INFORME DE SEGURIDAD

Exposición de datos en Constructores y Punto de Acuerdo

`hastaelfinal.app` y `puntodeacuerdo.info`: alcance real, riesgos y acciones

Fecha del informe	24 de noviembre de 2026
Elaborado para	Equipo de Vente Venezuela / Constructores
Elaborado por	José Rafael Gutiérrez, Senior Full Stack Developer Consultant
Fuentes primarias	VE sin Filtro (vesinfiltro.org, 22 y 23 de noviembre de 2026) y verificación propia pasiva del 24 de noviembre de 2026
Alcance de la verificación	Pasiva: archivo histórico público (Wayback Machine) y navegación normal. Sin fuerza bruta, sin explotación activa y sin evadir controles

0. Resumen

Los endpoints expuestos de `hastaelfinal.app` no estuvieron abiertos solo unos días de noviembre: el Wayback Machine los tiene archivados con datos sensibles **desde julio de 2024**, y esos snapshots siguen públicos aunque el sitio ya esté mitigado.

Ventana de exposición

jul 2024 → nov 2026

Más de dos años, no los días previos al aviso del 21 de noviembre.

Dato más grave

Biometría facial

Plantillas en texto plano. Una contraseña se cambia; una cara no.

Estado actual

Mitigado, no cerrado

Hay defensas nuevas en ambos dominios, pero el archivo histórico sigue público y no se auditaron otras rutas.

1. Qué se reportó

El 21 de noviembre de 2026, un actor de amenaza publicó en un canal de Telegram un método para acceder, **sin autenticación**, a dos endpoints de `hastaelfinal.app`, el backend de Constructores / Monitoreo Ciudadano:

- Un feed RSS que registraba altas de usuarios nuevos en texto plano.
- Un endpoint con información histórica de la plataforma, que incluía datos de participantes del proceso electoral de 2024 y de miembros de Vente Venezuela.

Un día después aparecieron dos fallas similares en `puntodeacuerdo.info`: un feed RSS con los últimos 10 "Puntos de Acuerdo" y su autor, y una página de usuarios identificados por **ID secuencial**. Este es el patrón típico de IDOR: referencias directas a objetos sin control de acceso.

Sitio	Vector	Datos expuestos (según VE sin Filtro)
`hastaelfinal.app`	Feed RSS de altas y endpoint histórico, sin autenticación	Nombre completo, nacionalidad, cédula, correo, teléfono, país de residencia, centro de votación, afiliación política y **plantillas biométricas de reconocimiento facial en texto plano**, generadas a partir de cédula + selfie en el registro
`puntodeacuerdo.info`	Feed RSS y página de usuarios por ID secuencial (IDOR)	Nombre, nacionalidad, cédula, teléfono, organización o comunidad, cargo, presentación personal y parte local del correo

> **LIMITACIÓN RECONOCIDA.** El informe de VE sin Filtro dice: "no podemos confirmar desde cuándo estuvieron expuestos los datos ni si terceros los extrajeron". Además, solo validó los vectores difundidos; no hizo una auditoría completa.

Cronología



Figura 1. Ventana real de exposición frente a la cronología reportada

2. Hallazgo propio: la ventana de exposición es mucho más larga

Usando solo la API pública del Wayback Machine (archive.org), sin tocar el sitio en producción, encontré que crawlers automáticos ya habían archivado estos endpoints **desde 2024**, mucho antes de la publicación en Telegram.

- `https://hastaelfinal.app/rss.xml` y `https://hastaelfinal.app/en/rss.xml` tienen snapshots de **julio a octubre de 2024**, con código de respuesta 200 y contenido `application/rss+xml`.
- El contenido archivado de esos feeds incluye, en texto plano:
  - **Cédulas de votantes usadas como nombre de usuario** (formato `V#########`), visibles en snapshots de septiembre y octubre de 2024.
  - **Tokens de Firebase Cloud Messaging** (notificaciones push) asociados a esas cédulas.

- **ID de dispositivo, modelo de teléfono y sistema operativo** del usuario (por ejemplo, "Infinix HOT 20S", Android).
- Nodos de "centro de votación" con el nombre completo del centro y su geolocalización implícita.

CONCLUSIÓN. El endpoint llevaba **más de un año abierto sin autenticación** antes de que el actor de amenaza lo publicara. No fue un hallazgo reciente de un atacante, sino una falla de configuración heredada, posiblemente desde el ciclo electoral de 2024.

