

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

- Objetivo: JosÃ© Luis Godoy Khattaoui
- Integrante: Javier Calvillo Acebedo
- Fecha(s) de investigaciÃ³n: [2026-01-31 a 2026-02-01]

1. Resumen ejecutivo

Objetivo. Determinar quÃ© informaciÃ³n pÃºblica existÃ¡ (antes del incidente supuesto) que podrÃ¡ haber facilitado la fase de reconocimiento de un atacante: identidades digitales, contactos, dominios/subdominios, huella documental (metadatos), menciones pÃºblicas y exposiciones derivadas.

Hallazgos clave (3-7 bullets). - Correo electrÃ³nico comprometido en brecha conocida (HIBP): permite reutilizaciÃ³n de contraseÃ±as en otros servicios. - Identidades digitales vinculadas a travÃ©s de Google Services: canal de YouTube, perfil en Google, y reseÃ±as en Google Maps. - InformaciÃ³n de ubicaciÃ³n y empleadores anterior: geolocalizaciÃ³n en San Fernando y empresas previas deducibles. - Perfil corporativo con posts histÃ³ricos: exposiciÃ³n de actividades previas a travÃ©s de Wayback Machine.

Riesgo global (una frase). - Alto por convergencia de datos personales en servicios Google interconectados e historial accesible vÃ¡a Wayback Machine; brecha anterior facilita suplantaciÃ³n.

Recomendaciones prioritarias (3-5 bullets). - Cambiar contraseÃ±a y habilitar autenticaciÃ³n de dos factores en todos los servicios Google (Gmail, YouTube, Maps). - Revisar y configurar privacidad de Google y limitar datos pÃºblicos en Google Maps. - Monitorizar apariciÃ³n en futuras brechas y revisar otros servicios con la misma direcciÃ³n de correo. - Documentar historial en Wayback Machine para servicios propios y considerar solicitud de eliminaciÃ³n si es posible.

2. Alcance, supuestos y reglas de compromiso

Alcance. Solo OSINT pasivo sobre la entidad (y su huella pÃºblica asociada). No se incluye investigaciÃ³n individual (apartado b).

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

Regla crÃtica. Prohibida cualquier acciÃ³n activa: escaneos, enumeraciÃ³n directa de servicios, pruebas de login, interacciÃ³n con formularios, generaciÃ³n de trÃ¡jico hacia los sistemas objetivo.

MinimizaciÃ³n y privacidad. - Evitar incluir datos personales innecesarios. - Si aparecen datos personales de terceros (p.ej., correos de empleados), aplicar reducciÃ³n: mostrar solo lo imprescindible o enmascarar parcialmente cuando no aporte valor al riesgo.

3. MetodologÃa (ciclo OSINT)

Esta secciÃ³n describe el proceso seguido segÃºn el ciclo OSINT: planificaciÃ³n, fuentes, adquisiciÃ³n, procesamiento, anÃ¡lisis y difusiÃ³n.

3.1 PlanificaciÃ³n y direcciÃ³n

- Preguntas guÃ¡a (ejemplos):
 - Ãs QuÃ© dominios y marcas usa la entidad?
 - Ãs Existen patrones de email usuarios visibles pÃºblicamente?
 - Ãs Existen documentos pÃºblicos con metadatos reveladores?
 - Ãs Hay menciones de tecnologÃías, proveedores, sedes, organigrama o personal?
 - Ãs La entidad aparece asociada a brechas pasadas o leaks pÃºblicos?
- Criterios de priorizaciÃ³n:
 - Impacto potencial en ingenierÃa social.
 - ReutilizaciÃ³n de credenciales/patrones.
 - ExposiciÃ³n de infraestructura por huella documental/histÃ³rica.
- Ventana temporal:
 - Consulta realizada en: 2026-02-01
 - Evidencias archivadas en: evidencias/ (todas deben quedar enlazadas en el informe).

