

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)
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/engañeo 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

Herramienta	Tipo	Uso concreto	Salida/evidencia
YouTube	Red social (RRSS)	Localizaci3n de canal personal	2026-02-01_google_busqueda4.png
Google Maps	Servicio de localizaci3n	Consulta de rese±as 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
Categor�a	Identidad / RRSS
Descripci3n	Canal de YouTube personal activo con m�ltiples videos publicados
Evidencia	2026-02-01_google_busqueda4.png,
Fecha evidencia	2026-02-01
Impacto	Vinculaci3n de identidad real con actividad online; vector para ingenier�a social y profiling
Riesgo	Medio
Recomendaci3n	Revisar configuraci3n de privacidad del canal; considerar cambiar URL de canal si es identificable

A-02: Perfil Google+ (archivado)

Campo	Contenido
ID	A-02
Categor�a	Identidad / RRSS
Descripci3n	Perfil de Google+ con posts hist3ricos accesibles v�a 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	Exposici3n hist3rica de actividades; confirmaci3n de identidad vinculada; datos persistentes en archivos web
Riesgo	Medio
Recomendaci3n	Solicitar eliminaci3n de datos a Archive.org si es posible; revisar policy de datos hist3ricos

5.2 Datos de contacto (emails, tel fonos, estructuras)

A-03: Ubicaci3n asociada

Campo	Contenido
ID	A-04
Categor�a	Contacto / Ubicaci3n
Descripci3n	Ubicaci3n deducida mediante rese±as de Google Maps en 2 restaurantes de San Fernando e interacci3n con tienda Orange
Evidencia	2026-02-01_google_busqueda5.png, 2026-02-01_google_busqueda6.png
Fecha evidencia	2026-02-01
Impacto	Geolocalizaci3n; permite deducir ubicaci3n habitual e historial de movimientos; facilita ingenier�a social
Riesgo	Medio
Recomendaci3n	Limitar datos de ubicaci3n en Google Maps; no publicar lugares de trabajo/frecuentes; revisar rese±as antiguas

5.3 Dominios, subdominios y huella DNS (pasivo)

(No aplicable en este caso: la investigaci3n se centr  en identidades en servicios Google, no en propiedades de dominio personal.)

5.4 Huella documental y metadatos (documentos p blicos)

A-04: Posts hist3ricos en Google+

Campo	Contenido
-------	-----------

Campo	Contenido
ID	A-05
Categor�a	Documentos / Huella hist�rica
Descripci�n	Posts hist�ricos de Google+ accesibles via Wayback Machine; demuestran actividad y contenido anterior
Evidencia	2026-02-01_google_busqueda3.png
Fecha evidencia	2026-02-01
Impacto	Exposici�n de historial personal; persistencia de datos en archivos web p�blicos
Riesgo	Bajo-Medio
Recomendaci�n	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
Categor�a	Brechas / Filtraciones
Descripci�n	Correo electr�nico personal registrado en Have I Been Pwned; comprometido en brecha anterior
Evidencia	2026-02-01_hibp_consulta.png (evidencia en HIBP; base de datos p�blica)
Fecha evidencia	2026-02-01
Impacto	Alto: facilita reutilizaci�n de contrase�as; permite deducci�n de patr�n de credenciales; acceso a cuentas vinculadas
Riesgo	Alto
Recomendaci�n	Cambiar contrase�a urgentemente; Activar 2FA en Gmail y servicios cr�ticos; Revisar acceso a cuentas reciente; Monitorizar futuras brechas

6. Resumen de riesgos

ID	Hallazgo (resumen)	Riesgo	Prioridad	Acci�n recomendada
A-03	Correo comprometido en brecha	Alto	P1	Cambiar contrase�a + 2FA inmediato
A-06	Datos de brecha HIBP	Alto	P1	Monitorizar y auditar acceso
A-04	Geolocalizaci�n deducida	Medio	P2	Limitar datos de ubicaci�n en Maps
A-01	Canal YouTube identificable	Medio	P2	Revisar privacidad y configuraci�n
A-02	Perfil Google+ hist�rico	Medio	P2	Solicitar eliminaci�n a Archive.org
A-05	Posts hist�ricos accesibles	Bajo	P3	Revisar contenido y privacidad

7. Conclusiones

- **Convergencia de identidades en ecosistema Google:** La exposici n principal radica en la interconexi n de m ltiples servicios Google (Gmail, YouTube, Maps, Google) bajo una  nica identidad. Un atacante aprovecha un  nico 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 manipulaci n social.
- **Informaci n de ubicaci n y patrones de vida:** Las rese as de Google Maps, aunque parecen secundarias, revelan ubicaci n habitual, lugares frecuentados e historial laboral. Esto facilita ataques de ingenier a social hiperpersonalizados o acoso.
- **Eficacia del OSINT pasivo:** La investigaci n demuestra que con solo un correo electr nico y herramientas OSINT pasivas p blicas, un atacante puede construir un perfil muy completo sin interacci n activa con sistemas objetivo.

8. Recomendaciones

Urgente - Cambiar contrase a de Gmail e inmediatamente habilitar Verificaci n en 2 pasos (2FA). - Revisar configuraci n de privacidad en YouTube: cambiar visibilidad de canal a privado si no es comercial; ocultar lista de reproducci n. - Limpiar Google Maps: eliminar o privatizar rese as antiguas; desactivar historial de ubicaci n; revisar ubicaci n del hogar. - Verificar sesiones activas en Google Account y terminar sesiones desconocidas. - Cambiar contrase a en otros servicios si reutilizaban patr n similar.

Medio plazo - Implementar gestor de contrase as y usar contrase as  nicas por servicio. - Revisar y limitar informaci n personal en todas las RRSS. - Configurar alertas de brechas: suscribirse a Have I Been Pwned para monitorizaci n. - Auditor a completa de aplicaciones de

terceros conectadas a Google Account.

Mejora continua - Revisar mensualmente configuración de privacidad en servicios Google. - Realizar OSINT trimestral sobre sÃ mismo para identificar nueva informaciÃ³n pÃblica. - Implementar polÃtica de no publicaciÃ³n de ubicaciÃ³n, empresas anteriores ni patrones de vida en RRSS. - Educar sobre riesgos de ingenierÃa social: datos pÃblicos facilitan suplantaciÃ³n 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	BÃsqueda de datos asociados al email
Google Search	https://www.google.com	2026-02-01	BÃsqueda mÃltiples 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	BÃsqueda de canal personal
Google Maps	https://maps.google.com	2026-02-01	BÃsqueda de reseÃas y ubicaciones

9.2 Consultas (dorks) empleadas

(Consultas realizadas en OSINT pasivo. Todas sobre datos ya pÃblicos sin interacciÃ³n 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 (Ãndice)

- evidencias/:
 - [2026-02-01_hibp_consulta.png](#) - Captura de Have I Been Pwned mostrando correo comprometido en brecha
 - [2026-02-01_google_busqueda0.png](#) - BÃsqueda 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 reseÃas: Orange y restaurantes San Fernando