



RUMOR VS. REALIDAD



SEGURIDAD ELECTORAL RUMOR VS. REALIDAD

¿Busca información sobre esfuerzos de seguridad electoral específicos de cada estado o preguntas frecuentes adicionales? Consulte la página [#TrustedInfo2024](#) de la Asociación Nacional de Secretarías de Estado (NASS)* y la página de [preguntas frecuentes](#) sobre elecciones de la Asociación Nacional de Directores Electorales Estatales (NASED)*.

Última actualización: Febrero 8 de 2024

Los funcionarios electorales estatales, locales y territoriales trabajan todo el año para preparar y administrar las elecciones, implementando una amplia gama de medidas de seguridad y actuando como fuentes autorizadas de información gubernamental oficial para sus votantes acerca de las elecciones. Si bien existen semejanzas importantes entre y dentro de los estados, cada jurisdicción electoral estatal, local y territorial maneja sus elecciones bajo un marco legal y procesal único que utiliza diferentes sistemas e infraestructura. Las diferencias y la complejidad introducidas por dicha descentralización pueden generar incertidumbre en la mente de los votantes; incertidumbre que puede ser aprovechada por actores maliciosos. Al complementar los esfuerzos en educación electoral y alfabetización cívica por parte de los funcionarios electorales, esta página busca informar a los votantes y ayudarlos a desarrollar resiliencia contra las narrativas de información errónea, desinformación, e información maliciosa (MDM) sobre la infraestructura electoral.

Rumor vs. Realidad está diseñado para proporcionar información precisa y confiable referente a narrativas y temas comunes de MDM que se relacionan ampliamente con la seguridad de la infraestructura electoral y los procesos relacionados con la misma. No tiene la intención de abordar declaraciones relacionadas específicamente con temas de jurisdicción. En cambio, este recurso aborda los rumores de seguridad electoral describiendo procesos de protección, medidas de seguridad y requisitos legales comunes y generalmente aplicables diseñados para disuadir, detectar y proteger contra amenazas de seguridad significativas relacionadas con la infraestructura y los procesos electorales.

Puede obtener más información sobre el trabajo de CISA para desarrollar resiliencia a MDM visitando la [Biblioteca de Recursos de MDM](#).

¡NUEVO!

Rumor Nuevo vs Realidad



Período Preelectoral



Día de Elecciones



Período Poselectoral

PERÍODO PREELECTORAL

✓ Realidad: Los funcionarios electorales actualizan regularmente las listas de registro de votantes de acuerdo con las protecciones legales contra la eliminación de votantes elegibles para registro.

✗ Rumor: Los funcionarios electorales no limpian las listas de votantes.

Conozca los hechos: Los funcionarios electorales actualizan regularmente sus listas de registro de votantes en función de las solicitudes de votación y los datos de diversas fuentes que puedan indicar que un votante ha fallecido,

Por favor tenga en cuenta: CISA reconoce que el lenguaje evoluciona continuamente y que la documentación traducida puede no capturar todos sus matices. Aunque hemos intentado ofrecer una traducción exacta de los materiales, la versión oficial y definitiva es aquella que contiene el texto original en inglés. Agradecemos sus comentarios - LanguageAccess@cisa.dhs.gov

Please note: CISA recognizes that language is continually evolving, and that translated work may not fully capture all nuance. Although we have attempted to provide an accurate translation of the materials, the official definitive version is the original English text. We welcome your feedback - LanguageAccess@cisa.dhs.gov

se ha mudado, se ha registrado en otro lugar, ha cambiado de nombre o no es elegible. Estas fuentes de datos incluyen agencias de registro de vehículos automotores, entidades que mantengan registros de defunción, notificaciones de confirmación enviadas por correo a los votantes e intercambios de datos interestatales. Esto ayuda a los funcionarios electorales a identificar y combinar registros duplicados y eliminar registros de personas que ya no son elegibles. Las leyes federales y estatales protegen contra la eliminación de personas elegibles para el registro de votantes. Estas incluyen prohibiciones federales, aplicables en la mayoría de los estados, contra la eliminación dentro de los 90 días previos a una elección federal de algunos votantes inscritos, y la eliminación de votantes inscritos únicamente por el hecho de no haber votado. A menos que un funcionario electoral tenga información de primera mano de que una persona registrada se ha mudado, los procesos utilizados para eliminar los registros de personas que se hayan mudado pueden demorar más de dos años debido a las protecciones que evitan que las personas registradas sean eliminadas por error.

Dichas protecciones legales y el momento en que se comparten los datos pueden generar un retraso entre el momento cuando una persona deja de ser elegible y la eliminación de su registro. Esto puede llevar a que parte del correo electoral oficial, incluidas las papeletas para voto por correo en algunos estados, se envíe a direcciones de personas que se han mudado o que no sean elegibles. Los funcionarios electorales a menudo sugieren al público que si reciben correo electoral de personas que ya no residan en la dirección, notifiquen a la oficina electoral.