3.2 IdentificaciÃ³n de fuentes

Tabla de fuentes (aÃ±adir/quitar segÃºn 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
RSS	YouTube (público)	canal, videos, actividad	solo contenido público
RSS	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).
 - Corroborción 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/engañar 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)	LocalizaciÃ³n de canal personal	2026-02-01_google_busqueda4.png
Google Maps	Servicio de localizaciÃ³n	Consulta de reseÃ±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
CategorÃa	Identidad / RRSS
DescripciÃ³n	Canal de YouTube personal activo con mÃºltiples videos publicados
Evidencia	2026-02-01_google_busqueda4.png,
Fecha evidencia	2026-02-01
Impacto	VinculaciÃ³n de identidad real con actividad online; vector para ingenierÃa social y profiling
Riesgo	Medio
RecomendaciÃ³n	Revisar configuraciÃ³n de privacidad del canal; considerar cambiar URL de canal si es identifiable

A-02: Perfil Google+ (archivado)

Campo	Contenido
ID	A-02
CategorÃa	Identidad / RRSS
DescripciÃ³n	Perfil de Google+ con posts histÃricos accesibles vÃa 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	ExposiciÃ³n histÃrica de actividades; confirmaciÃ³n de identidad vinculada; datos persistentes en archivos web
Riesgo	Medio
RecomendaciÃ³n	Solicitar eliminaciÃ³n de datos a Archive.org si es posible; revisar policy de datos histÃricos

5.2 Datos de contacto (emails, telÃ©fonos, estructuras)

A-03: UbicaciÃ³n asociada

Campo	Contenido
ID	A-04
CategorÃa	Contacto / UbicaciÃ³n
DescripciÃ³n	UbicaciÃ³n deducida mediante reseÃ±as de Google Maps en 2 restaurantes de San Fernando e interacciÃ³n con tienda Orange
Evidencia	2026-02-01_google_busqueda5.png, 2026-02-01_google_busqueda6.png
Fecha evidencia	2026-02-01
Impacto	GeolocalizaciÃ³n; permite deducir ubicaciÃ³n habitual e historial de movimientos; facilita ingenierÃa social
Riesgo	Medio
RecomendaciÃ³n	Limitar datos de ubicaciÃ³n en Google Maps; no publicar lugares de trabajo/frecuentes; revisar reseÃ±as antiguas

5.3 Dominios, subdominios y huella DNS (pasivo)

(No aplicable en este caso: la investigaciÃ³n se centrÃ³ en identidades en servicios Google, no en propiedades de dominio personal.)

5.4 Huella documental y metadatos (documentos pÃºblicos)

A-04: Posts histÃricos en Google+

Campo	Contenido

Campo	Contenido
ID	A-05
Categoría	Documentos / Huella histórica
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 respuestas de Google Maps, aunque parecen secundarias, revelan ubicación habitual, lugares frecuentados e historial laboral. Esto facilita ataques de ingeniería social hipersonalizados 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 respuestas 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 configuraciÃ³n de privacidad en servicios Google. - Realizar OSINT trimestral sobre sÃ mismo para identificar nueva informaciÃ³n pÃºblica. - Implementar polÃtica de no publicaciÃ³n de ubicaciÃ³n, empresas anteriores ni patrones de vida en RSS. - Educar sobre riesgos de ingenierÃa social: datos pÃºblicos 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	BÃºsqueda de datos asociados al email
Google Search	https://www.google.com	2026-02-01	BÃºsquedas mÃºltiples 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	BÃºsqueda de canal personal
Google Maps	https://maps.google.com	2026-02-01	BÃºsqueda de reseÃ±as y ubicaciones

9.2 Consultas (dorks) empleadas

(Consultas realizadas en OSINT pasivo. Todas sobre datos ya pÃºblicos 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](#) - BÃºsqueda 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 reseÃ±as: Orange y restaurantes San Fernando