INDIVIDUAL: Auditoría de Identidad Digital y Huella en Internet (Ethical Profiling)

- Objetivo: José Luis Godoy Khattaoui
- Integrante: Javier Calvillo Acebedo
- Fecha(s) de investigación: [2026-01-31 a 2026-02-01]

1. Resumen ejecutivo

Objetivo. Determinar qué información pública existía (antes del incidente supuesto) que podría haber facilitado la fase de reconocimiento de un atacante: identidades digitales, contactos, dominios/subdominios, huella documental (metadatos), menciones públicas y exposiciones derivadas.

Hallazgos clave (3-7 bullets). - Correo electrónico comprometido en brecha conocida (HIBP): permite reutilización de contraseñas en otros servicios. - Identidades digitales vinculadas a través de Google Services: canal de YouTube, perfil en Google, y reseñas en Google Maps. - Información de ubicación y empleadores anterior: geolocalización a San Fernando y empresas previas deducibles. - Perfil corporativo con posts históricos: exposición de actividades previas a través de Wayback Machine.

Riesgo global (una frase). - Alto por convergencia de datos personales en servicios Google interconectados e historial accesible vía Wayback Machine; brecha anterior facilita suplantación.

Recomendaciones prioritarias (3-5 bullets). - Cambiar contraseña y habilitar autenticación de dos factores en todos los servicios Google (Gmail, YouTube, Maps). - Revisar y configurar privacidad de Google y limitar datos públicos en Google Maps. - Monitorizar aparición en futuras brechas y revisar otros servicios con la misma dirección de correo. - Documentar historial en Wayback Machine para servicios propios y considerar solicitud de eliminación si es posible.

2. Alcance, supuestos y reglas de compromiso

Alcance. Solo OSINT pasivo sobre la entidad (y su huella pública asociada). No se incluye investigación individual (apartado b).

Fuentes permitidas (ejemplos). Motores de búsqueda, hemeroteca, registros públicos, perfiles públicos en RRSS, repositorios públicos, documentos públicos, Wayback/archivos, bases de datos de brechas.

Regla crítica. Prohibida cualquier acción activa: escaneos, enumeración directa de servicios, pruebas de login, interacción con formularios, generación de tráfico hacia los sistemas objetivo.

Minimización y privacidad. - Evitar incluir datos personales innecesarios. - Si aparecen datos personales de terceros (p. ej., correos de empleados), aplicar reducción: mostrar solo lo imprescindible o enmascarar parcialmente cuando no aporte valor al riesgo.

3. Metodología (ciclo OSINT)

Esta sección describe el proceso seguido según el ciclo OSINT: planificación, fuentes, adquisición, procesamiento, análisis y difusión.

3.1 Planificación y dirección

- Preguntas guía (ejemplos):
  - ¿Qué dominios y marcas usa la entidad?
  - ¿Existen patrones de email/usuarios visibles públicamente?
  - ¿Existen documentos públicos con metadatos reveladores?
  - ¿Hay menciones de tecnologías, proveedores, sedes, organigrama o personal?
  - ¿La entidad aparece asociada a brechas pasadas o leaks públicos?
- Criterios de priorización:
  - Impacto potencial en ingeniería social.
  - Reutilización de credenciales/patrones.
  - Exposición de infraestructura por huella documental/histórica.
- Ventana temporal:
  - Consulta realizada en: 2026-02-01
  - Evidencias archivadas en: `evidencias/` (todas deben quedar enlazadas en el informe).

