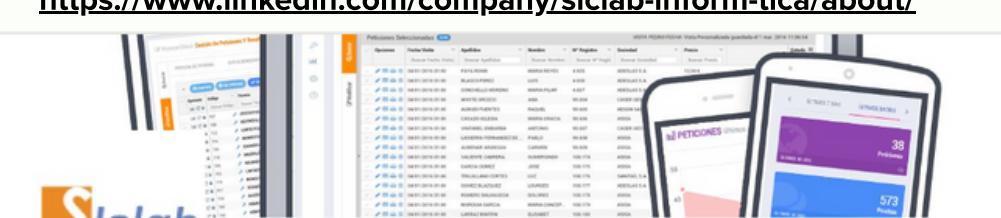
Perfiles sociales Slclab

En cuanto a las redes sociales oficiales de la organización, cuenta con un LinkedIn general para **SLCLAB**, y otro específico para **Zendo Lims**, el cual también cuenta con su propia cuenta de Instagram, un blog y un canal de YouTube, y otro canal de YouTube para su otro producto, Alfa21. La empresa también deja visible parte de su personal en plataformas profesionales.



SLCLAB
Software de gestión para laboratorios: Zendo LIMS / Alfa21 LIMS
Desarrollo de software · SALAMANCA, Salamanca · 2 mil seguidores · 11-50 empleados

<https://www.linkedin.com/company/slclab-inform-tica/about/>



ZENDO LIMS
Sistemas de gestión de información de laboratorios (LIMS) de SLCLAB
 Utilizado por Saica Group y 20 clientes destacados

<https://www.linkedin.com/company/slclab-inform-tica/about/>



zendolims ·
Zendo Lims
31 publicaciones · 213 seguidores · 697 seguidos
Producto/servicio
El Software para Laboratorios que se adapta a tus necesidades
📍 Salamanca
... más

<https://www.linkedin.com/company/slclab-inform-tica/about/>



Zendo LIMS

@ZendoLIMS · 2 suscriptores · 1 vídeo

ZENDO LIMS | Software de Gestión para Laboratorios en la Nube ...más
zendolims.com y 1 enlace más

[Suscribirme](#)

<https://www.linkedin.com/company/slclab-inform-tica/about/>



Inicio Empresa Zendolims Alfa21 Clientes Distribuidores Soporte Contacto



CARACTERÍSTICAS SECTORES PRECIOS SOPORTE CONTACTO [Solicitar Demo](#)

Blog de Lims

Buscar



La importancia de una buena planificación en la implantación de un LIMS

Por Pedro Marcos Montero / General / Redactado el 05/08/2025

<https://www.linkedin.com/company/slclab-inform-tica/about/>

ALFA21 - Software de Gestión para el Laboratorio

@AprendiendoALFA21 · 70 suscriptores · 79 vídeos

Principales funcionalidades de Alfa21 - Software de gestión para el laboratorio. ...más
slclab.com y 1 enlace más

[Suscribirme](#)

<https://www.linkedin.com/company/slclab-inform-tica/about/>



Infraestructura digital y terceros críticos

La organización **SLCLAB** mantiene una infraestructura técnica distribuida entre varios proveedores externos que cumplen funciones clave en la operación de sus servicios digitales.

Sitios web oficiales:

- El dominio principal www.slclab.com está vinculado a la dirección IP **93.189.91.160**, alojada por el proveedor **Clouding**, con sede en España (ASN 49635).
- El dominio zendolims.com, correspondiente a uno de sus productos, también está alojado por **Clouding**, en la IP **185.253.153.148** (ASN 49635).
- Ambos sitios están gestionados por el mismo proveedor de hosting, lo que sugiere una centralización de la infraestructura web.

Correo electrónico corporativo:

- El sistema de correo utiliza servicios de protección y filtrado proporcionados por **Microsoft Outlook**, bajo el dominio técnico **slclab-com.mail.protection.outlook.com**. Esto indica que la empresa confía en soluciones empresariales ampliamente adoptadas para la gestión segura del correo.

Proveedor de hosting:

- Clouding (La evaluación externa de la influencia de las redes sociales mediante el uso de herramientas analíticas dará como resultado datos tangibles.) es el proveedor responsable del alojamiento web. Se trata de una empresa española especializada en servidores en la nube, lo que permite a SLCLAB escalar sus servicios de forma flexible.

Esta información permite identificar a los terceros críticos que sustentan la infraestructura digital de la organización. Su análisis es relevante para evaluar posibles dependencias técnicas, riesgos asociados a proveedores externos y oportunidades de mejora en la seguridad o resiliencia operativa.



Durante el proceso de investigación OSINT se identificaron diversos elementos públicos como documentación institucional y comercial.

A través de realizar una búsqueda en la herramienta **WhatsMyName** con el correo **diego.gonzalez@slclab.com** se localizaron documentos públicos vinculados a la empresa, incluyendo registros mercantiles y menciones en el **BORME** relacionadas con cambios de domicilio social en Salamanca en el año 2010. También se encontraron inscripciones telemáticas en el **Ayuntamiento de Salamanca**.

[HTTPS://WWW.BOE.ES/BORME/DIAS/2010/02/09/PDFS/BORME-A-2010-26-37.PDF](https://www.boe.es/BORME/DIAS/2010/02/09/PDFS/BORME-A-2010-26-37.PDF)

BOE	BOLETÍN OFICIAL DEL ESTADO	BOLETA OFICIAL DEL ESTADO
Núm. 210	Miércoles 2 de septiembre de 2015	Supl. N. Pág. 1
Suplemento de Notificaciones ADMINISTRACIÓN LOCAL SALAMANCA AYUNTAMIENTO DE SALAMANCA		
<i>ORGANISMO AUTÓNOMO DE GESTIÓN ECONÓMICA Y RECAUDACIÓN. Anuncio de notificación de 27 de agosto de 2015 en procedimiento Edicto de notificación.</i>		
ID: N1500122468		
Departamento: ORGANISMO AUTÓNOMO DE GESTIÓN ECONÓMICA Y RECAUDACIÓN.		
Procedimiento: NOTIFICACIÓN DE INCLUSIÓN OBLIGATORIA EN EL SISTEMA DE COMUNICACIONES TRIBUTARIAS TELEMÁTICAS MUNICIPALES		
Motivo: NOTIFICACIÓN A AUSENTES O DESCONOCIDOS		
Lugar y plazo para la comparecencia: Lugar:		
O.A.G.E.R. Calle Espoz y Mina, 16-18, Planta Baja		
Centro Municipal Integrado "Julién Sánchez El Charro". Plaza de la Concordia, s/n		

B37430279	Sitrans Salamanca Sl
B86770633	Skremm Licenses S
B37460938	Siclab Informatica Sl
B37526084	Smart Technology Brands Sl
B37437076	Soares & Vera Sl

1748622114944b16550



Además, se accedió a material comercial alojado en plataformas abiertas, como una presentación completa del sistema **Zendo LIMS** publicada en **Scribd**.

Esta presentación describe las principales funcionalidades del producto, lo que permite entender su enfoque y aplicación sin necesidad de acceder a documentación interna.

Como complemento a las búsquedas OSINT realizadas en plataformas como **WhatsMyName**, se aplicaron técnicas de filtrado en motores de búsqueda utilizando **Google Dorks**, una metodología que permite localizar archivos específicos publicados en dominios concretos.

En este caso, se utilizó el dork **site:slclab.com filetype:pdf**, con el objetivo de identificar documentos PDF alojados directamente en el sitio web oficial de la empresa. Esta búsqueda permitió localizar material técnico vinculado al software **Alfa21**, incluyendo instrucciones sobre el proceso de registro web.

Este hallazgo se suma a la documentación previamente identificada sobre **Zendo LIMS**, reforzando la idea de que **SLCLAB** mantiene parte de sus recursos técnicos y comerciales accesibles públicamente.

Para una investigación **OSINT**, este tipo de contenido resulta valioso tanto para entender el alcance funcional de sus productos como para evaluar el nivel de exposición informativa de la organización.

[HTTPS://WWW.SLCLAB.COM/REDCANARIALABORATORIOS/ALFA21/INSTRUCCIONESALFA21NET.PDF](https://WWW.SLCLAB.COM/REDCANARIALABORATORIOS/ALFA21/INSTRUCCIONESALFA21NET.PDF)

[HTTPS://WWW.SLCLAB.COM/LABTOVAR/EXPORTAR/INSTRUCCIONES.PDF](https://WWW.SLCLAB.COM/LABTOVAR/EXPORTAR/INSTRUCCIONES.PDF)

[HTTPS://LRDIAGNOSTICO.COM/WP-CONTENT/UPLOADS/2024/03/FOLLETO-ZENDO-LIMS.PDF](https://LRDIAGNOSTICO.COM/WP-CONTENT/UPLOADS/2024/03/FOLLETO-ZENDO-LIMS.PDF)



También a través de una búsqueda en la herramienta **RocketReach** con el correo **jnavajo@slclab.com** para consultar el perfil público de **José Navajo Gallego**, identificado como **CEO de SLCLAB Informática S.L.** se obtuvo un listado de personas vinculadas a la empresa, junto con lo que parecen ser correos electrónicos corporativos.

Al analizar esta información, se identificó un patrón consistente en la estructura de los correos: **nombre.apellido@slclab.com**. Este tipo de formato, aunque común en entornos empresariales, puede facilitar intentos de contacto no deseado o incluso ataques de suplantación de identidad (**phishing**), especialmente si los nombres del personal son visibles en plataformas públicas.

Desde una perspectiva de seguridad, este patrón predecible —combinado con la exposición de nombres y cargos en redes profesionales— puede considerarse una **vulnerabilidad menor**, ya que reduce el esfuerzo necesario para generar direcciones válidas y dirigir correos maliciosos. Aunque no representa una brecha crítica, sí es recomendable que la organización evalúe medidas de protección complementarias, como filtros avanzados de correo, autenticación reforzada y políticas de visibilidad digital para su personal.