IMPLICACIÓN GRAVE. Ese contenido sigue público hoy en el Wayback Machine, aunque el sitio en producción ya esté mitigado. Archive.org no borra snapshots salvo que el propietario del dominio lo solicite formalmente. Un `robots.txt` retroactivo no sirve; hay que pedir la remoción directamente a archive.org.

Comprobación	Resultado	Lectura
Snapshots históricos de `hastaelfinal.app`	ENCONTRADOS	Julio a octubre de 2024, con datos sensibles
Snapshots históricos de `puntodeacuerdo.info`	NINGUNO	El sitio es más nuevo o nunca fue rastreado; buena noticia relativa
Indexación en Google (búsqueda `site:`)	NO CONCLUYENTE	La búsqueda no devolvió resultados utilizables. Debe verificarse desde Google Search Console del dominio

Acción recomendada inmediata

1. **Pedir a archive.org la eliminación de los snapshots** de `hastaelfinal.app/rss.xml`, `/en/rss.xml` y rutas relacionadas que contengan cédulas, tokens push o datos de dispositivo, mediante su formulario de exclusión o contacto directo.
2. **Revisar Google Search Console** del dominio por URLs indexadas con datos sensibles, y usar la herramienta de eliminación de contenido obsoleto de Google.
3. **Invalidar o rotar los tokens de Firebase Cloud Messaging expuestos.** Son credenciales funcionales, no solo metadatos: si siguen activos, alguien podría intentar enviar notificaciones push suplantando a la app.
4. **Asumir una ventana de exposición de al menos julio de 2024 a noviembre de 2026** al redactar la notificación a los usuarios afectados, no solo "unos días en noviembre".

3. Verificación pasiva en vivo (24 de noviembre de 2026)

Hecha solo con navegación normal, sin fuerza bruta ni explotación activa. Ambos dominios tienen defensas nuevas que no existían antes del 21 de noviembre.

Ruta	Resultado	Lectura
`hastaelfinal.app/feed`, `/rss`	404	Respuesta estándar del sitio

Ruta	Resultado	Lectura
`hastaelfinal.app/rss.xml`	BLOQUEADO	El WAF de Cloudflare responde "Sorry, you have been blocked". Antes del 22 de noviembre esa ruta respondía sin fricción
`puntodeacuerdo.info` (toda la raíz, incluido `/robots.txt`)	CHALLENGE	Detrás de una verificación de bots tipo Cloudflare. Cambio fuerte de postura respecto a antes del incidente

LO QUE CONFIRMA. Hay defensas nuevas activas en ambos dominios que no existían antes del 21 de noviembre.

LO QUE NO CONFIRMA. Que no exista otra ruta, subdominio o endpoint de API equivalente todavía abierto. No se probaron variantes de API, subdominios ni la posible app móvil.

No se intentó evadir el challenge de bots ni probar rutas no documentadas, por estar fuera del alcance acordado.

Siguiente paso técnico (requiere al equipo que administra el servidor)

- Pedir a VE sin Filtro los nombres exactos de los endpoints que reportaron por correo, en vez de que un tercero los adivine desde fuera.
- Revisar los logs del servidor Drupal desde julio de 2024 por accesos no autenticados y en volumen a `/rss.xml`, `/en/rss.xml` y rutas `/node/*`. Eso permitiría estimar cuántas IPs distintas extrajeron el feed antes del 21 de noviembre de 2026.
- Auditoría de seguridad independiente, ya recomendada por VE sin Filtro.

4. Consecuencias y posible mal uso

La gravedad no viene de un dato aislado, sino de la combinación.

