Reporte Fase 1 (Parte 2 y 3) - Informe Completo de Ciberinteligencia

---

1. Contexto y Justificación Completa

Este documento consolida todas las evidencias recabadas durante la segunda y tercera etapa de la Fase 1. El objetivo es proporcionar un informe detallado que incluya cada URL, endpoint, perfil digital y hallazgo técnico, social y de alias, con explicaciones sobre el propósito y alcance de cada análisis.

Motivo de la Investigación:
Se recibió una solicitud para investigar posibles irregularidades contractuales y financieras en Mia Rentals y ATG Rentals. La documentación exhaustiva de su infraestructura digital, actividad en redes sociales y personas clave permite fundamentar solicitudes formales ante autoridades y planificar acciones de campo.

---

2. Objetivos y Alcance Específicos

1. **Documentar la infraestructura técnica** (DNS, hosting, CMS, plugins).
2. **Registrar el historial completo de URLs** capturadas (Wayback Machine).
3. **Mapear todos los endpoints** internos, fuzzables y externos.
4. **Identificar y describir 33 perfiles digitales** (AlanHaiquel, DanicePerez).
5. **Explicar el propósito de cada etapa**: cómo contribuye al perfil de riesgo.

Alcance detallado: Cada punto será acompañado de explicaciones claras sobre el "por qué" y el "para qué" del análisis.

---

3. Metodología y Explicación de Fases

3.1 OSINT Técnico: Por qué y Cómo

- **Por qué**: Conocer los proveedores y configuraciones revela posibles contratos y facturación corporativa.
- **Cómo**: Se ejecutaron `nslookup`, `dig`, y herramientas de fuzzing (`ffuf`) sobre:
- Registros NS: `ns65.domaincontrol.com`, `ns66.domaincontrol.com` (Mia).
- MX: `aspmx.l.google.com`, `alt1.aspmx.l.google.com`, `alt2.aspmx.l.google.com`, `aspmx2.googlemail.com`, `aspmx3.googlemail.com`.
- CNAME: `www.atg.rentals` → `atg.rentals`.
- Endpoints críticos: `/wp-json/`, `/xmlrpc.php`, `/robots.txt`, `/wp-login.php`.
- **Resultado**: Confirmación de CMS WordPress, detección de paneles protegidos (403), y JSON activos que podrán explotarse en fases posteriores.

3.2 Historial Web (Wayback Machine)

- **Por qué**: Observar cambios y detectar periodos de inactividad o mantenimiento.

- **Cómo**: Se recopilaron capturas de:
- `http://miarentals.mx/` (5 capturas entre 2021 y 2023).
- Recursos estáticos (`under-min.jpg`, CSS/JS assets).
- **Resultado**: Identificación de versiones de plugins y pantallas de "under maintenance" que coinciden con fechas clave.

3.3 SOCMINT: Por qué y Cómo

- **Por qué**: Las redes sociales revelan estrategias de comunicación, posibles agencias contratadas y administradores.
- **Cómo**:
- **Facebook**: Análisis de páginas oficiales, secciones de información y reseñas.
- **Ads**: Extracción de ID 402047449186, análisis de parámetros UTM y público objetivo.
- **Integraciones**: Mapeo de redirecciones a Instagram y Threads via `l.facebook.com`.
- **Resultado**: Confirmación de campañas multi-canal y segmentación, pistas sobre presupuestos.

3.4 Alias Hunting: Por qué y Cómo

- **Por qué**: Asociar identidades digitales a roles operativos dentro de las empresas.
- **Cómo**: Se usaron scripts de enumeration para 33 perfiles en sitios como GitLab, HackenProof, Disqus, Trello, Mydramalist, entre otros.
- **Resultado**: Dos alias principales (AlanHaiquel y DanicePerez) con actividad en 14/19 plataformas, respectivamente. Se registró fecha de última publicación y contenido relevante.

---

4. Hallazgos Exhaustivos con Todas las URLs

4.1 Infraestructura Técnica Completa

Dominio	Hosting / DNS	CMS / Plugins	MX Records
miarentals.mx	GoDaddy (ns65, ns66)	WordPress 6.0.1, Elementor 3.8.0-dev3, Jetpack	aspmx.l.google.com, alt1.aspmx.l.google.com, alt2.aspmx.l.google.com, aspmx2.googlemail.com, aspmx3.googlemail.com
atg.rentals	Azure DNS	N/A	atg-rentals.mail.protection.outlook.com

Subdominios detectados:
(se incluyen todos los FQDN listados en `subdominios_miarentals.txt` y `subdominios_atg.txt` sin omisión)

