# Formato de Auditoría OSINT: Reconocimiento Pasivo de Dominio

## Introducción

Objetivo: Realizar un reconocimiento pasivo completo de un dominio utilizando dnsdumpster.com, centrolops.net, FOCA, Shodan, Google Dorks y otras herramientas de OSINT.  
Llena cada sección con la información obtenida durante la actividad.

## 1. Mapeo DNS y Subdominios

Dominio objetivo: https://www.fiestamericanatravelty.com/

Fecha de análisis: 15-06-2025

1.1 Subdominios encontrados:

|  |  |  |  |
| --- | --- | --- | --- |
| Subdominio | IP | TTL | Ubicación geográfica |
| trk.notify.fiestamericanatravelty.com | 52.71.250.148 | 3600s | AMAZON-AES United States |

1.2 Name Servers (NS):

- pdns.2.ultradns.net

- pdns3.ultradns.org

- pdns4.ultradns.org

- pdns5.ultradns.info

Pdns6.ultradns.co.uk

- pdns1.ultradns.net

Ssl.xo7.tech

- amber.ns.cloudflare.com  
- derek.ns.cloudflare.com

1.3 Registros MX (servidores de correo):

- 0 fiestamericanatravelty-com.mail.protection.outlook.com

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

- "v=spf1 ip4:201.149.61.3 ip4:189.199.94.6 ip4:189.204.0.2 include:spf.protection.outlook.com -all"

- "MS=ms76072979"

## 2. WHOIS y Datos de Registro

2.1 Registrar: Akky Online Solutions, S.A. de C.V.

2.2 Fecha de creación: 2022-12-14

2.3 Fecha de expiración: 2025-12-14

2.4 Estado del WHOIS (público/privado): Privado

2.5 Contacto Técnico: https://www.akky.mx/WhoisContact

2.6 Contacto Administrativo: https://www.akky.mx/WhoisContact

## 3. Metadatos de Documentos (FOCA)

3.1 Lista de documentos recuperados (nombre y URL):

|  |  |  |
| --- | --- | --- |
| Nombre de documento | URL | Metadatos clave (Autor, Software, Fechas) |

3.2 Hallazgos relevantes de metadatos:

- Rutas internas encontradas: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

- Autores de documentos: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

- Software y versiones: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## 4. Servicios Expuestos (Shodan)

4.1 Lista de IPs a verificar (extraídas en Sección 1):

- 209.164.5.147 / 8010

4.2 Detalle de servicios expuestos:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP | Puerto | Servicio/Versión | CVE asociadas | Ubicación geográfica |
| 52.71.250.148 | 80, 443 |  |  | Los Angeles, US |

4.3 Observaciones adicionales:

- Puertos críticos expuestos: 8010

- Versiones vulnerables detectadas: -

## 5. Hallazgos con Google Dorks

5.1 Consultas utilizadas y resultados encontrados:

|  |  |
| --- | --- |
| Consulta Dork | URL/Resultado encontrado |
| site:fiestamericanatravelty.com | <https://packages.fiestamericanatravelty.com/>  <https://paquetes.fiestamericanatravelty.com/>  <https://www.fiestamericanatravelty.com/ofertas>  <https://www.fiestamericanatravelty.com/blog>  <https://www.fiestamericanatravelty.com/contacto>  <https://www.fiestamericanatravelty.com/hotfat>  <https://www.fiestamericanatravelty.com/en>  <https://www.fiestamericanatravelty.com/homesandresidences>  <https://www.fiestamericanatravelty.com/accesibilidad>  <https://www.fiestamericanatravelty.com/curamoria> |
| allintext:"contraseña"site:fiestamericanatravelty.com | <https://www.fiestamericanatravelty.com/fiesta-americana-funeeq/privacy-policy>  <https://autos.fiestamericanatravelty.com/ayuda/> |
|  |  |

5.2 Descripción de riesgos de cada hallazgo:

- Hallazgo 1: Permite ver todo el contenido indexado públicamente del dominio.

- Hallazgo 2: Indica que hay páginas que contienen la palabra "password" en su texto visible.

- Hallazgo 3: Facilita el mapeo de la estructura web para futuros ataques.

## 6. Recomendaciones de Hardening Inicial

Basado en los hallazgos anteriores, sugerir medidas para mejorar la seguridad:

1. Controlar la indexación pública.

2. Prevenir la exposición de información sensible.

3. Protección de paneles administrativos y login.

4. Implementar registros DNS y correo seguros

5. Monitoreo Continuo

## 7. Conclusión

Resumen de los hallazgos más relevantes y lecciones aprendidas:

El análisis reveló que el sitio usa Cloudflare para proteger su infraestructura, pero carece de configuraciones básicas para proteger el correo electrónico y controlar qué información se muestra públicamente. Esto puede facilitar que datos sensibles o accesos importantes queden expuestos. La lección principal es que, además de usar servicios de seguridad, es vital gestionar bien el contenido visible y proteger los datos para evitar riesgos innecesarios.