 Jose Navajo Gallego CEO In	SLCLAB Informática Salamanca, CL, ES	 jnavajo@slclab.com  Your plan doesn't currently include phone information. Learn More
 Pedro Marcos Montero Sales Manager In	SLCLAB Informática Málaga, AL, ES	 pedro.marcos@slclab.com  Your plan doesn't currently include phone information. Learn More
 Juan Carlos V. Programador informático In	SLCLAB Informática	 v@slclab.com   Your plan doesn't currently include phone information. Learn More
 Santos Gómez Sánchez Technical Support Manager In	SLCLAB Informática Salamanca, CL, ES	 santos.gomez@slclab.com  Your plan doesn't currently include phone information. Learn More
 Jose Alberto Hernandez Fraile Analista programador In	SLCLAB Informática Salamanca, CL, ES	 jose.fraile@slclab.com   Your plan doesn't currently include phone information. Learn More No credit used.
 Diego Gonzalez Hernandez Software Developer In	SLCLAB Salamanca, CL, ES	 diego.gonzalez@slclab.com   Your plan doesn't currently include phone information. Learn More
 Sara Martin Ruano Desarrolladora - Soporte IT In	SLCLAB Salamanca, CL, ES	 @slclab.com
 Jorge Martin Rodriguez Especialista en soporte técnico y consultoría de software In	SLCLAB Salamanca, Castille and León, Spain	 jorge.martin@slclab.com   Your plan doesn't currently include phone information. Learn More



Mapa de empleados y huella digital.



José Navajo Gallego (CEO)
jnavajo@slclab.com

Se encuentra un perfil en LinkedIn y un perfil privado en Facebook. Se le menciona también en un documento del Boletín Oficial del Registro Mercantil donde trabajó anteriormente pero nada de significado.



Pedro Marcos Montero (Manager de ventas)
pedro.marcos@slclab.com

De Pedro si aparece su correo en tres data breaches y una posible contraseña del mismo en [dehashed.com](https://www.dehashed.com) : **ZS+JFb/DqZ5m*******

Al tener un perfil mas público se le pueden encontrar entradas de blogs y apariciones en entrevistas de radio local, así como está activo en LinkedIn publicando regularmente.



Diego González Hernández (Software Developer)
diego.gonzales@slclab.com

Encargado del desarrollo del software de la empresa, no se encuentra mucha información de esta persona a parte del perfil de LinkedIn donde define las tecnologías que utiliza como Java, C#y HTML5.



Resto de empleados

Juan Carlos V.

Puesto: Software Developer

- No se ha identificado correo corporativo.
- Cuenta pública en LinkedIn.
- No se han encontrado otras redes sociales asociadas.

Santos Gómez Sánchez

Puesto: Technical Support Manager

- Correo corporativo: santos.gomez@slclab.com
- Perfil público en LinkedIn.

Sara Martín Ruano

Puesto: Desarrolladora - Soporte IT

- Correo corporativo: sara.martin@slclab.com
- Solo se ha identificado perfil en LinkedIn.
- No se han encontrado otras redes sociales personales.

Susana Martín Castaño

Puesto: Relaciones Internacionales

- No se ha identificado correo corporativo.
- No se han encontrado perfiles en redes sociales.

Jorge Martín Rodríguez

Puesto: Especialista en Soporte Técnico

- Correo corporativo: jorge.martin@slclab.com
- Presencia en redes sociales personales (Instagram, YouTube) bajo el alias “jota.drones”.
- No publica contenido relacionado con la empresa.

Julio Rodríguez Estévez

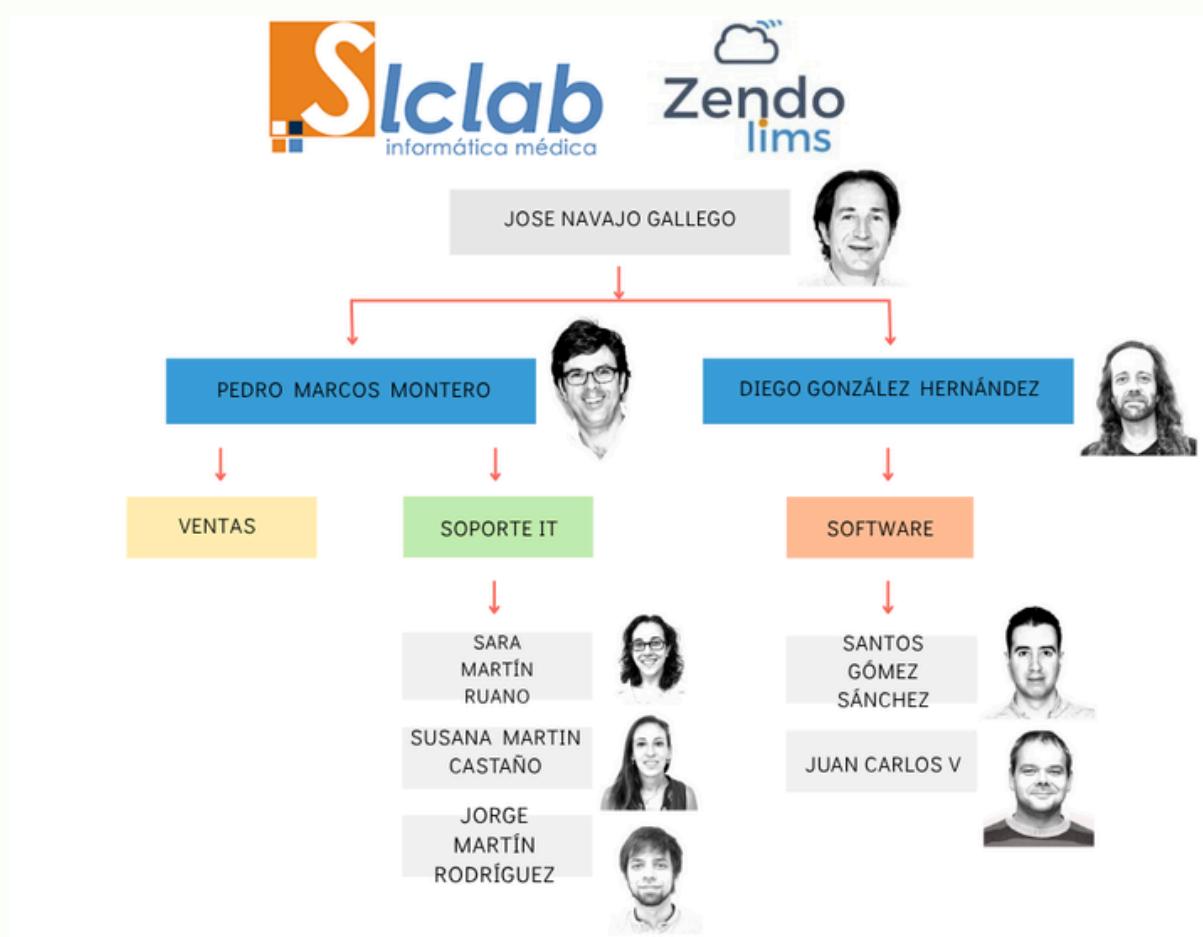
Puesto: Programador

- Solo se ha identificado perfil en LinkedIn.
- No se han encontrado otras redes sociales personales.

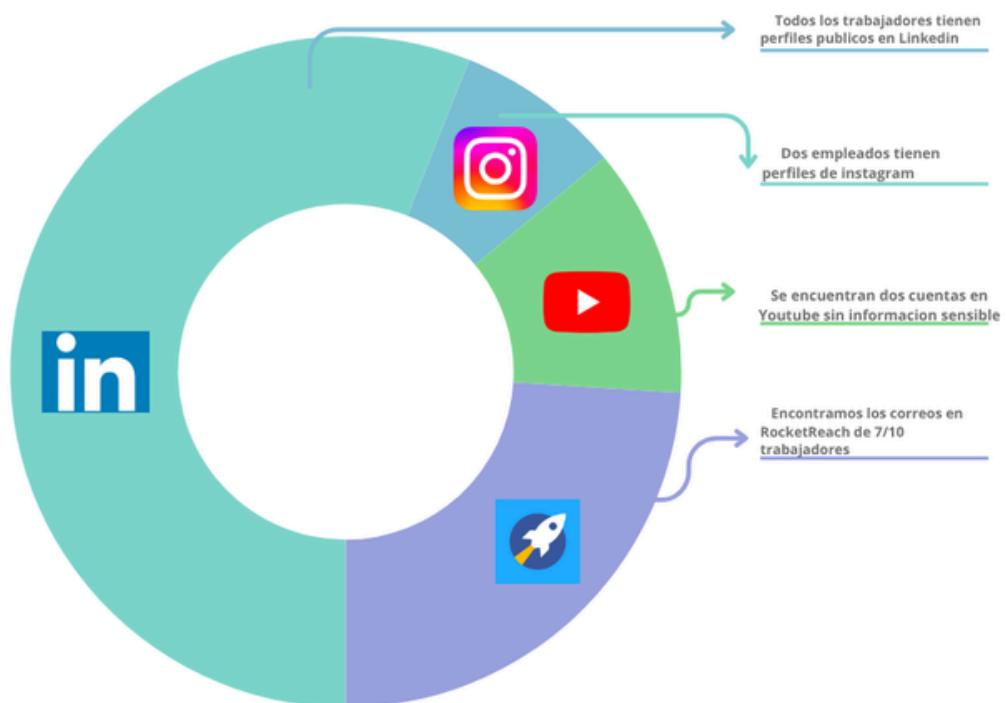
Adrián Clavero Cortés

Puesto: Programador

- Se han encontrado cuentas privadas en Facebook e Instagram.
- No se ha identificado correo corporativo



Presencia en redes sociales





PERFILADO TÉCNICO

Dominios, DNS y correo

Dominio principal slclab.com; sitio y marca de producto zendolims.com también presentes. El correo se gestiona con **Microsoft 365**. El **DNS** está alojado en **DonDominio**. Información obtenida con dnsdumpster.com



SPF está bien configurado y estricto (**-all**), lo que ayuda a evitar correos falsos. **DMARC** aplica rechazo total (**p=reject**), que bloquea suplantaciones. **DKIM** aparece activo, aunque con clave de **1024 bits** en observaciones previas del equipo; hoy se recomienda 2048 bits. Esta información se obtuvo con **nslookup**, la cual es una herramienta que sirve para consultar registros **DNS** (Domain Name System).

```
PS C:\Users\vmelo> nslookup -type=txt _dmarc.slclab.com 8.8.8.8
Servidor: dns.google
Address: 8.8.8.8

Respuesta no autoritativa:
_dmarc.slclab.com      text =
                            "v=DMARC1; p=reject; pct=100"
```

Significado: reduce el riesgo de correos falsos desde “@slclab.com”.