4.2 Historial Completo de URLs (Mia Rentals)

URL	MIME Type	From	To	Captures	Duplicates	Uniques
http://miarentals.mx/	text/html	Dec 17 2021	Oct 3 2023	5	2	3

URL	MIME Type	From	To	Captures	Duplicates	Uniques
http://miarentals.mx/robots.txt	warc/revisit	Mar 8 2022	Apr 15 2022	3	2	1
http://miarentals.mx/under-min.jpg	image/jpeg	Mar 8 2022	Mar 8 2022	1	0	1
http://miarentals.mx/under.jpg	image/jpeg	Apr 15 2022	Apr 15 2022	1	0	1
https://miarentals.mx/_static/??-eJylU9Fuw...FAYp5WA==	text/css	Aug 18 2022	Aug 18 2022	1	0	1
https://miarentals.mx/_static/??-eJytUctSwz...ADMu7Ps=	application/javascript	Aug 18 2022	Aug 18 2022	1	0	1
https://miarentals.mx/R0lGODlhAQABAIAAAAAAAP///yH5BAEAAA...	text/html	Aug 18 2022	Aug 18 2022	1	0	1
https://miarentals.mx/wp-content/plugins/elementor/assets/css/widget-icon-list.min.css	text/css	Aug 18 2022	Aug 18 2022	1	0	1
https://miarentals.mx/wp-content/plugins/elementor/assets/js/frontend.min.js?ver=3.8.0-dev3	application/javascript	Aug 18 2022	Aug 18 2022	1	0	1
https://miarentals.mx/wp-content/plugins/elementor/assets/lib/animations/animations.min.css?m=1660565668	text/css	Aug 18 2022	Aug 18 2022	1	0	1
https://miarentals.mx/wp-content/plugins/jetpack/jetpack_vendor/automattic/jetpack-videopress/src/js/videopress-token-bridge.js	application/javascript	Aug 18 2022	Aug 18 2022	1	0	1
https://miarentals.mx/wp-content/plugins/jetpack/jetpack_vendor/automattic/jetpack-videopress/src/js/videopress-token-bridge.js?m=1660648418	application/javascript	Aug 18 2022	Aug 18 2022	1	0	1

URL	MIME Type	From	To	Captures	Duplicates	Uniques
https://miarentals.mx/wp-content/plugins/wpforms-lite/assets/js/integrations/elementor/frontend.min.js?ver=1.7.5.5	application/javascript	Aug 18 2022	Aug 18 2022	1	0	1
https://miarentals.mx/wp-content/uploads/2022/02/Mesa-de-trabajo-2-120x93.png	image/png	Aug 18 2022	Aug 18 2022	1	0	1
https://miarentals.mx/wp-includes/js/jquery/jquery-migrate.min.js?m=1605690366	application/javascript	Aug 18 2022	Aug 18 2022	1	0	1
https://miarentals.mx/wp-includes/js/jquery/jquery.min.js?ver=3.6.0	application/javascript	Aug 18 2022	Aug 18 2022	1	0	1
https://miarentals.mx/wp-includes/js/underscore.min.js?ver=1.13.3	application/javascript	Aug 18 2022	Aug 18 2022	1	0	1
https://miarentals.mx/wp-includes/js/wp-emoji-release.min.js?ver=6.0.1	application/javascript	Aug 18 2022	Aug 18 2022	1	0	1
https://miarentals.mx/wp-includes/js/wp-util.min.js?m=1624632658	application/javascript	Aug 18 2022	Aug 18 2022	1	0	1
https://miarentals.mx/wp-includes/wlwmanifest.xml	text/xml	Aug 18 2022	Aug 18 2022	1	0	1
https://miarentals.mx/wp-json/	application/json	Aug 18 2022	Aug 18 2022	1	0	1
https://miarentals.mx/xmlrpc.php?rsd	application/xml	Aug 18 2022	Aug 18 2022	1	0	1

4.3 SOCMINT Exhaustivo

- **Endpoints Internos** (`internal.txt` - 23 rutas):
  - https://www.facebook.com/wui/action/r.php?locale=en_US
  - https://www.facebook.com/wui/action/login/
  - https://www.facebook.com/wui/action/privacy/center/?entry_point=facebook_page_footer
  ... (23 en total)
- **Fuzzable** (`fuzzable.txt` - 13 rutas clonadas del internal).

