# Anuncio de interés público

del FBI y la CISA

**4 de octubre de 2022**

Número de alerta:

**I-100422b-PSA**

De tener preguntas acerca de este anuncio de interés público, diríjase a la **oficina regional del FBI** en su área.

Ubicaciones de las oficinas regionales del FBI por área: www.fbi.gov/contact-us/field-offices

## Es poco probable que la ciberactividad malintencionada contra la infraestructura electoral interrumpa o impida la votación

El Buró Federal de Investigaciones (FBI, por sus siglas en inglés) y la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA, por sus siglas en inglés) estiman que es poco probable que los intentos por parte de ciberactores que tengan el objeto de vulnerar la infraestructura electoral provoquen interrupciones a gran escala o impidan la votación. A fecha de este informe, el FBI y la CISA **no** cuentan con ningún informe que sugiera que en algún momento la ciberactividad haya impedido que un votante registrado vote, que haya vulnerado la integridad de alguna papeleta o que haya afectado la exactitud de la información de los registros electorales de los votantes. Todo intento que el FBI y la CISA hayan rastreado ha permanecido restringido y se ha obstaculizado o mitigado de manera satisfactoria, y la interrupción que haya causado en los procesos electorales ha sido mínima o nula.

El público debe ser consciente de que los funcionarios electorales utilizan una variedad de controles tecnológicos, físicos y de procedimiento para mitigar la probabilidad de que se produzcan actividades cibernéticas malintencionadas (p. ej., ciberestafas, programas de cibersecuestro de datos, denegación de servicio o suplantación de dominios) que afecten la confidencialidad, la integridad o la disponibilidad de los sistemas de la infraestructura electoral, o los datos relativos a esta, y que alterarían los votos o que, de otra manera, interrumpirían o impedirían la votación. Estos controles comprenden medidas a prueba de fallas, como las papeletas provisionales y las copias de cuadernos de votación, y salvaguardias que protegen contra fallas en la votación (p. ej., pruebas de lógica y precisión, procedimientos de cadena de custodia, papeletas en papel y auditorías después de las elecciones). En vista de las muchas salvaguardias existentes, y de la naturaleza distribuida de la infraestructura electoral, el FBI y la CISA continúan estimando que sería difícil que se realicen intentos para manipular los votos a escala sin que se detecten.

Los sistemas electorales que albergan información de los registros electorales de los votantes o que administran procesos electorales que no tienen que ver con la votación siguen siendo un blanco de interés para los actores perniciosos de amenazas. Los ciberactores también pueden intentar difundir o intensificar afirmaciones falsas o exageradas sobre vulneraciones a la ciberseguridad de la infraestructura electoral; sin embargo, estos intentos no impedirían la votación o la divulgación precisa de los resultados[a].

El FBI y la CISA continuarán respondiendo rápidamente a toda posible amenaza, brindando recomendaciones para fortalecer la infraestructura electoral, notificando a las partes interesadas sobre las amenazas y las actividades de intrusismo, e imponiendo riesgos y consecuencias a los ciberactores que busquen amenazar las elecciones estadounidenses.

**Recomendaciones**

- Para obtener información sobre la manera de registrarse para votar, los lugares donde se lleva a cabo la votación, la votación por correo, el proceso relativo a la boleta electoral provisional y los resultados finales de la elección, cuente con los funcionarios electorales de los gobiernos estatales y locales.
- Manténgase alerta ante las tretas relacionadas con las elecciones mediante las que se podría intentar impedir la gestión de estas.
- Tenga cuidado con los correos electrónicos o las llamadas telefónicas que provengan de direcciones de correo electrónico o números de teléfono desconocidos y a través de los que se hagan afirmaciones sospechosas sobre el proceso electoral, y tenga cuidado con las publicaciones en las redes sociales que parezcan difundir información incoherente sobre incidentes o resultados relacionados con las elecciones.
- No se comunique con remitentes de correos electrónicos no solicitados. No abra archivos adjuntos procedentes de personas desconocidas ni tampoco proporcione información personal por correo electrónico sin confirmar la identidad del solicitante. Tenga en cuenta que muchos correos electrónicos que solicitan su información personal suelen parecer legítimos.
- Verifique a través de muchas fuentes dignas de confianza toda comunicación acerca de la vulneración de información electoral o de sistemas de votación, y considere buscar otras fuentes fiables antes de compartir dicha información a través de las redes sociales u otras vías.
- Tenga cuidado con los sitios web no afiliados con los gobiernos locales o estatales que soliciten información sobre la votación, como información sobre el registro de votantes. Los sitios web que terminan en ".gov" o los sitios web que usted sepa que están afiliados a su oficina electoral estatal o local suelen ser fiables. Asegúrese de saber con antelación cuáles son los sitios web de sus oficinas electorales, estatal y local, para evitar proporcionar involuntariamente su información a sitios web o a actores perniciosos.
- Denuncie los posibles delitos —como los ciberataques a los sistemas de votación— a la oficina local del FBI.
- Denuncie los ciberincidentes contra la infraestructura electoral a los funcionarios electorales locales y a la CISA (Central@CISA.gov).