Web principal y cabeceras

La web usa **Microsoft IIS** y **ASP.NET**; el certificado del sitio principal es válido. En análisis de cabeceras **no aparecen algunas cabeceras de seguridad habituales**, como **HSTS** o **CSP**.

¿Por qué importa? la tecnología es correcta, pero añadir cabeceras **ayuda a reducir riesgos** comunes de web (por ejemplo, **clickjacking** o ciertos **XSS**).



RESULTS: 23 • DURATION: 0.61s

www.slclab.com: 443 • WEB PROPERTY

AS OF 22 OCT 2025 | 14:52 UTC

HTML Title	SLCLAB INFORMATICA Software de Gestión para Laboratorios LIMS en la nube	1 Endpoint
Browser Trust	Trusted	443 / HTTP
Software	Microsoft Asp.Net Microsoft Internet Information Services	
MATCHED FIELDS		
web.cert.names	slclab.com	
web.cert.parsed.subject.common_name	www.slclab.com	
web.cert.parsed.subject_dn	CN=www.slclab.com	
web.endpoints.hostname	www.slclab.com	
web.endpoints.http.favicons.name	tp://www.slclab.com/favicon.i	
web.endpoints.http.html_tags	tp://www.slclab.com/img/slclab	
web.endpoints.http.url	tp://www.slclab.com/	
web.hostname	www.slclab.com	

Subdominios y certificados

Se revisaron los subdominios y los certificados TLS asociados a los dominios [slclab.com](https://www.slclab.com) y zendolims.com mediante fuentes abiertas (navegador, catálogos de certificados y visores de huella web). El objetivo fue identificar qué nombres están publicados, qué certificados atienden a cada nombre y si esos certificados son reconocidos por los navegadores.

slclab.com y subdominio

- www.slclab.com

Dominio público que sirve la web corporativa. Responde con servidor **Microsoft IIS** y aplicación **ASP.NET**. El sitio presenta un certificado válido reconocido por los navegadores.

VISOR DE CERTIFICADOS: WWW.SLCLAB.COM

General Detalles

Enviado a

Nombre común (CN)	www.slclab.com
Organización (O)	<No es parte del certificado>
Unidad organizativa (OU)	<No es parte del certificado>

Emitido por

Nombre común (CN)	Sectigo RSA Domain Validation Secure Server CA
Organización (O)	Sectigo Limited
Unidad organizativa (OU)	<No es parte del certificado>

Período de validez

Emitido el	martes, 10 de diciembre de 2024, 1:00:00
Vencimiento el	sábado, 10 de enero de 2026, 05:59:59

Huellas digitales SHA-256

Certificado	2c319c4bc368de0b3882f7e25c956db5cebfbedfc254f77838689ef86279d295
Clave pública	2e35cd560221e45c2b718dcfc5bc1d6b51084714701b2835f99c58c2a8611959

VISOR DE CERTIFICADOS: WWW.SLCLAB.COM

General Detalles

Jerarquía de certificado

- ▼ USERTrust RSA Certification Authority
- = Sectigo RSA Domain Validation Secure Server CA
- www.slclab.com

Campos del certificado

- Restricciones básicas del certificado
- Uso extendido de la clave
- Políticas del certificado
- Acceso a información de autoridades
- Nombre alternativo de la entidad receptora del certificado**

Lista de marcas de tiempo de certificados firmados

Algoritmo de firma de certificado

Valor de campo

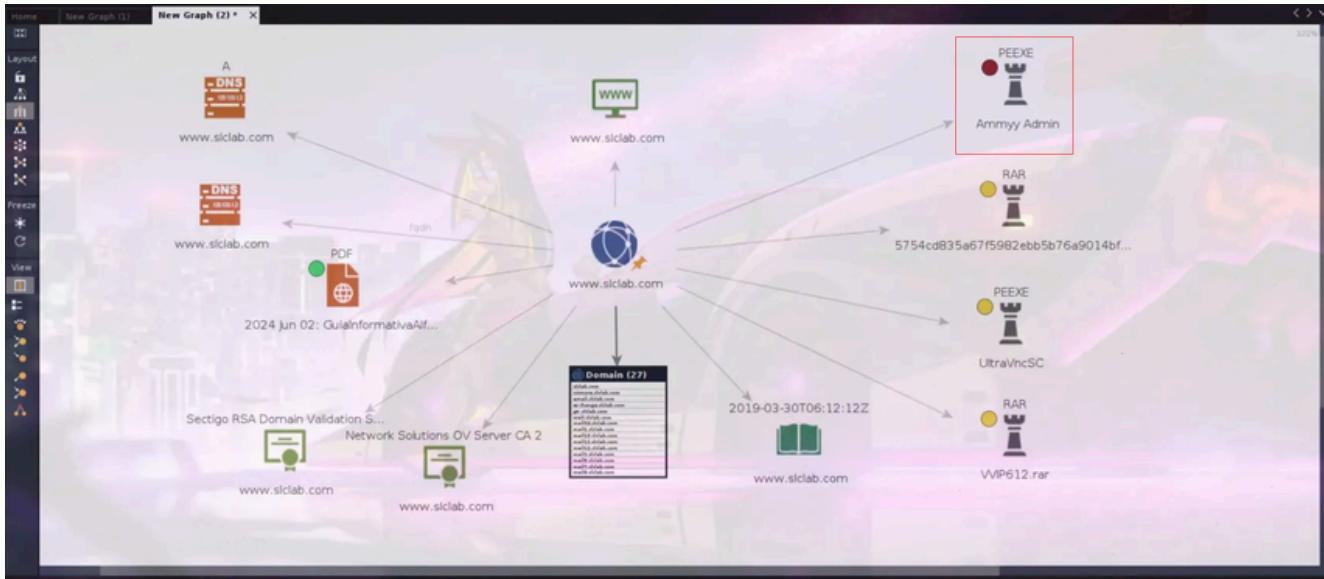
No critica
Nombre DNS: www.slclab.com
Nombre DNS: slclab.com

Exportar...



Se ha utilizado la herramienta **Maltego** para ver que tipo de información esconde dicha empresa.

Esta da varios registros **DNS**. Entre ellos se encuentra el **Registro A (IPv4): 93.189.91.160** y otros ítem de interés (en la imagen se filtraron ya los interesantes)



Investigando un poco más dentro de **Maltego**, aparece una **vulnerabilidad importante** bajo el nombre “**PEEXE Ammy Admin**”

¿Que es **PEEXE Ammy Admin** y porque es un **fallo crítico**?

Ammy Admin es una herramienta legal de **Escritorio Remoto** similar a TeamViewer. Su función es **crítica**: permite que un usuario tome control completo del ordenador de otro.

Algunas versiones de **Ammy Admin** se pueden usar como un "**dropper**" (archivo pequeño con la única función de instalar y ejecutar el malware) o un "**backdoor**" (puerta trasera secreta que permite al atacante saltarse los métodos de autenticación normales). Es decir, instalan **Ammy Admin** para mantener el acceso al sistema comprometido.

Sabiendo todo ésto, se introduce el ítem reportado en **Maltego** y con una de las claves Hash que contiene este registro (por ejemplo la de SHA-256) en la plataforma **VirusTotal** y, efectivamente, se detecta que tiene una **red flag** señalando que es un **fallo crítico de seguridad**.

The screenshot shows the VirusTotal analysis results for the file **c63e76a46e3a0089d7f8bdc28eca540e1609f07e42fa867d632972c213e090db**, identified as **Ammy Admin**. The analysis includes:

- Community Score: 53 / 75
- 53/75 security vendors flagged this file as malicious
- File Type: EXE
- Size: 732.00 KB
- Last Analysis Date: 1 year ago
- Tags: peexe, checks-user-input, detect-debug-environment, long-sleeps, checks-disk-space

Una puntuación de **53 sobre 75** es **extremadamente alto**. No es un falso positivo. Significa que la comunidad de expertos en la ciberseguridad han llegado a un consenso.



- www.interno.slclab.com

Subdominio publicado con denominación que sugiere un uso privado interno. Al acceder, responde una página por defecto de **IIS** (página de bienvenida estándar del servidor web), y el servicio presenta un certificado auto firmado (no emitido por una autoridad certificadora). El certificado consta como vigente dentro de la ventana observada (24-09-2025 al 26-03-2026), pero **no es de confianza para el navegador por su naturaleza autofirmada.**

interno.slclab.com • CERTIFICATE

AS OF 25 SEPT 2025 | 11:40 UTC

never-trusted self-signed unexpired untrusted

Issuer: CN=interno.slclab.com

Validity Period: 24 SEPT 2025 — 28 MAR 2026

Browser Trust: Untrusted

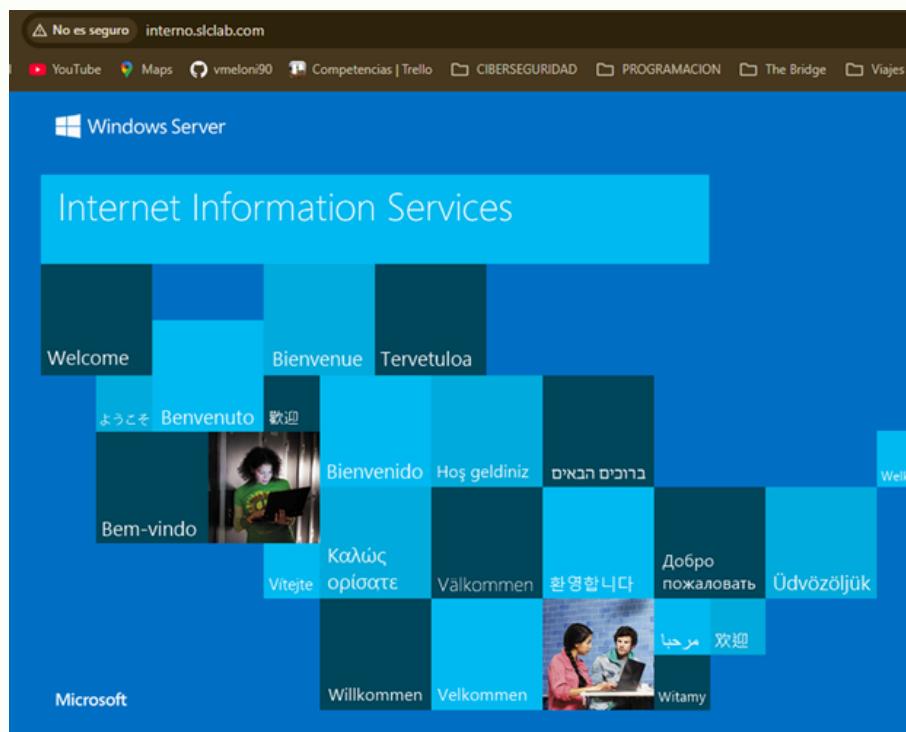
All Names: interno.slclab.com

Matched Fields:

cert.fingerprint_sha256	9ed1402d5cccd49cddb66
cert.names	interno.slclab.com
cert.parsed.issuer_dn	N=interno.slclab.com
cert.parsed.subject_dn	N=interno.slclab.com

Notas de lectura para slclab.com

- En www.slclab.com el certificado abarca los nombres esperados (dominio raíz y “www”), lo que **permite la conexión HTTPS sin advertencias**.
- En interno.slclab.com el servidor contesta con la página genérica de **IIS**, y el certificado observado **no está emitido por una autoridad**, por lo que el navegador lo marca como no confiable aunque esté dentro de su periodo de validez.





