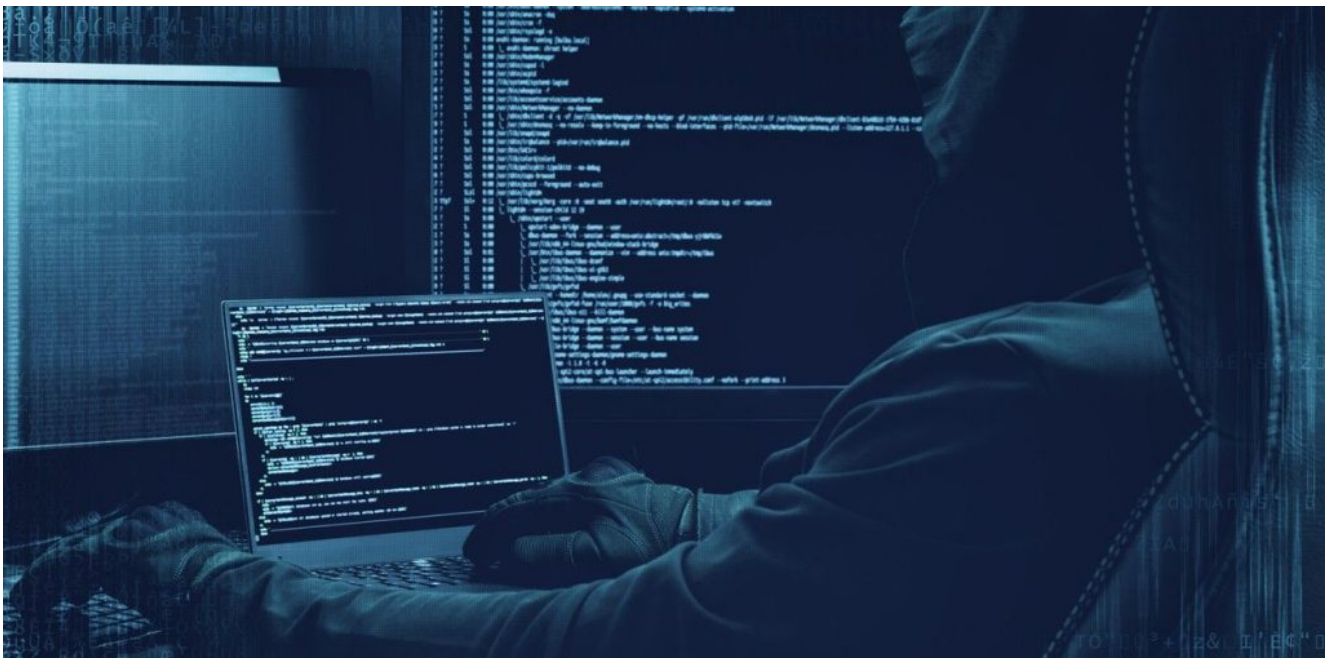
# Una filtración expone datos de argentinos en la dark web: qué tipo de información se difundió

19/12/2025



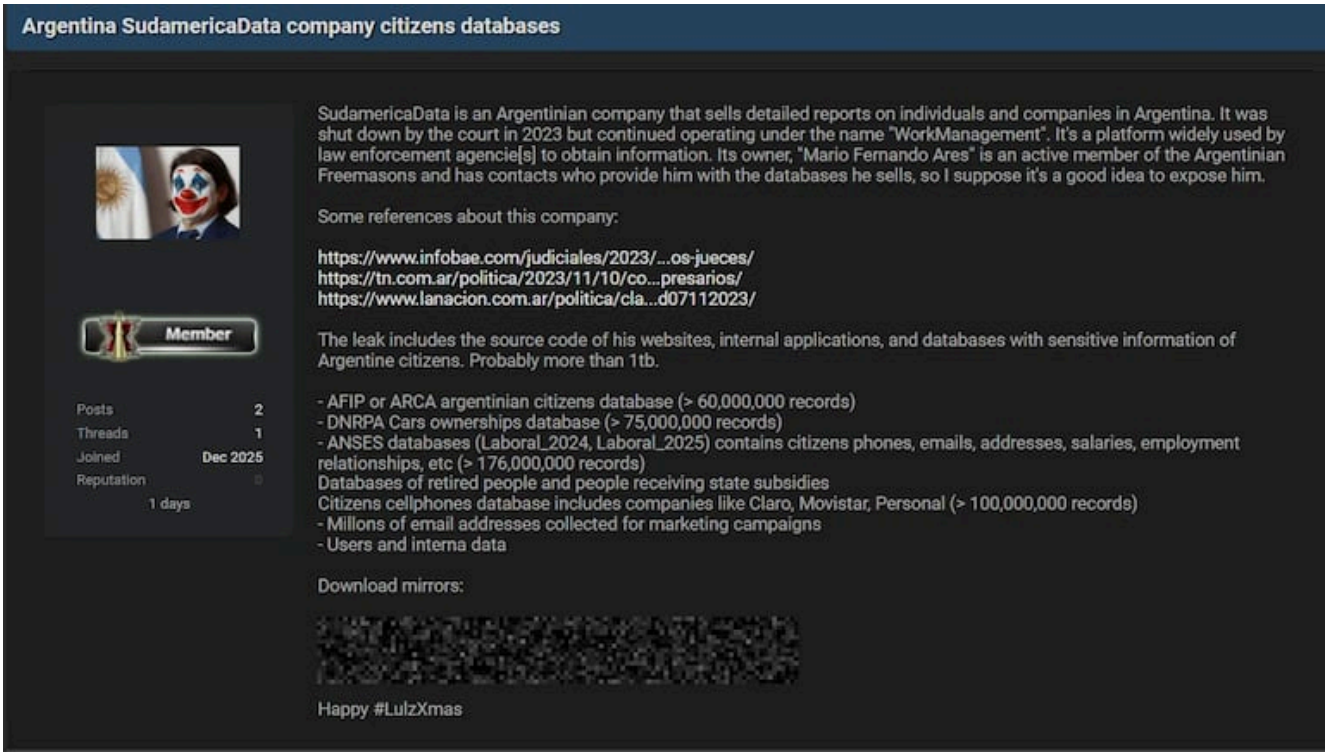
Más de **1 terabyte de información confidencial** habría quedado expuesta tras un presunto ataque informático a **SudamericaData**, una empresa dedicada a la elaboración y venta de reportes sobre personas y compañías. El incidente fue reportado por **Daily Dark Web**, aunque hasta el momento **no hubo confirmación oficial** por parte de los organismos estatales mencionados en las bases.