3.2 Identificación de fuentes

Tabla de fuentes (añadir/quitar según aplique):

Categoría	Fuente/Herramienta	Qué se busca	Notas (pasivo)

Categoría	Fuente/Herramienta	Qué se busca	Notas (pasivo)
Buscadores	Google Search / Epieos	correo, identidad digital	solo lectura en resultados
Archivo web	Wayback Machine (Archive.org)	versiones antiguas perfiles	solo lectura
Brechas	Have I Been Pwned (HIBP)	apariciones en leaks	consulta pasiva de BDD
RRSS	YouTube (público)	canal, videos, actividad	solo contenido público
RRSS	Google Maps (público)	reseñas, ubicaciones	solo lectura de datos públicos
Servicios	Google (vía Wayback)	perfil histórico, posts	acceso a snapshots archivados

3.3 Adquisición (recopilación)

- Consultas realizadas (resumen):
  - Búsqueda del correo en Have I Been Pwned
  - Búsqueda de datos asociados al correo en Epieos
  - Búsqueda de links de servicios Google
  - Búsqueda del perfil en Google Plus Archive vía Wayback Machine
  - Búsqueda del canal de YouTube asociado al perfil
  - Búsqueda de reseñas y ubicación en Google Maps
- Evidencias:
  - Guardar capturas o PDFs en `evidencias/` con nombres: `YYYY-MM-DD_fuente_tema.ext`
  - Registrar URL (y, cuando sea útil, captura) y fecha de acceso en cada hallazgo.
  - Toda evidencia mencionada en el informe debe estar enlazada (URL y/o ruta relativa a `evidencias/`).

3.4 Procesamiento y organización

- Normalización:
  - Deduplicación de correos/teléfonos/dominios.
  - Agrupación por categoría (contacto, identidad, infra, documentos).
- Criterios de calidad:
  - Fiabilidad de la fuente (primaria vs. terciaria).
  - Fecha y vigencia (actual vs. histórico).
  - Corroboración cruzada (>= 2 fuentes cuando sea posible).

3.5 Análisis e interpretación

- Correlaciones (ejemplos):
  - Patrones de email + nombres de empleados + roles (posible spear phishing).
  - Documentos públicos -> metadatos -> nombres de usuario/software.
  - Dominios/subdominios históricos -> superficies olvidadas.
- Valoración de riesgo: usar una escala simple.
  - Alto: facilita acceso/engaño de alta probabilidad o alto impacto.
  - Medio: aporta información útil, pero requiere pasos adicionales.
  - Bajo: información marginal o muy genérica.

3.6 Difusión

- Este informe resume hallazgos, evidencia y recomendaciones accionables.
- Presentación clara para audiencias técnicas y no técnicas.

4. Herramientas utilizadas

Herramienta	Tipo	Uso concreto	Salida/evidencia
Have I Been Pwned (HIBP)	Base de datos de brechas	Verificar compromiso de correo	`2026-02-01_hibp_consulta.png`
Epieos	Búsqueda de datos de correo	Obtener información asociada a email	`2026-02-01_google_busqueda0.png`
Google Search	Motor de búsqueda	Búsqueda de identidades vinculadas	`2026-02-01_google_busqueda1.png`
Wayback Machine (Archive.org)	Archivo web	Acceso a Google Plus histórico	`2026-02-01_google_busqueda3.png`
YouTube	Red social (RRSS)	Localización de canal personal	`2026-02-01_google_busqueda4.png`

Herramienta	Tipo	Uso concreto	Salida/evidencia
Google Maps	Servicio de localización	Consulta de reseñas y ubicaciones	2026-02-01_google_busqueda2.png, 2026-02-01_google_busqueda5.png, 2026-02-01_google_busqueda6.png

5. Resultados (hallazgos)

5.1 Identidades digitales (nicks, perfiles, cuentas)

A-01: Canal de YouTube

Campo	Contenido
ID	A-01
Categoría	Identidad / RRSS
Descripción	Canal de YouTube personal activo con múltiples videos publicados
Evidencia	2026-02-01_google_busqueda4.png,
Fecha evidencia	2026-02-01
Impacto	Vinculación de identidad real con actividad online; vector para ingeniería social y profiling
Riesgo	Medio
Recomendación	Revisar configuración de privacidad del canal; considerar cambiar URL de canal si es identificable