SIclab.com - emisores y nombres cubiertos

En el histórico de certificados de la web principal se observan **cambios de entidad emisora a lo largo del tiempo** (por ejemplo, diferentes Autoridades de Certificación en períodos distintos). Este patrón refleja rotaciones o migraciones habituales. Los *Subject Alternative Names (SANs)* de los certificados de la web principal incluyen el dominio raíz y “www”, que son los nombres esperados para el sitio corporativo.

Información extraída de crt.sh:

crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
15694689048	2024-12-10	2024-12-10	2026-01-09	www.slclab.com	slclab.com www.slclab.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
15694689044	2024-12-10	2024-12-10	2026-01-09	www.slclab.com	slclab.com www.slclab.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
11117802700	2023-11-16	2023-11-16	2024-12-15	www.slclab.com	slclab.com www.slclab.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
11117802980	2023-11-16	2023-11-16	2024-12-15	www.slclab.com	slclab.com www.slclab.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
7871347850	2022-10-31	2022-10-31	2023-11-30	www.slclab.com	slclab.com www.slclab.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
7871331850	2022-10-31	2022-10-31	2023-11-30	www.slclab.com	slclab.com www.slclab.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
5342874881	2021-10-04	2021-10-04	2022-11-03	www.slclab.com	slclab.com www.slclab.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
5342496216	2021-10-04	2021-10-04	2022-11-03	www.slclab.com	slclab.com www.slclab.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
3501677192	2020-10-13	2020-10-13	2021-10-13	www.slclab.com	slclab.com www.slclab.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
3501677175	2020-10-13	2020-10-13	2021-10-13	www.slclab.com	slclab.com www.slclab.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
881270870	2018-10-22	2018-10-22	2020-10-15	www.slclab.com	slclab.com www.slclab.com	C=US, ST=VA, L=Herndon, O=Network Solutions L.L.C., CN=Network Solutions OV Server CA 2
881220006	2018-10-22	2018-10-22	2020-10-15	www.slclab.com	slclab.com www.slclab.com	C=US, ST=VA, L=Herndon, O=Network Solutions L.L.C., CN=Network Solutions OV Server CA 2
869707985	2018-10-17	2018-10-17	2019-01-15	www.slclab.com	www.slclab.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
869791586	2018-10-17	2018-10-17	2019-01-15	www.slclab.com	www.slclab.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
37525275	2016-10-01	2009-12-22	2011-11-27	www.slclab.com	www.slclab.com	C=ES, ST=MADRID, L=MADRID, O=ips Certification Authority, OU=Certificaciones, CN=ipsCA Level 1 CA_emailAddress=ipscalevel1@ipsca.com
37454966	2016-10-01	2011-11-29	2013-12-04	www.slclab.com	www.slclab.com	C=ES, ST=MADRID, L=MADRID, O=ips Certification Authority, OU=Certificaciones, CN=ipsCA Level 1 CA_emailAddress=ipscalevel1@ipsca.com
10179132	2015-10-16	2015-10-13	2018-10-17	www.slclab.com	slclab.com www.slclab.com	C=US, ST=VA, L=Herndon, O=Network Solutions L.L.C., CN=Network Solutions OV Server CA 2
2844037	2013-10-19	2013-10-17	2015-10-17	www.slclab.com	www.slclab.com	C=US, O=Network Solutions L.L.C., CN=Network Solutions EV Server CA
683013	2013-03-26	2012-10-11	2013-10-16	www.slclab.com	www.slclab.com	C=ES, ST=MADRID, L=MADRID, O=ips Certification Authority, OU=Certificaciones, CN=ipsCA Level 1 CA_emailAddress=ipscalevel1@ipsca.com

Zendolims.com - dominio observado

Dominio público asociado a la marca de producto. Responde con servicio web accesible por HTTPS con certificado válido.

zendolims.com: 443 - WEB PROPERTY		AS OF 17 OCT 2025 20:55 UTC
HTML Title	Document Moved	Endpoints (2) 443 / HTTP 443 / HTTP /index... Software (2)
Browser Trust		Microsoft ASP.NET Microsoft Internet Information Services
MATCHED FIELDS		
web.cert.names	zendolims.com	
web.cert_parsed.subject.common_name	*.zendolims.com	
web.cert_parsed.subject_dn	CN=*.zendolims.com	
web.endpoints.hostname	www.zendolims.com	
web.endpoints.http.body	https://www.zendolims.com/index	
web.endpoints.http.favicon.name	https://www.zendolims.com/asset	
web.endpoints.http.headers.value	https://www.zendolims.com/index	
web.endpoints.http.html_tags	https://www.zendolims.com/asset	
web.endpoints.http.url	https://www.zendolims.com/	
web.hostname	www.zendolims.com	
zendolims.com: 443 - WEB PROPERTY		AS OF 17 OCT 2025 20:54 UTC
HTML Title	Document Moved	Endpoints (2) 443 / HTTP Software (2)
Browser Trust		Microsoft ASP.NET Microsoft Internet Information Services
MATCHED FIELDS		
web.cert.names	zendolims.com	
web.cert_parsed.subject.common_name	*.zendolims.com	
web.cert_parsed.subject_dn	CN=*.zendolims.com	
web.endpoints.hostname	zendolims.com	
web.endpoints.http.body	https://www.zendolims.com/*;char	
web.endpoints.http.headers.value	https://www.zendolims.com/	
web.endpoints.http.url	https://zendolims.com/	
web.hostname	zendolims.com	



VISOR DE CERTIFICADOS: *.ZENDOLIMS.COM

General Detalles

Enviado a

Nombre común (CN)	*.zendolims.com
Organización (O)	<No es parte del certificado>
Unidad organizativa (OU)	<No es parte del certificado>

Emitido por

Nombre común (CN)	Sectigo Public Server Authentication CA DV R36
Organización (O)	Sectigo Limited
Unidad organizativa (OU)	<No es parte del certificado>

Periodo de validez

Emitido el	lunes, 2 de junio de 2025, 2:00:00
Vencimiento el	viernes, 3 de julio de 2026, 1:59:59

Huellas digitales SHA-256

Certificado	e7d5b9cb89ba0c6860a68562a1ed71dc3baa467b0b6c98ab78aac022fcea3d64
Clave pública	838a93f2e2618b5e85be9bb9cefc5af62ede20ff11a7e344d6cd53ddc6ec6ef8

VISOR DE CERTIFICADOS: *.ZENDOLIMS.COM

General **Detalles**

Jerarquía de certificado

- ▼ Sectigo Public Server Authentication Root R46
- ▼ Sectigo Public Server Authentication CA DV R36
- *.zendolims.com

Campos del certificado

- ▼ *.zendolims.com
 - ▼ Certificado
 - Versión
 - Número de serie
 - Algoritmo de firma de certificado
 - Emisor
 - ▼ Validez
 - No antes de

Valor de campo

CN = Sectigo Public Server Authentication CA DV R36
 O = Sectigo Limited
 C = GB

Exportar...

Durante la revisión pasiva **no se identificaron subdominios adicionales de uso público** con contenido propio más allá de “www”, salvo referencias puntuales de alias o nombres técnicos presentes en evidencias de infraestructura. En cualquier caso, los certificados observados para el dominio de producto cubren los nombres esperados (dominio raíz y “www”)

Notas de lectura para [zendolims.com](#)

- La presencia de dos nombres principales ([zendolims.com](#) y [www.zendolims.com](#)) dentro del certificado es el comportamiento estándar para un sitio público.
- En la evidencia técnica del equipo aparecen **IPs** asociadas donde el nombre resuelve por **HTTP/ HTTPS**; esto no altera el comportamiento del certificado mientras el nombre del sitio coincide con alguno de los **SANs** del certificado presentado por el servidor.
- crt.sh (histórico de certificados): el registro publico muestra uso continuado de certificados **wildcard** para [*.zendolims.com](#) (incluyen [zendolims.com](#) como SAN), con renovaciones anuales y emisores predominantes de **Sectigo** en los últimos años, además de entradas antiguas emitidas por **Network Solutions**. Esto confirma una **línea temporal de renovaciones ordenada y coherente** con el uso de “www” como subdominio principal.



Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	18765951424	2025-06-02	2025-06-02	2026-07-02	*.zendolims.com	*.zendolims.com zendolims.com	C=GB,O=Sectigo Limited,CN=Sectigo Public Server Authentication CA DV R36
	18765950698	2025-06-02	2025-06-02	2026-07-02	*.zendolims.com	*.zendolims.com zendolims.com	C=GB,O=Sectigo Limited,CN=Sectigo Public Server Authentication CA DV R36
	12971273474	2024-05-06	2024-05-06	2025-06-05	*.zendolims.com	*.zendolims.com zendolims.com	C=GB,ST=Greater Manchester,L=Salford,O=Sectigo Limited,CN=Sectigo RSA Domain Validation Secure Server CA
	12971273472	2024-05-06	2024-05-06	2025-06-05	*.zendolims.com	*.zendolims.com zendolims.com	C=GB,ST=Greater Manchester,L=Salford,O=Sectigo Limited,CN=Sectigo RSA Domain Validation Secure Server CA
	9136483636	2023-04-13	2023-04-13	2024-05-12	*.zendolims.com	*.zendolims.com zendolims.com	C=GB,ST=Greater Manchester,L=Salford,O=Sectigo Limited,CN=Sectigo RSA Domain Validation Secure Server CA
	9136483853	2023-04-13	2023-04-13	2024-05-12	*.zendolims.com	*.zendolims.com zendolims.com	C=GB,ST=Greater Manchester,L=Salford,O=Sectigo Limited,CN=Sectigo RSA Domain Validation Secure Server CA
	6367151488	2022-03-18	2022-03-18	2023-04-17	*.zendolims.com	*.zendolims.com zendolims.com	C=GB,ST=Greater Manchester,L=Salford,O=Sectigo Limited,CN=Sectigo RSA Domain Validation Secure Server CA
	6367151426	2022-03-18	2022-03-18	2023-04-17	*.zendolims.com	*.zendolims.com zendolims.com	C=GB,ST=Greater Manchester,L=Salford,O=Sectigo Limited,CN=Sectigo RSA Domain Validation Secure Server CA
	4193532488	2021-03-10	2021-03-10	2022-04-09	*.zendolims.com	*.zendolims.com zendolims.com	C=GB,ST=Greater Manchester,L=Salford,O=Sectigo Limited,CN=Sectigo RSA Domain Validation Secure Server CA
	4193532494	2021-03-10	2021-03-10	2022-04-09	*.zendolims.com	*.zendolims.com zendolims.com	C=GB,ST=Greater Manchester,L=Salford,O=Sectigo Limited,CN=Sectigo RSA Domain Validation Secure Server CA
	2556561174	2020-03-09	2020-03-09	2021-04-08	*.zendolims.com	*.zendolims.com zendolims.com	C=GB,ST=Greater Manchester,L=Salford,O=Sectigo Limited,CN=Sectigo RSA Domain Validation Secure Server CA
	2556561178	2020-03-09	2020-03-09	2021-04-08	*.zendolims.com	*.zendolims.com zendolims.com	C=GB,ST=Greater Manchester,L=Salford,O=Sectigo Limited,CN=Sectigo RSA Domain Validation Secure Server CA
	1352870297	2019-04-05	2019-04-05	2020-04-04	*.zendolims.com	*.zendolims.com zendolims.com	C=GB,ST=Greater Manchester,L=Salford,O=Sectigo Limited,CN=Sectigo RSA Domain Validation Secure Server CA
	1352869878	2019-04-05	2019-04-05	2020-04-04	*.zendolims.com	*.zendolims.com zendolims.com	C=GB,ST=Greater Manchester,L=Salford,O=Sectigo Limited,CN=Sectigo RSA Domain Validation Secure Server CA
	33578192	2016-09-21	2016-09-16	2019-09-16	www.zendolims.com	www.zendolims.com zendolims.com	C=US,ST=VA,L=Herndon,O=Network Solutions L.L.C.,CN=Network Solutions OV Server CA 2

Comparación entre ambos dominios

- Cobertura de certificados:

En [slclab.com](#), los certificados públicos vigentes cubren el dominio raíz y “www”, permitiendo navegación **HTTPS** sin advertencias en la web principal.

En [zendolims.com](#), el histórico de crt.sh muestra uso continuado de certificados **wildcard** * [zendolims.com](#) (incluyen [zendolims.com](#) y [www.zendolims.com](#) como identidades cubiertas), con renovaciones periódicas.

- Subdominios especiales:

En [slclab.com](#) figura publicado el subdominio “interno”, que responde con la página por defecto de **IIS** y presenta un certificado **autofirmado**.

En [zendolims.com](#) no se observaron subdominios adicionales con contenido público relevante durante la revisión pasiva.

- Emisores/ línea temporal:

En [slclab.com](#) se aprecian cambios de emisores a lo largo del tiempo (rotaciones habituales).

En [zendolims.com](#) crt.sh refleja emisores predominantes de **Sectigo** en los últimos años y entradas más antiguas emitidas por **Network Solutions**.

- Ecosistema técnico:

Las evidencias muestran **Microsoft IIS/ASP.NET** en la web principal de [SLC Lab](#) y certificados “Trusted” para los nombres de cara al público. El caso “interno” constituye una respuesta distinta por el tipo de certificado presentado y la página genérica del servidor.



Contenido y estructura

Visión general

Se revisaron los ficheros públicos de indexación del sitio (**robots.txt** y **sitemaps**) y se consultó el histórico del sitio en archivos públicos. Con ello se obtuvo una fotografía de la estructura de contenidos y de algunos módulos publicados por la organización.

robots.txt - rutas declaradas

El fichero <https://www.slclab.com/robots.txt> **declara numerosas rutas** bajo **Disallow** (por ejemplo, nombres de proyectos, clientes o “demos”) y permite el acceso a carpetas de idiomas (/en/, /pt/). También incluye la regla **Disallow: /*.asp\$**.

En la documentación del equipo se listan ejemplos como: /Pruebas/, /Demos.../, y carpetas con nombres propios de personas o entidades.

¿Qué significa?

robots.txt indica a los buscadores no indexar, **pero no oculta esas rutas**; permite inferir la estructura de la web. La presencia de denominaciones tipo clientes/ demos sugiere históricos de trabajo y secciones funcionales.

```

User-agent: *
Allow: /css/
Allow: /img/
Allow: /fonts/
Allow: /pt/
Allow: /en/
Disallow: /*.asp$
Disallow: /descargas/
Disallow: /downloads/
Disallow: /emailimages/
Disallow: /emails/
Disallow: /novedades/
Disallow: /Alkimia/
Disallow: /Avance/
Disallow: /BonaNova/
Disallow: /CDDB/
Disallow: /Cendisa/
Disallow: /CentroPama/
Disallow: /CentroTeruel/
Disallow: /CesfamCabrero/
Disallow: /ClinicaMarazuela/
Disallow: /ClinicaSantiago/
Disallow: /ControlSMS/
Disallow: /DamianTrujillo/
Disallow: /DemoNueva/
Disallow: /DemoPeticionElectronica/
Disallow: /DrAzua/
Disallow: /EncarnacionRodriguez/

```



sitemap.xml - estructura y fechas de actualización

Existen sitemaps por idioma: [sitemap.xml](https://www.slclab.com/sitemap.xml), [sitemap-en.xml](https://www.slclab.com/sitemap-en.xml), [sitemap-pt.xml](https://www.slclab.com/sitemap-pt.xml).

```
Sitemap: https://www.slclab.com/sitemap.xml
Sitemap: https://www.slclab.com/sitemap-en.xml
Sitemap: https://www.slclab.com/sitemap-pt.xml
```

En sitemap.xml aparecen URLs con lastmod antiguos (por ejemplo, 2015/2022) como [/productos.aspx](https://www.slclab.com/productos.aspx), secciones **ALFA21** y **Zendo**.

¿Qué significa?

Los **sitemaps** ofrecen una lista completa de URLs que el sitio publica; las fechas ayudan a entender la antigüedad de algunas páginas y la evolución de módulos.

```
This XML file does not appear to have any style information associated with it. The document tree is shown below.

<urlset xmlns="http://www.sitemaps.org/schemas/sitemap/0.9" xmlns:xhtml="http://www.w3.org/1999/xhtml">
  <url>
    <loc>https://www.slclab.com/index.aspx</loc>
    <lastmod>2022-10-05</lastmod>
    <changefreq>monthly</changefreq>
    <priority>1</priority>
  </url>
  <url>
    <loc>https://www.slclab.com/empresa.aspx</loc>
    <lastmod>2022-10-05</lastmod>
    <changefreq>monthly</changefreq>
  </url>
  <url>
    <loc>https://www.slclab.com/productos.aspx</loc>
    <lastmod>2015-01-20</lastmod>
    <changefreq>monthly</changefreq>
    <priority>0.9</priority>
  </url>
  <url>
    <loc>https://www.slclab.com/alfa21-analisisclinicos.aspx</loc>
    <lastmod>2022-10-05</lastmod>
    <changefreq>monthly</changefreq>
    <priority>0.5</priority>
  </url>
  <url>
    <loc>https://www.slclab.com/alfa21-veterinaria.aspx</loc>
    <lastmod>2022-10-05</lastmod>
    <changefreq>monthly</changefreq>
    <priority>0.5</priority>
  </url>
  <url>
    <loc>https://www.slclab.com/alfa21-fqm.aspx</loc>
    <lastmod>2022-10-05</lastmod>
    <changefreq>monthly</changefreq>
    <priority>0.5</priority>
  </url>
</urlset>
```

Idiomas y organización del contenido

La web pública contenido en varios idiomas (ES/EN/PT). En robots.txt se permiten /en/ y /pt/, y existen sitemaps específicos por idioma.

¿Qué significa?

El contenido multilenguaje implica que la misma estructura (menús, fichas, soporte) se replica en varias versiones, aumentando la superficie de la publicación a revisar.



Páginas funcionales y endpoints visibles

Durante la revisión pasiva, los siguientes **endpoints** del dominio público responden con código **HTTP 200 (OK)** y cargan contenido:

- <https://www.slclab.com/sitemap.aspx>

Name	Status	Type	Initiator	Size	Time
sitemap.aspx	200	document	Other	5.9 kB	~1.00 ms

- <https://www.slclab.com/alfa21net.aspx>

Name	Status	Type	Initiator	Size	Time
alfa21net.aspx	200	document	Other	0.7 kB	~1.00 ms

- <https://www.slclab.com/alfa21-peticionelectronica.aspx>

Name	Status	Type	Initiator	Size	Time
alfa21-peticionelectronica.aspx	200	document	Other	7.1 kB	~1.00 ms

- <https://www.slclab.com/enviosms.aspx>

Name	Status	Type	Initiator	Size	Time
enviosms.aspx	200	document	Other	5.9 kB	~1.00 ms

Estos recursos forman parte del área funcional del sitio (módulos vinculados a **ALFA21** y páginas auxiliares como **sitemap.aspx**). En las capturas de red del navegador se observa el **200 OK**, con servidor **Microsoft-IIS** y tipo de contenido **text/html; charset=utf-8**.

¿Qué significa?

Los **endpoints** citados están publicados y operativos (respuesta 200) en el momento de la revisión, por lo que constituyen parte de la superficie de contenido actualmente expuesta por la organización.