Combinación de datos	Riesgo
Cédula + nombre + teléfono + correo	Suplantación de identidad, apertura de líneas o cuentas a nombre de la víctima, y phishing o vishing dirigido con datos reales, mucho más efectivo que el genérico
Centro de votación + afiliación política + membresía en Vente Venezuela	En el contexto venezolano es un dato de riesgo físico y político, no de marketing. Permite construir listas de activistas identificables por ubicación. Hay precedente histórico (listas Tascón y Maisanta) de uso de estos datos para discriminación laboral y represión
Plantilla biométrica facial en texto plano	El dato más difícil de remediar: una contraseña se cambia, una cara no. Si la plantilla es reutilizable contra otros sistemas de verificación facial, abre la puerta a la suplantación biométrica
Tokens FCM + ID de dispositivo (hallazgo propio)	Permiten, en teoría, intentos de manipulación de notificaciones push dirigidas a usuarios concretos identificados por cédula

Combinación de datos	Riesgo
Datos históricos de 2024	El universo de afectados probablemente es mayor que el de quienes se registraron hace poco, porque el feed estuvo abierto desde al menos julio de 2024

USOS PROBABLES POR UN ACTOR MALICIOSO, DE MÁS A MENOS PROBABLE

1. Phishing o spam dirigido con datos reales.
2. Extorsión usando cédula y afiliación política.
3. Venta de la base en mercados de datos.
4. Construcción de perfiles de intimidación.
5. Fraude de identidad con cédula y biometría.

> **EVIDENCIA.** No hay evidencia confirmada de exfiltración masiva ni de venta de los datos, ni por parte de VE sin Filtro ni en esta verificación. Pero un endpoint abierto y automatizable durante más de un año, como muestran los snapshots del Wayback Machine, no deja un rastro fácil de quién lo consultó antes de ser reportado.

5. Consejos para usuarios sobre formularios web

Pensado para difundir entre los usuarios de la plataforma y la comunidad.

Antes de llenar cualquier formulario

- Si pide biometría (selfie + foto de cédula) para algo que no es una gestión financiera o legal regulada, desconfía. Un registro de activismo o una encuesta política no necesitan reconocimiento facial.
- Verifica HTTPS. Es necesario, pero no suficiente: cifra el transporte, no protege contra un backend mal configurado.
- Busca quién es el responsable del tratamiento y si hay una política de privacidad concreta, no genérica.

Minimización de datos

- Si un campo es "opcional" y no te da un beneficio directo, déjalo vacío.
- Para afiliación política o centro de votación, evalúa si el beneficio vale el riesgo de terminar en una lista pública. En contextos de alta exposición, como el activismo o la oposición, ese cálculo pesa distinto.
- Nunca subas copia de tu cédula ni selfies a un formulario que no sea de una entidad regulada (banco o trámite oficial). Un partido, una ONG o una plataforma de "verificación" pueden confirmar tu identidad por medios menos sensibles.

Señales de alerta sin saber programar

- Si cambias un número en la URL (`?id=123` → `?id=124`) y ves datos de otra persona, es un fallo de control de acceso (IDOR). Repórtalo y deja de usar el sitio con datos reales.
- Un feed RSS, un endpoint `/api/...` abierto o un panel de administración accesible sin login son señales de que nadie auditó la seguridad.

Si ya diste tus datos en Constructores o Punto de Acuerdo

- Asume que tu nombre, cédula, teléfono, correo y afiliación están potencialmente comprometidos desde hace tiempo, no solo desde noviembre de 2026.
- Mantente alerta ante phishing o vishing que use esos datos como "prueba de legitimidad".
- Si subiste selfie + cédula: no hay remedio para la plantilla biométrica en sí; vale la pena vigilar posibles fraudes de identidad.

6. Recomendaciones para el equipo técnico

#	Acción	Detalle
1	**Publicar un análisis técnico del alcance real**	Incluir la ventana de exposición desde 2024, no solo los días de noviembre de 2026
2	**Notificar individualmente a los usuarios afectados**	A todos los potencialmente afectados desde julio de 2024 en adelante
3	**Retirar el contenido archivado e indexado**	Pedir la remoción de snapshots sensibles a archive.org y revisar la indexación en Google
4	**Rotar o invalidar los tokens FCM expuestos**	Son credenciales funcionales de notificaciones push
5	**Auditoría de seguridad independiente**	De toda la infraestructura: `hastaelfinal.app`, `puntodeacuerdo.info` y cualquier backend compartido
6	**Rediseñar el registro**	No exigir biometría ni datos sensibles innecesarios, y permitir que cada usuario ajuste su propio nivel de riesgo
7	**Confirmar las rutas exactas con VE sin Filtro**	Para cerrar cualquier variante no descubierta en esta verificación pasiva

ELABORADO POR

José Rafael Gutiérrez

Senior Full Stack Developer Consultant

Teléfono: +57 302 617 8155

Sitio web: jose-gutierrez.com/es