A-02: Perfil Google+ (archivado)

Campo	Contenido
ID	A-02
Categoría	Identidad / RRSS
Descripción	Perfil de Google+ con posts históricos accesibles vía Wayback Machine; posts coinciden con actividad YouTube
Evidencia	2026-02-01_google_busqueda0.png , 2026-02-01_google_busqueda1.png
Fecha evidencia	2026-02-01
Impacto	Exposición histórica de actividades; confirmación de identidad vinculada; datos persistentes en archivos web
Riesgo	Medio
Recomendación	Solicitar eliminación de datos a Archive.org si es posible; revisar policy de datos históricos

5.2 Datos de contacto (emails, teléfonos, estructuras)

A-03: Ubicación asociada

Campo	Contenido
ID	A-04
Categoría	Contacto / Ubicación
Descripción	Ubicación deducida mediante reseñas de Google Maps en 2 restaurantes de San Fernando e interacción con tienda Orange
Evidencia	2026-02-01_google_busqueda5.png, 2026-02-01_google_busqueda6.png
Fecha evidencia	2026-02-01
Impacto	Geolocalización; permite deducir ubicación habitual e historial de movimientos; facilita ingeniería social
Riesgo	Medio
Recomendación	Limitar datos de ubicación en Google Maps; no publicar lugares de trabajo/frecuentes; revisar reseñas antiguas

5.3 Dominios, subdominios y huella DNS (pasivo)

(No aplicable en este caso: la investigación se centró en identidades en servicios Google, no en propiedades de dominio personal.)

5.4 Huella documental y metadatos (documentos públicos)

A-04: Posts históricos en Google+

Campo	Contenido
ID	A-05
Categoría	Documentos / Huella histórica

Campo	Contenido
Descripción	Posts históricos de Google+ accesibles via Wayback Machine; demuestran actividad y contenido anterior
Evidencia	`2026-02-01_google_busqueda3.png`
Fecha evidencia	2026-02-01
Impacto	Exposición de historial personal; persistencia de datos en archivos web públicos
Riesgo	Bajo-Medio
Recomendación	Verificar contenido accesible; solicitar derecho al olvido a Archive.org si procede

5.5 Brechas y filtraciones (consulta pasiva)

A-06: Correo comprometido en brecha HIBP

Campo	Contenido
ID	A-06
Categoría	Brechas / Filtraciones
Descripción	Correo electrónico personal registrado en Have I Been Pwned; comprometido en brecha anterior
Evidencia	`2026-02-01_hibp_consulta.png` (evidencia en HIBP; base de datos pública)
Fecha evidencia	2026-02-01
Impacto	Alto: facilita reutilización de contraseña; permite deducción de patrón de credenciales; acceso a cuentas vinculadas
Riesgo	Alto
Recomendación	Cambiar contraseña urgentemente; Activar 2FA en Gmail y servicios críticos; Revisar acceso a cuentas reciente; Monitorizar futuras brechas

6. Resumen de riesgos

ID	Hallazgo (resumen)	Riesgo	Prioridad	Acción recomendada
A-03	Correo comprometido en brecha	Alto	P1	Cambiar contraseña + 2FA inmediato
A-06	Datos de brecha HIBP	Alto	P1	Monitorizar y auditar acceso
A-04	Geolocalización deducida	Medio	P2	Limitar datos de ubicación en Maps
A-01	Canal YouTube identificable	Medio	P2	Revisar privacidad y configuración
A-02	Perfil Google+ histórico	Medio	P2	Solicitar eliminación a Archive.org
A-05	Posts históricos accesibles	Bajo	P3	Revisar contenido y privacidad