Documentos y metadatos (FOCA)

Alcance de la revisión

Se buscaron documentos públicos (**PDF/ DOC**) vinculados a los dominios de la organización mediante búsquedas pasivas:

- **Google dorks** (por ejemplo, ***site:slclab.com filetype:pdf***).
- **FOCA** para localizar y extraer **metadatos** (autores, software, rutas internas, etc.).

Resultados por dominio

slclab.com

- Se localizaron pocos documentos públicos (material comercial y de ayuda), entre ellos: “*instrucciones de registro web/ Alfa21net*”, “*FOLLETO-ZENDO-LIMS.pdf*”, y otros PDFs similares.
- El análisis con **FOCA** devolvió **1 PDF útil para revisión**, no se observaron metadatos sensibles (sin usuario internos ni rutas críticas relevantes).

Type	Path	Download Date	Doc - Metadata	Author - Title	Reader Date
PDF	https://www.slclab.com/LabTutor/reporta/instruccione...	10/23/2023 12:01:04	108,67 KB		09/01/2023 10:51:20

Log output at the bottom:

```

Time      Source      Severity      Message
12:00:42  MetadataSearch  error      An error has occurred on Bing(BingSearchWeb). Contact the vendor vendor_id: 4025. Possible:
12:00:44  MetadataSearch  medium    Bing(Bing) search finished successfully! Total found result count: 0
12:00:49  MetadataSearch  medium    GoogleAPI search finished successfully! Total found result count: 1

```



INSTRUCCIONES DE REGISTRO WEB DE RESULTADOS
www.slclab.com/LabTovar

Estimado Usuario.

Si ya se registró anteriormente en nuestra página web no es necesario que vuelva a hacerlo. En este caso, en la página anterior, introduzca su usuario y contraseña. En caso de no recordarla haga clic en Recordar Contraseña y siga los pasos indicados.

Si es la primera vez que accede, siga estas instrucciones para poder entrar en sus resultados y ver sus analíticas:

1. En el campo Identificador del Laboratorio introduzca el Número de Identificador facilitado por la enfermera o centro médico el día de la extracción o de entrega de muestra. Si lo ha extraviado, no se preocupe, contacte con el laboratorio y se lo facilitaremos.
2. Introduzca su Fecha de Nacimiento. En caso de no haberla facilitado a nuestro personal con anterioridad no podrá registrarse en este momento, y deberá contactar con el laboratorio con el número de identificador del primer punto, o en su defecto sus datos personales, y su Fecha de Nacimiento.
3. Posteriormente introduzca su mail. Este mail está asociado a su número de historia clínica, por tanto, cada paciente deberá facilitar un mail diferente en su registro.

zendolims.com

- En la revisión pasiva **no se hallaron documentos públicos expuestos** para este dominio.

Qué significan los metadatos

- Los metadatos son **información oculta dentro del archivo** (por ejemplo, Autor, Software usado, Fechas, Rutas de archivo).
- Ayudan a identificar **quién creó el documento** o con qué herramienta, y a veces revelan nombres de usuario o carpetas internas.
- En esta revisión, los metadatos observados en el PDF de **slclab.com** no aportan datos sensibles aprovechables.

Resumen del hallazgo

- **Volumen documental bajo:** apenas algunos PDFs comerciales/ informativos en **slclab.com**; sin exposición documental en **zendolims.com**.
- **Metadatos revisados:** sin información sensible (no se detectaron usuarios internos ni rutas críticas).

Exposición en índices (Shodan/ Censys)

Visión general

Se consultaron índices públicos de internet para observar qué servicios están visibles hacia el exterior y como se identifican (puertos, banners, certificados, pilas tecnológicas).

- **Shodan:** muestra puertos/ servicios detectados y parte del banner de cada servicio.
- **Censys:** consolida propiedades web (hostnames) y certificados presentados por esos hosts.



slclab.com - hosts e IPs observadas en índices

En los índices se asocian hostnames del dominio con IPs que exponen servicios web y otros servicios comunes:

- **93.189.91.160 (Clouding)**
 - Servicios observados: **FTP/21, HTTP/80 y HTTPS/ 443.**
 - Identificación web: Microsoft IIS con contenido público accesible por HTTPS.
- **80.24.200.197 (Telefónica/ Movistar)**
 - Servicios observados: **SIP/ 5060 (UDP)** y servicio web **IIS**
 - En el banner **SIP** se visualizó un campo **Contact** con **IP interna** (dirección privada), lo que evidencia que el servicio **SIP** responde públicamente e incluye datos de su entorno

93.189.91.160 - HOST	
dd2b685f-82e7-4300-8c41-a3fe28d86eeb.clouding.host	
OS	Microsoft Windows
Network (AS)	CLOUDING (49635)
Location	Barcelona, Catalonia (ES)
MATCHED FIELDS	
host.dns.forward_dns.key	slclab.com
host.dns.forward_dns.value.name	slclab.com
host.dns.names	slclab.com
host.ip	93.189.91.160
host.services.cert.names	slclab.com 443 / HTTP
host.services.cert.parsed.subject.common_name	www.slclab.com 443 / HTTP
host.services.cert.parsed.subject_dn	CN=www.slclab.com 443 / HTTP
host.services.endpoints.http.body	https://www.slclab.com/*>here</a 80 / HTTP 443 / HTTP
host.services.endpoints.http.headers.value	https://www.slclab.com/ 80 / HTTP 443 / HTTP

80.24.200.197 - HOST	
197.red-80-24-200.staticip.rima-tde.net	
OS	Microsoft Windows
Network (AS)	TELEFONICA_DE_ESPAÑA (3352)
Location	Salamanca, Castile and León (ES)
MATCHED FIELDS	
host.dns.forward_dns.key	interno.slclab.com
host.dns.forward_dns.value.name	interno.slclab.com



93.189.91.160

General Information

Hostnames: dd2b685f-82e7-4300-8c41-a3fe28d86eeb.clouding.host

Domains: clouding.host

Country: Spain

City: Barcelona

Organization: CLOUDI NEXTGEN SL

ISP: CLOUDI NEXTGEN SL

ASN: AS49635

Operating System: Windows

Web Technologies

Operating Systems: Windows Server

Web Servers: IIS 100

Open Ports

21 / TCP

Microsoft ftpd

220 Microsoft FTP Service
530 User cannot log in.
214 The following commands are recognized (* ==> s unimplemented).
ABOR
ACCT
ADAT *
ALLO
APPE
AUTH
CCC
CDUP
CMD
DELE
ENC *
EPRT
EPSV
FEAT
HELP
HOST
LANG
LIST
MDTM
MLC *
MDT

// LAST SEEN: 2025-10-18

80.24.200.197

General Information

Hostnames: 197red-80-24-200.staticip.rima-tde.net

Domains: rima-tde.net

Country: Spain

City: Salamanca

Organization: TELEFONICA DE ESPANA S.A.U.

ISP: TELEFONICA DE ESPANA S.A.U.

ASN: AS3352

Operating System: Windows

Web Technologies

Operating Systems: Windows Server

Web Servers: IIS 100

Open Ports

80 / TCP

Microsoft IIS httpd 10.0

IIS Windows Server

HTTP/1.1 200 OK
Content-type: text/html
Last-Modified: Thu, 24 Sep 2020 16:12:25 GMT
Accept-Ranges: bytes
ETag: "8365167e8d02d610"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Sat, 25 Oct 2025 07:25:02 GMT
Content-Length: 703

100 / TCP

Microsoft IIS httpd 10.0

401 - No autorizado: acceso denegado debido a credenciales no válidas.

HTTP/1.1 401 Unauthorized
Cache-control: private

zendolims.com - hosts e IPs observadas en índices

Para el dominio de producto aparecen resoluciones hacia dos **IPs** con triada típica **21/80/443**:

- **185.253.153.148**
- **46.183.114.177**



En ambas se observan respuesta **HTTP/ HTTPS** y disponibilidad del puerto **FTP/ 21**. La parte web sirve contenido por HTTPS con certificado válido vinculado a los nombres del dominio.

185.253.153.148 - HOST
Sc2509f9-b663-4bf9-8314-39b96f55fac0.clouding.host

OS	Microsoft Windows	3 Total Services
Network (All)	CLOUDING (49635)	21 / FTP 80 / HTTP 443 / HTTP
Location	Barcelona, Catalonia (ES)	

MATCHED FIELDS

```
host.dns.forward_dns.key zendolines.com
host.dns.forward_dns.value.name zendolines.com
host.dns.names zendolines.com
host.ip 185.253.153.148
host.services.cert.names zendolines.com 443 / HTTP
host.services.cert.parsed.subject.common_name *.zendolines.com 443 / HTTP
host.services.cert.parsed.subject_dn CN=*.zendolines.com 443 / HTTP
```

46.183.114.177 - HOST
c0c36f6e-73c1-49dd-8e76-d378900a2f57.clouding.host

OS	Microsoft Windows	3 Total Services
Network (All)	CLOUDING (49635)	21 / FTP 80 / HTTP 443 / HTTP
Location	Telè, Catalonia (ES)	

MATCHED FIELDS

```
host.ip 46.183.114.177
host.services.cert.names zendolines.com 443 / HTTP
host.services.cert.parsed.subject.common_name *.zendolines.com 443 / HTTP
host.services.cert.parsed.subject_dn CN=*.zendolines.com 443 / HTTP
host.services.endpoints.http.body <title>Zendolines</title> 80 / HTTP | 443 / HTTP
host.services.endpoints.http.html_tags <title>Zendolines</title> 80 / HTTP | 443 / HTTP
host.services.endpoints.http.html_tags https://www.zendolines.com/* /> 80 / HTTP | 443 / HTTP
host.services.endpoints.http.html_tags Zendolines 80 / HTTP | 443 / HTTP
```

SHODAN Explore Pricing Search

185.253.153.148

General Information

Hostnames: Sc2509f9-b663-4bf9-8314-39b96f55fac0 clouding.host, zendolines.com

Domains: clouding.host, zendolines.com

Country: Spain

City: Barcelona

Organization: CLOUDI NEXTGEN SL

ISP: CLOUDI NEXTGEN SL

ASN: AS49635

Operating System: Windows

Open Ports

// 21 / TCP

Microsoft ftpd

21 Microsoft FTP Service
53 User cannot log in, home directory inaccessible.
254 The following commands are recognized (* =='s implementation):
ABOR
ACCT
ALLO
ALLO
APPE
CDUP
CWD
DELE
EMTCL
EPRT
FEAT
HELP
LIST
LRETR
LSTOR
MDTM
MKD
MLSD
NLST
NSWP
OPTS
PASV
PWD
QUIT



General Information

Hostnames: c0c36f6e-73c1-49dd-8e76-dd78900a2f57.clouding.host, zendolims.com

Domains: clouding.host, zendolims.com

Country: Spain

City: Telè

Organization: Clouding.io Virtual Machine Hosting

ISP: CLOUDI NEXTGEN SL

ASN: AS49635

Operating System: Windows

Open Ports

// 80 / TCP Microsoft IIS httpd 100

Zendolims

HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Mon, 23 Oct 2023 07:47:05 GHT
Accept-Ranges: bytes
ETag: "0fadfd1d855d01:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Sat, 25 Oct 2025 15:41:28 GHT
Content-Length: 253

// 443 / TCP Microsoft IIS httpd 100

Zendolims

HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Mon, 23 Oct 2023 07:47:05 GHT
Accept-Ranges: bytes
ETag: "0fadfd1d855d01:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Fri, 10 Oct 2025 14:39:11 GHT
Content-Length: 253

Banners y pilas tecnológicas visibles

En los servicios web indexados, los banners/ cabeceras identifican **Microsoft IIS** y **ASP.NET** como tecnología de servidor en el frontal público.

