INTERNACIONAL

Investiga FBI posible hackeo a su base de datos criminal; Trump minimiza el incidente

21 de noviembre de 2026 · 4 min de lectura



El Buró Federal de Investigaciones (FBI) de Estados Unidos investiga una posible intrusión en el Centro Nacional de Información Criminal (NCIC), una de sus bases de datos más importantes, utilizada por autoridades federales, estatales y locales para consultar órdenes de arresto, antecedentes y otra información policial.

La posible vulneración fue reportada por medios estadounidenses, que citaron a dos personas familiarizadas con el caso. Hasta el momento, el FBI no ha confirmado públicamente el alcance del incidente ni ha respondido a las solicitudes de información de la prensa.

La base de datos NCIC permite a las corporaciones policiales compartir información necesaria para identificar a personas buscadas por la justicia y realizar verificaciones de antecedentes. Por ello, una eventual alteración o filtración de sus registros podría representar un riesgo para las investigaciones y la seguridad pública.

Trump resta importancia al posible ataque

El presidente Donald Trump reaccionó al incidente durante una entrevista telefónica con Fox News, en la que reconoció que acababa de enterarse de la situación.

“Diré que no es algo bueno; no me gusta”, expresó. Sin embargo, enseguida sugirió que la intrusión podría tener un lado positivo, al afirmar que quizá permitiría conocer información que de otra manera no habría salido a la luz.

Trump aprovechó el tema para volver a cuestionar la investigación del FBI sobre la posible interferencia rusa en las elecciones presidenciales de 2016, a la que se refirió como el “engaño de Rusia”.

El mandatario también insinuó, sin presentar pruebas, que el acceso a la base de datos podría revelar información sobre presuntos fraudes electorales y otros asuntos relacionados con investigaciones de su primer mandato.

Una base de datos clave para las fuerzas del orden

La importancia del NCIC radica en que es una herramienta de consulta cotidiana para agentes de todo el país. Un exfuncionario del FBI explicó a CNN que las corporaciones dependen de este sistema para localizar fugitivos, verificar órdenes de arresto y acceder a información que puede influir directamente en la seguridad de los elementos policiales y de la población.

El exfuncionario advirtió que la preocupación no se limita a que los hackers hayan podido obtener información confidencial, sino también a la posibilidad de que alteren la precisión de los registros en los que confían las autoridades.

Por ahora, no se ha informado públicamente qué datos pudieron quedar expuestos ni si hubo modificaciones en la información almacenada.

Antecedentes de vulneraciones al FBI

El posible hackeo ocurre meses después de otro incidente de ciberseguridad. En septiembre, el FBI informó que investigaba una presunta intrusión atribuida al grupo de ciberdelincuentes ShinyHunters, que afirmó haber robado información confidencial de aproximadamente 38 mil empleados de la agencia.

De acuerdo con CNN, los datos estaban relacionados con un sitio web de ofertas de empleo del FBI. El incidente generó preocupación entre trabajadores y exempleados por los posibles riesgos de que su información personal terminara en manos de delincuentes o grupos de hackers.

También se reportó una vulneración en 2023 contra un sistema informático de la oficina del FBI en Nueva York, utilizado en investigaciones sobre explotación sexual infantil. Entre los archivos del sistema había imágenes relacionadas con la investigación sobre Jeffrey Epstein.

Otros incidentes de ciberseguridad en Estados Unidos

La investigación se desarrolla en un contexto de preocupación por una serie de fallas tecnológicas registradas recientemente en sectores como la banca, la aviación y otras áreas de infraestructura estadounidense.

Aunque autoridades han señalado que las interrupciones no fueron provocadas por ciberataques, los incidentes generaron cuestionamientos sobre la seguridad de los sistemas tecnológicos del país.

Por separado, NBC reportó un presunto ataque contra el Departamento de Agricultura de Estados Unidos (USDA). Según el medio, empleados fueron informados de que el sistema de pagos agrícolas había sido objetivo de una intrusión. La dependencia no había emitido comentarios públicos sobre el caso.

En medio de estos acontecimientos, el director del FBI, Kash Patel, defendió las acciones de la agencia en materia de ciberseguridad y destacó la llamada “Operación Winter Shield”, una iniciativa para impulsar actualizaciones de sistemas y prevenir el acceso de hackers a información confidencial.

Hasta el momento, las autoridades estadounidenses no han detallado quién estaría detrás de la posible intrusión al NCIC ni qué información habría sido comprometida.

Publicado en Punto de Referencia. Dirección original: https://puntodereferencia.mx/internacional/investiga-fbi-posible-hackeo-a-su-base-de-datos-criminal-trump-minimiza-el-incidente
Descargado el 21 de noviembre de 2026.