Según la información difundida, la firma habría continuado operando bajo el nombre **Work Management** luego de una clausura judicial en 2023. El material filtrado incluiría tanto bases de datos como **código fuente de sistemas internos**, lo que amplifica el impacto potencial del episodio.

# Qué tipo de datos se habrían filtrado

De acuerdo con los detalles publicados en foros clandestinos, el archivo expuesto contendría información de distintas fuentes, entre ellas:

- **Bases de datos fiscales** atribuidas a AFIP/ARCA, con decenas de millones de registros.
- **Registros del DNRPA**, con información vinculada a la titularidad de vehículos.
- **Datos laborales y previsionales de ANSES**, que incluirían teléfonos, correos electrónicos, direcciones, salarios y relaciones laborales.
- **Información de jubilados y beneficiarios de subsidios estatales**.
- **Bases de números de teléfonos celulares** de los principales operadores del país.
- **Millones de direcciones de correo electrónico** utilizadas para campañas de marketing.
- **Código fuente y datos internos** de la empresa.



Captura de una publicación en la Dark Web publicada (Vía Daily DArk Web)

Más allá del volumen, el principal riesgo radica en la **combinación de múltiples bases en un solo repositorio**, lo que permite reconstruir perfiles completos de personas físicas con un alto nivel de detalle.

# Por qué es una filtración especialmente grave

En el ámbito de la ciberseguridad, este tipo de exposiciones son consideradas de **alto impacto** porque facilitan delitos como:

- **Suplantación de identidad**, para abrir cuentas, solicitar créditos o realizar trámites a nombre de terceros.
- **Estafas personalizadas**, mediante correos electrónicos, mensajes o llamados con datos reales de la víctima.
- **Ataques dirigidos**, que utilizan información específica para aumentar la efectividad del engaño.

Además, la presunta presencia de **código fuente** podría

facilitar nuevos ataques o vulnerabilidades si esos sistemas continúan activos.

## Antecedentes judiciales y un negocio bajo la lupa

**SudamericaData** ya había quedado en el centro de una investigación judicial en 2023, vinculada al uso y comercialización de información sensible. En ese contexto, la empresa fue **clausurada por orden judicial,** aunque algunos especialistas sostienen que habría seguido operando bajo otra razón social.

El caso vuelve a poner en discusión el rol de empresas privadas que concentran grandes volúmenes de datos personales y la necesidad de **controles más estrictos sobre el uso, almacenamiento y protección de esa información**.

## Qué pueden hacer los usuarios

Aunque no existe, por ahora, un canal oficial para verificar si una persona está afectada, las recomendaciones son prestarle atención a la seguridad y estar alerta:

- **Cambiar contraseñas** de servicios digitales y evitar reutilizarlas.
- **Activar la autenticación en dos pasos** en todas las cuentas posibles.
- **Desconfiar de mensajes, correos o llamadas** que soliciten datos personales o financieros.
- **Monitorear movimientos bancarios y financieros** ante cualquier actividad sospechosa.

El caso funciona como un recordatorio del valor de los datos personales y de los riesgos que implica su circulación sin controles adecuados, tanto para los ciudadanos como para las

empresas y el Estado.

Fuente: TN