- En **HTTPS** se presentan certificados “**Trusted**” para los nombres principales (slclab.com, www.slclab.com, zendolims.com, www.zendolims.com).
- En **HTTP/ 80** los índices ven el título y el encabezado **Server (IIS)**, y en **FTP/ 21** se observa el servicio expuesto (sin detalle de credenciales, al tratarse de una lectura pasiva del banner).

Certificados observados desde índices

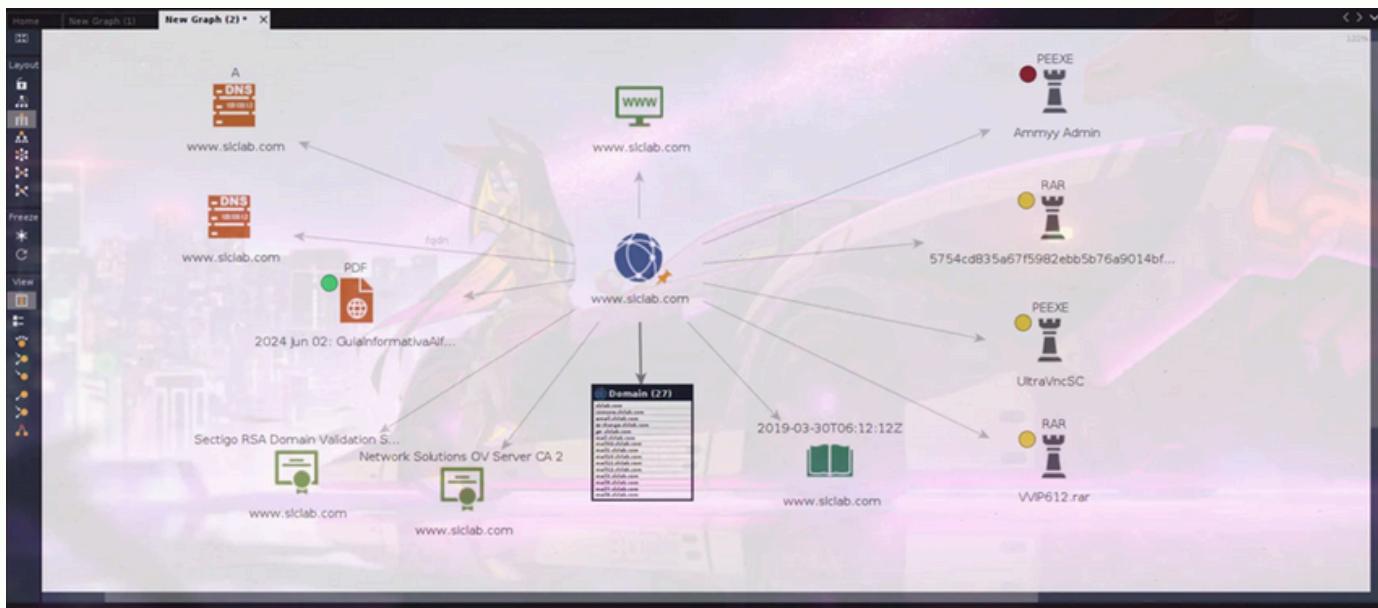
Los índices enlazan hosts con los certificados que presentan:

- En slclab.com los certificados válidos cubren dominio y “www”, el subdominio “**interno**” responde con autofirmado.
- En zendolims.com se aprecian certificados validos, el histórico público (crt.sh) muestra **wildcards** *.zendolims.com y renovaciones periódicas.



Vista consolidada en Maltego

Se elaboró un gráfico en **Maltego** para consolidar dominios, subdominios, IPs y certificados. La vista facilita entender relaciones (que nombre apunta a que IP, que certificado cubre a que host, y que proveedor está detrás).





Hallazgos relevantes por puertos

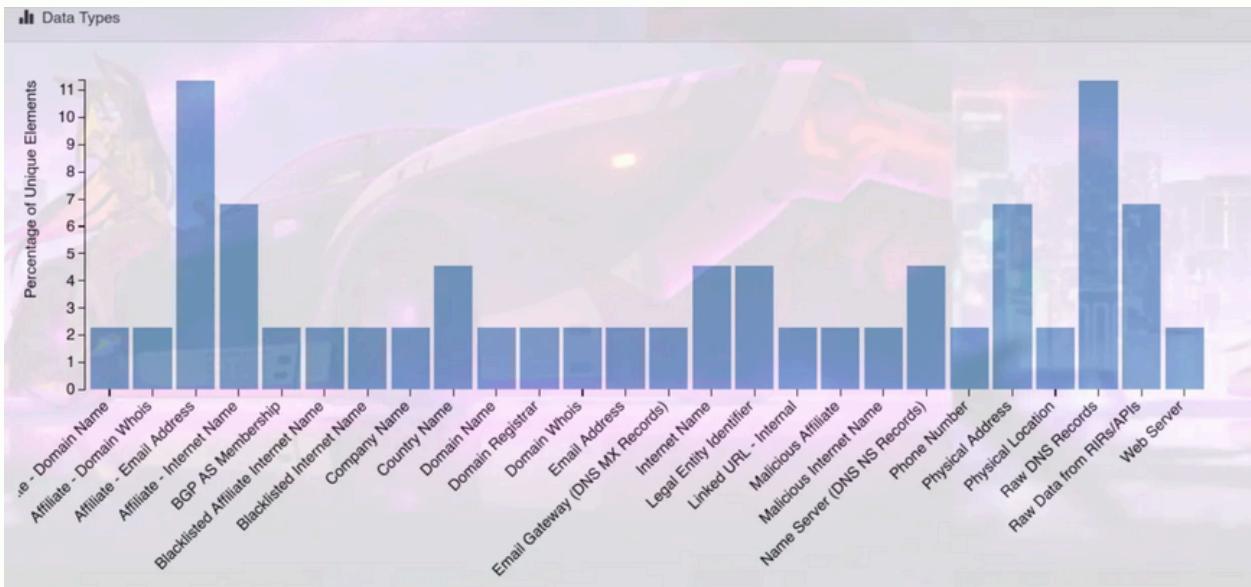
La siguiente tabla resume los servicios observados en **índices públicos** para los dominios analizados, con referencia a la evidencia ya incluida en este informe.

IP / Host	Puerto	Servicio / Protocolo	Observado en	Observación
93.189.91.160 (slclab.com)	21	FTP (Microsoft FTP Service)	Shodan	Servicio FTP visible en Internet.
93.189.91.160 (slclab.com)	80 / 443	HTTP / HTTPS (IIS)	Shodan / Censys	Frontal web accesible; HTTPS con certificado válido.
80.24.200.197 (slclab.com)	5060/UDP	SIP / 3CX	Shodan	Banner SIP expone el campo <i>Contact</i> con IP privada.
80.24.200.197 (slclab.com)	80 / 443	HTTP / HTTPS (IIS)	Shodan / Censys	Frontal web accesible.
185.253.153.148 (zendolims.com)	21 / 80 / 443	FTP / HTTP / HTTPS	Shodan	Tríada estándar visible públicamente.
46.183.114.177 (zendolims.com)	21 / 80 / 443	FTP / HTTP / HTTPS	Censys / Shodan	Misma tríada asociada al dominio de producto.



SpiderFoot

Es una herramienta **OSINT** que, sin interactuar con los sistemas, recoge datos públicos del dominio (**DNS y correo**) y ofrece una foto inicial para luego contrastar en otros índices (Censys/ Shodan).



DNS y correo

- Registros DNS básicos: obtuvo **A/MX/NS/TXT** para zendolims.com. No encontró **AAAA (IPv6)**. Hoy el sitio funciona sólo en IPv4.
- Postura de correo en **TXT**:
 - SPF**: configuración estricta (-all).
 - DKIM**: clave observada de **1024 bits** (lo actual **recomendado es 2048**).
 - DMARC**: falta el parámetro **-rua** (no se recibieron informes agregados de DMARC).

www.z endol ims.c om	[{"task": {"visibility": "public", "method": "manual", "domain": "www.zendolims.com", "apexDomain": "zendolims.com", "time": "2021-10-25T16:16:31.916Z", "uuid": "fbc51647-bdff-4da5-9fd2-71f22d683189", "url": "https://www.zendolims.com/laboratoriordmari/resultados/"}, "stats": {"uniqIPs": 5, "uniqCountries": 3, "dataLength": 8322362, "encodedDataLength": 2846527, "requests": 32}, "page": {"country": "UA", "server": "Microsoft-IIS/10.0", "ip": "185.253.153.148", "mimeType": "text/html", "title": "Zendolims", "url": "https://www.zendolims.com/laboratoriordmari/resultados/", "tlsValidDays": 395, "tlsAgeDays": 229, "ptr": "5c2509f9-b663-4bf9-8314-39b96f55fac0.clouding.host", "tlsValidFrom": "2021-03-10T00:00:00.000Z", "domain": "www.zendolims.com", "apexDomain": "zendolims.com", "asname": "CLOUDING_ES", "asn": "AS49635", "tlsIssuer": "Sectigo RSA Domain Validation Secure Server CA", "status": "200"}, "_id": "fbc51647-bdff-4da5-9fd2-71f22d683189", "_score": None, "sort": [1635178591916, "fbc51647-bdff-4da5-9fd2-7"]}]	sfp_dnsr esolve
-------------------------------	--	-----------------



Subdominios

SpiderFoot no identificó subdominios públicos relevantes adicionales (más allá de www). Se probó con **Google Dorks**, y tampoco aparecieron subdominios indexados útiles. El dominio de producto **no exhibe subdominios significativos** en fuentes públicas.