El FBI está a cargo de investigar los delitos electorales, las operaciones de influencia extranjera perniciosa y las ciberactividades malintencionadas contra la infraestructura electoral y demás instituciones democráticas de los Estados Unidos. La CISA ayuda a los propietarios y a los operadores de infraestructuras críticas, incluidos los de la comunidad electoral, a mantenerse resistentes ante las amenazas físicas y las ciberamenazas. El FBI y la CISA brindan servicios e información para mantener la seguridad, la integridad y la resistencia de la infraestructura electoral estadounidense.

**Denuncias de víctimas e información adicional**

El FBI y la CISA urgen al público a dar parte de información sobre actividades sospechosas o delictivas a la oficina regional del FBI en su área (www.fbi.gov/contact-us/field). Visite los siguientes sitios web para encontrar más ayuda, mejores prácticas y términos comunes:

- *FBI's Protected Voices* [Iniciativa del FBI "Voces Protegidas"]: www.fbi.gov/investigate/counterintelligence/foreign-influence/protected-voices

- Página del FBI sobre delitos electorales y seguridad: www.fbi.gov/scams-and-safety/common-scams-and-crimes/election-crimes-and-security
- Biblioteca de recursos de la CISA en materia de seguridad electoral: Election Security Library | CISA
- Página de la CISA para detener los programas de cibersecuestro de datos: https://www.cisa.gov/stopransomware
- Biblioteca de recursos de la CISA sobre la información errónea, la desinformación y la mala información: https://www.cisa.gov/mdm-resource-library
- Página de la CISA sobre los rumores frente a la realidad con relación a la seguridad electoral: https://www.cisa.gov/rumorcontrol

Para acceder a los anuncios de interés público del FBI y la CISA que se publicaron previamente, y que se relacionan con las elecciones de 2020, haga clic en los siguientes enlaces de IC3.gov:

- Distributed Denial of Service Attacks Could Hinder Access to Voting Information, Would Not Prevent Voting
  [Los ataques distribuidos de denegación de servicio podrían obstaculizar el acceso a la información electoral, aunque no impedirían la votación]
- Cyber Threats to Voting Processes Could Slow But Not Prevent Voting
  [Las ciberamenazas a los procesos de votación podrían ralentizar la votación, aunque no impedirla]
- Spoofed Internet Domains and Email Accounts Pose Cyber and Disinformation Risks to Voters
  [Los dominios de internet y las cuentas de correo electrónico falsificados plantean ciberriesgos y riesgos de desinformación a los votantes]
- Foreign Actors Likely to Use Online Journals to Spread Disinformation Regarding 2020 Elections
  [Es probable que los actores extranjeros utilicen las revistas en línea para difundir desinformación sobre las elecciones de 2020]
- Foreign Actors and Cybercriminals Likely to Spread Disinformation Regarding 2020 Election Results
  [Es probable que los actores extranjeros y los ciberdelincuentes difundan desinformación sobre los resultados de las elecciones de 2020]
- False Claims of Hacked Voter Information Likely Intended to Cast Doubt on Legitimacy of U.S. Elections
  [Es probable que afirmaciones falsas sobre información de votantes pirateada tenga la intención de poner en duda la legitimidad de las elecciones estadounidenses]

[a] Es probable que las personas estadounidenses que vinculen, citen o expresen los mismos argumentos presentados por actores perniciosos sean partícipes de actividades que la primera Enmienda de la Constitución proteja, salvo que la ley lo prohíba. Además, no debe suponerse que las variantes de los temas tratados en el presente documento, incluso las que comprendan términos divisivos, reflejen actividades malintencionadas cuando no haya información que atribuya concretamente el contenido a actores perniciosos. Los actores perniciosos con frecuencia intensifican temas que ya se ventilan en el debate nacional legítimo. Los actores endógenos legales en los Estados Unidos tienen derecho a valerse de argumentos que se originen de cualquier fuente, incluso de narrativas adversarias. Esta información debe considerarse en el contexto de toda autoridad legal y política aplicable sobre la utilización de la información de fuentes públicas mientras se protege la privacidad, los derechos civiles y las libertades civiles.