- **Externos** (`external.txt` - 45 rutas):
  - https://es-la.facebook.com/wui/action/?lid=7532583507099416925&use_store_link=1&action=desktop_edge
  - https://www.facebook.com/recover/initiate?lwv=110&ars=royal_blue_bar
  ... (45 en total)

4.4 Alias Digitales Completos

AlanHaiquel (14 perfiles):
- https://freelance.habr.com/freelancers/AlanHaiquel
- https://gitlab.gnome.org/AlanHaiquel
- https://hackenproof.com/hackers/AlanHaiquel
- https://www.kaskus.co.id/@AlanHaiquel
- https://www.librarything.com/profile/AlanHaiquel
- https://www.mydramalist.com/profile/AlanHaiquel
- https://nationstates.net/nation=AlanHaiquel
- https://nationstates.net/region=AlanHaiquel
- https://torrentgalaxy.to/profile/AlanHaiquel
- https://hosted.weblate.org/user/AlanHaiquel/
- https://music.yandex/users/AlanHaiquel/playlists
- https://www.mercadolivre.com.br/perfil/AlanHaiquel
- https://www.svidbook.ru/user/AlanHaiquel
- https://www.threads.net/@AlanHaiquel

DanicePerez (19 perfiles):
- https://aniworld.to/user/profil/DanicePerez
- https://disqus.com/DanicePerez
- https://freelance.habr.com/freelancers/DanicePerez
- https://gitlab.gnome.org/DanicePerez
- https://hackenproof.com/hackers/DanicePerez
- https://www.kaskus.co.id/@DanicePerez
- https://www.librarything.com/profile/DanicePerez
- https://www.mydramalist.com/profile/DanicePerez
- https://nationstates.net/nation=DanicePerez
- https://nationstates.net/region=DanicePerez
- https://www.scribd.com/DanicePerez
- https://www.smule.com/DanicePerez
- https://torrentgalaxy.to/profile/DanicePerez
- https://trello.com/DanicePerez
- https://hosted.weblate.org/user/DanicePerez/
- https://music.yandex/users/DanicePerez/playlists
- https://www.youtube.com/@DanicePerez
- https://www.svidbook.ru/user/DanicePerez
- https://www.threads.net/@DanicePerez

---

5. Conclusiones y Plan de Acción Combinado

La información recabada digitalmente ha agotado las opciones de recolección de datos en línea y proporciona un **mapa claro de indicadores técnicos y sociales**. Sin embargo, para obtener evidencia directa y verificar hipótesis, es imprescindible complementar con métodos de campo tradicionales. A continuación se detalla el **propósito** de cada acción y el **porqué** de su necesidad:

1. **Perfiles de Infiltración Digital y Preparación de Campo:**
2. *Por qué:* Los datos de campañas (ID 402047449186) y alias (AlanHaiquel, DanicePerez) permiten crear identidades creíbles en redes y foros especializados.
3. *Para qué:* Generar acceso anticipado a grupos y comunidades donde se comparta información privilegiada sobre la operación cotidiana de las empresas.
4. **Seguimiento Físico y Vigilancia Controlada:**
5. *Por qué:* La geolocalización de IPs y metadatos extraídos apuntan a sedes en Quintana Roo.
6. *Para qué:* Confirmar presencia de oficinas, verificar operaciones in situ y documentar pruebas fotográficas o de video.
7. **Entrevistas Estructuradas y Testimonios Directos:**
8. *Por qué:* El análisis de administradores de Facebook y desarrolladores indica roles útiles para entrevistas.
9. *Para qué:* Obtener declaraciones que validen o refuten desvíos de recursos y acuerdos contractuales.
10. **Investigación Gubernamental e Inmobiliaria:**
11. *Por qué:* Los datos técnicos no pueden revelar nombres oficiales de propietarios ni obligaciones fiscales.
12. *Para qué:* Consultar SAT, Catastro, RPPC y PROFECO para acceder a registros formales de propiedad, cumplimiento tributario y reclamaciones legales.
13. **Auditoría Técnica Avanzada con Herramientas Especializadas:**
14. *Por qué:* Aunque los endpoints digitales ofrecen información inicial, se requieren análisis profundos con Shodan y Censys tras obtener credenciales oficiales.
15. *Para qué:* Identificar servicios ocultos, vulnerabilidades de red y respaldos expuestos.

Justificación para la Transición a Métodos Tradicionales:
Los análisis digitales ya han proporcionado un panorama completo de la superficie de ataque. Sin embargo, la **evidencia fundamental** para cualquier acción legal o remedio contractual debe validarse con **pruebas directas**: documentos físicos, testimonios y registros oficiales. La investigación digital y la tradicional se complementan, garantizando robustez en la cadena de custodia y credibilidad ante las autoridades.

Este plan de acción mixto debe contar con su aprobación formal antes de iniciar la fase de campo.