Data Element	Source Data Element	Source Module	Identified
www.zendolims.com. 10 IN CNAME zendolims.com.	www.zendolims.com	sfp_dnsraw	2025-10-20 08:18:14
www.zendolims.com. 56 IN CNAME zendolims.com.	www.zendolims.com	sfp_dnsraw	2025-10-20 08:18:14
zendolims.com. 150 IN MX 5 smtp.rzone.de.	zendolims.com	sfp_dnsraw	2025-10-20 08:17:21
zendolims.com. 150 IN NS shades07.rzone.de. zendolims.com. 150 IN NS docks09.rzone.de.	zendolims.com	sfp_dnsraw	2025-10-20 08:17:21
zendolims.com. 98 IN NS docks09.rzone.de. zendolims.com. 98 IN NS shades07.rzone.de.	www.zendolims.com	sfp_dnsraw	2025-10-20 08:18:14

IP/ ASN y contraste en índices

Con la base de **SpiderFoot** se contrastó en índices (**Censys/ Shodan**) para completar la foto pública:

- Se asociaron dos IPs **zendolims.com** : **185.253.153.0/24** y **46.183.114.177**, ambas con la triada **21/80/443 (FTP/HTTP/HTTPS)**.
- En esa infraestructura se describe el bloque **185.253.153.0/24** y el proveedor **Clouding** como contexto operativo.

Hacia internet, el dominio de producto presenta servicios web estándar (**80/ 443**) y **FTP/21** visible; este último no cifra por defecto si no se usa modo seguro.

Para **slclab.com** , **SpiderFoot** no aportó hallazgos nuevos más allá de confirmar la base de DNS/correo ya recogida por otras fuentes; en cambio, para **zendolims.com** sí permitió consolidar **DNS/TXT**, confirmar la ausencia de **IPv6**, y orientar el contraste posterior en Censys/Shodan.

Conclusiones generales



La investigación **OSINT** realizada sobre **SLCLAB Informática S.L.** ha permitido identificar **varios elementos técnicos expuestos públicamente** que podrían representar **riesgos para la seguridad de la organización**. Aunque algunos hallazgos no constituyen fallos graves por sí mismos, en conjunto revelan una **superficie de exposición amplia**, con servicios visibles desde Internet, documentación accesible y configuraciones que **podrían ser aprovechadas por actores maliciosos**.

Se observa una infraestructura activa y funcional, pero con *áreas de mejora en términos de endurecimiento, visibilidad innecesaria y control de accesos*. La **presencia de servicios antiguos, configuraciones por defecto y falta de medidas de protección básicas** sugiere que no todas las capas de seguridad están implementadas o actualizadas.

Resumen de vulnerabilidades detectadas y nivel de criticidad

Nivel de Criticidad	Vulnerabilidad	Riesgos Principales	Ataques Probables
█ Crítica	FTP expuesto públicamente	Transmisión insegura, acceso no autorizado	Fuerza bruta, exfiltración pivoting
█ Crítica	SIIIP/VoIP con fuga de IP interna	Fuga de red interna, servicio expuesto	Spoofing, DoS, reconocimiento interno
█ Crítica	Archivo “Ammy Admin” alojado	Control remoto del sistema. Robo de información. Persistencia.	Ransomware. Robo de credenciales. Escalada de privilegios.
█ Alta	Subdominio interno accesible con ISS Default	Exposición de entorno privado. Cifrado débil	Fingerprinting, MITM, phising interno
█ Media	HTTP sin redireccionamiento a HTTPS	Tráfico sin cifrar, downgrade de seguridad	MITM. Manipulación de contenido.
█ Media	robots.txt revela estructura interna	Divulgación de rutas sensibles	Enumeración. Acceso a entornos ocultos.
█ Baja	Cabeceras de seguridad ausentes	Endurecimiento débil. Vulnerabilidad de ataques web.	XSS, clickjacking, downgrade
█ Baja	Certificados Wildcard con rotación normal	Riesgo ampliado si se compromete el wildcard.	Suplantación de subdominios. Uso indebido de certificados



Ataques más probables

A partir de los hallazgos, **los escenarios de ataque más plausibles incluyen:**

- **Suplantación de identidad (phishing):** debido a la exposición de correos corporativos con un patrón predecible y la falta de protección reforzada en el correo.
- **Acceso no autorizado a servicios internos:** como el subdominio “interno” accesible desde fuera o el servicio FTP sin cifrado.
- **Intercepción de comunicaciones:** por el uso simultáneo de HTTP (sin cifrar) y HTTPS, lo que podría permitir capturar información si no se redirige correctamente.
- **Ataques de fuerza bruta o escaneo automatizado:** contra servicios como SIP/VoIP o FTP, que están visibles desde Internet y pueden ser detectados fácilmente por herramientas automáticas.
- **Recopilación de información para ataques dirigidos:** gracias a la estructura revelada en el archivo robots.txt y la falta de cabeceras de seguridad en la web.





Recomendaciones

A partir de los hallazgos identificados, **se proponen las siguientes recomendaciones organizadas por nivel de prioridad y esfuerzo**. El objetivo es reducir la exposición digital de la organización, mitigar riesgos y fortalecer su postura de seguridad de forma progresiva.

Recomendaciones inmediatas:

- **Restringir el acceso al subdominio “interno”:** actualmente es accesible desde Internet y muestra una página por defecto con un certificado no confiable. Debería limitarse su acceso o eliminarse si no es necesario.
- **Forzar la redirección de HTTP a HTTPS:** para asegurar que toda la navegación se realice de forma cifrada y evitar posibles interceptaciones de tráfico.
-
- **Deshabilitar el servicio FTP expuesto:** dado que transmite información sin cifrar, se recomienda eliminarlo o reemplazarlo por alternativas seguras como SFTP.
- **Revisar el archivo robots.txt:** contiene rutas internas que, aunque no son fallos por sí mismas, pueden revelar información útil para un atacante. Se sugiere limpiar o reestructurar este archivo.
- **Actualizar o eliminar certificados auto firmados:** especialmente en entornos públicos, para evitar que los usuarios se acostumbren a ignorar advertencias de seguridad.



Recomendaciones de fortalecimiento

- **Implementar cabeceras de seguridad web:** como **HSTS, CSP y X-Frame-Options**, que ayudan a prevenir ataques comunes del lado del navegador.
- **Limitar la exposición del servicio SIP/VoIP:** aplicar autenticación robusta y restringir el acceso desde el exterior si no es estrictamente necesario.
- **Bloquear la ejecución y descarga de Ammy Admin y software similar** por políticas de seguridad y listas de aplicaciones permitidas (**whitelisting**).
- **Implementar un sistema de monitoreo** que detecte intentos de ejecución de archivos portables y **herramientas de acceso remoto no autorizadas**, incluyendo **Ammy Admin**.
- **Auditar los servicios visibles desde Internet:** identificar cuáles son realmente necesarios y cerrar aquellos que no aporten valor o representen un riesgo innecesario.
- **Revisar la visibilidad del personal en plataformas públicas:** especialmente si se combinan con correos corporativos predecibles, para reducir el riesgo de suplantación o ingeniería social.

Recomendaciones estratégicas

- **Establecer una política de gestión de exposición digital:** que incluya revisiones periódicas de dominios, subdominios, servicios y documentación pública.
- **Desarrollar un plan de endurecimiento de servidores y aplicaciones:** con configuraciones seguras por defecto y controles de acceso adecuados.
- **Integrar la detección de software remoto no corporativo** en los procedimientos de respuesta a incidentes y auditorías periódicas de seguridad.
- **Capacitar al personal en buenas prácticas de seguridad digital:** tanto a nivel técnico como no técnico, para fomentar una cultura de seguridad en toda la organización.
- **Implementar monitoreo continuo de la infraestructura expuesta:** para detectar cambios, nuevas exposiciones o posibles amenazas en tiempo real.



Anexos

- MFA (Autenticación multifactor)

Método de acceso que exige más de una prueba (por ejemplo, contraseña + código del móvil).

- SOC (Security Operations Center)

Equipo o servicio que monitoriza y responde a incidentes de seguridad.

- SIP/VoIP

- Protocolos para telefonía sobre IP; SIP es el más común para establecer llamadas.

- ASN (Autonomous System Number)

Identificador público del bloque de direcciones IP gestionado por un proveedor de Internet.

- IP

Dirección numérica que identifica un dispositivo en la red.

- HSTS / CSP

HSTS indica al navegador que solo use HTTPS; CSP controla qué recursos externos puede cargar una página.

- HTTP / HTTPS

- Protocolos de navegación; HTTPS es la versión cifrada (segura) de HTTP.

- FTP es un protocolo para transferir archivos, SFTP es su alternativa segura (cifrada).

- Subdominio

- División del dominio principal (por ejemplo, interno.slclab.com).

- PII

Información de identificación personal. Datos que identifican a una persona (nombre completo, correo, DNI, teléfono).

- DNS; Sistema de nombres de dominio. Traduce un nombre web (ej. slclab.com) a una dirección numérica (IP).

- SPF

Registro que indica qué servidores pueden enviar correo en nombre de un dominio. DKIM

Firma digital de correos que verifica que un mensaje no fue alterado y proviene del dominio declarado.

- DMARC

Política que indica qué hacer con los correos que fallan SPF o DKIM (por ejemplo, rechazarlos).

- TLS / Certificado TLS

- Tecnología que cifra la conexión web (HTTPS) mediante un certificado; diferencia entre certificado emitido por una autoridad y uno autofirmado.

- SAN Subject Alternative Names

Campo del certificado que indica qué nombres de dominio están cubiertos por ese certificado.

Equipo de trabajo :

**Vanessa Meloni
Eduardo Martin
Alejandra Marin
David Nuñez**