7. Conclusiones

- **Convergencia de identidades en ecosistema Google**: La exposición principal radica en la interconexión de múltiples servicios Google (Gmail, YouTube, Maps, Google) bajo una única identidad. Un atacante aprovecha un único punto de compromiso (correo + brecha HIBP) para acceder a toda la huella digital.
- **Persistencia de datos en Wayback Machine**: Aunque Google+ fue desmantelado, sus datos persisten en Archive.org, permitiendo acceso indefinido al historial de actividades. Esto amplifica el riesgo de profiling y manipulación social.
- **Información de ubicación y patrones de vida**: Las reseñas de Google Maps, aunque parecen secundarias, revelan ubicación habitual, lugares frecuentados e historial laboral. Esto facilita ataques de ingeniería social hiperpersonalizados o acoso.
- **Eficacia del OSINT pasivo**: La investigación demuestra que con solo un correo electrónico y herramientas OSINT pasivas públicas, un atacante puede construir un perfil muy completo sin interacción activa con sistemas objetivo.

8. Recomendaciones

Urgente - Cambiar contraseña de Gmail e inmediatamente habilitar Verificación en 2 pasos (2FA). - Revisar configuración de privacidad en YouTube: cambiar visibilidad de canal a privado si no es comercial; ocultar lista de reproducción. - Limpiar Google Maps: eliminar o privatizar reseñas antiguas; desactivar historial de ubicación; revisar ubicación del hogar. - Verificar sesiones activas en Google Account y terminar sesiones desconocidas. - Cambiar contraseña en otros servicios si reutilizaban patrón similar.

Medio plazo - Implementar gestor de contraseñas y usar contraseñas únicas por servicio. - Revisar y limitar información personal en todas las RRSS. - Configurar alertas de brechas: suscribirse a Have I Been Pwned para monitorización. - Auditoría completa de aplicaciones de terceros conectadas a Google Account.

Mejora continua - Revisar mensualmente configuración de privacidad en servicios Google. - Realizar OSINT trimestral sobre sí mismo para

identificar nueva información pública. - Implementar política de no publicación de ubicación, empresas anteriores ni patrones de vida en RRSS. - Educar sobre riesgos de ingeniería social: datos públicos facilitan suplantación y spear phishing.

9. Anexos

9.1 Registro de fuentes

Fuente	URL	Fecha acceso	Nota
Have I Been Pwned	https://haveibeenpwned.com	2026-02-01	Consulta de brecha del correo
Epieos	https://epieos.com	2026-02-01	Búsqueda de datos asociados al email
Google Search	https://www.google.com	2026-02-01	Búsquedas múltiples de identidades vinculadas
Wayback Machine	https://web.archive.org	2026-02-01	Acceso a snapshots de Google+
YouTube	https://www.youtube.com	2026-02-01	Búsqueda de canal personal
Google Maps	https://maps.google.com	2026-02-01	Búsqueda de reseñas y ubicaciones

9.2 Consultas (dorks) empleadas

(Consultas realizadas en OSINT pasivo. Todas sobre datos ya públicos sin interacción activa con sistemas.)- `aldimeneira91@gmail.com` en Have I Been Pwned- `aldimeneira91@gmail.com` en Epieos- `\"Jose Luis Godoy\" Google+`- `\"Aldimeneira\" YouTube`- `\"Aldimeneira\"`

9.3 Evidencias (índice)

- `evidencias/`:
  - `2026-02-01_hibp_consulta.png` - Captura de Have I Been Pwned mostrando correo comprometido en brecha
  - `2026-02-01_google_busqueda0.png` - Búsqueda inicial y datos de correo en Epieos
  - `2026-02-01_google_busqueda2.png` - Links adicionales y servicios Google vinculados
  - `2026-02-01_google_busqueda4.png` - Perfil Google+ archivado con posts coincidentes con YouTube
  - `2026-02-01_google_busqueda5.png` - Canal de YouTube personal encontrado
  - `2026-02-01_google_busqueda6.png`(../evidencias/2026-02-01_google_busqueda5.png)(../evidencias/2026-02-01_google_busqueda6.png) - Google Maps con 4 reseñas: Orange y restaurantes San Fernando