Las leyes estatales y federales prohíben la suplantación de identidad de los votantes, lo que incluye votar en nombre de una persona que haya fallecido, se haya mudado o haya perdido la elegibilidad de alguna forma, pero cuyo registro permanece temporalmente en las listas de votantes. Las garantías adicionales de integridad electoral, incluida la comparación de firmas y la verificación de otros datos personales, protegen contra personas que votan en nombre de otros.

Las prácticas de registro de votantes descritas en esta entrada no se aplican en Dakota del Norte, donde el registro de votantes no ocurre.

Recursos útiles

- 18 U.S.C. § 1708
- 52 U.S.C. §§ 10307(c), 20507, 20511(2), 21083(a)(2)(A)
- [Election Infographic Products](#)
- [The National Voter Registration Act of 1993: Questions and Answers](#), DOJ
- [Election Crimes](#), FBI
- [Election Mail Information Center](#),
- USPS Sus funcionarios electorales locales o estatales. [EAC state-by-state directory](#)
- [Maintenance of State Voter Registration Lists](#), NASS
- [Voter List Accuracy](#), NCSL
- [Election FAQs](#), NASED

✓ Realidad: Las garantías protegen la integridad del proceso de voto por correo/en ausencia, incluso en relación con el uso de formularios de solicitud de papeleta por correo/en ausencia.

✗ Rumor: Las personas pueden violar fácilmente la integridad del proceso de solicitud de papeletas por correo/en ausencia para recibir y emitir papeletas por correo/en ausencia no autorizadas, o impedir que los votantes autorizados logren voten en persona.

Conozca los hechos: Los funcionarios electorales utilizan varias medidas de seguridad para proteger la integridad del proceso de votación por correo o en ausencia, incluidas aquellas que protegen contra el uso no autorizado de formularios de solicitud de papeletas de votación, en los estados donde se usan dichos formularios, el envío de papeletas de votación por correo o en ausencia a personas no elegibles, y votantes en persona elegibles a los quienes por error se les impidió votar debido a que aparecían en el registro de votación como que ya habían recibido una papeleta de votación de por correo o en ausencia.

Los formularios de solicitud de papeleta de votación por correo o en ausencia generalmente requieren que los

solicitantes firmen el formulario y afirmen su elegibilidad para emitir su voto por correo o en ausencia bajo pena de ley. Al recibir un formulario de solicitud de papeleta por correo/en ausencia, los funcionarios electorales implementan diversos procedimientos para verificar la identidad y elegibilidad del solicitante antes de enviarle una papeleta por correo/en ausencia. Dichos procedimientos incluyen verificar la firma y la información enviada en el formulario con el registro de votante correspondiente, así como garantizar que no se envíen múltiples papeletas por correo o en ausencia en respuesta a solicitudes que utilicen la misma información de votante.

Los funcionarios electorales implementan además diversos procedimientos para verificar la identidad y elegibilidad de quienes envían boletas por correo o en ausencia. Aquellos que envíen boletas por correo o en ausencia deben firmar el sobre de la papeleta para votación por correo o en ausencia. En algunos estados, también se requiere una firma notariada, la firma de un testigo o testigos y/o una copia de un documento de identificación válido. Al recibir una papeleta de voto por correo/en ausencia, los funcionarios electorales verifican la firma en el sobre de la papeleta de voto por correo/en ausencia y/o que dicha papeleta haya sido enviada correctamente antes de sacarla de su sobre y entregarla para el conteo. Algunos estados notifican al votante si hay una discrepancia o si falta una firma, lo que le da al votante la oportunidad de corregir el problema.

Las políticas estatales sobre cómo manejar a un votante en persona que aparece en el registro de votación como si se le hubiera enviado una papeleta por correo o en ausencia varían. En la mayoría de los estados, se requiere que el votante emita una papeleta provisional que puede ser revisada posteriormente por los funcionarios electorales. En otros, el votante puede emitir una papeleta regular y cualquier papeleta por correo o en ausencia correspondiente devuelta a nombre de ese votante sería rechazada. En todos estos casos, los casos de posible doble voto o suplantación de identidad de votante podrían remitirse a las autoridades correspondientes para su investigación.

Recursos útiles

- [Mail-in Voting in 2020 Infrastructure Risk Assessment](#), CISA
- [Mail-in Voting in 2020 Infrastructure Risk Infographic](#), CISA
- [Mail-in Voting Integrity Safeguards Infographic](#), CISA
- [USPS Election Mail Information Center](#), USPS
- [How States Verify Absentee Ballot Applications](#), NCSL
- [How States Verify Voted Absentee Ballots](#), NCSL
- [States That Permit Voters to Correct Signature Discrepancies](#), NCSL
- 52 U.S.C. § 21082
- [Provisional Ballots](#), NCSL
- [State Policies on Voting In-Person or Changing Vote After Requesting a Mail/Absentee Ballot](#), NASS
- [Election FAQs](#), NASED
- Sus funcionarios electorales locales o estatales. [EAC state-by-state directory](#)

 **Realidad: Medidas sólidas de seguridad protegen contra la manipulación de boletas devueltas a través del buzón.**

 **Rumor: Los buzones utilizados por los funcionarios electorales para recolectar las papeletas enviadas por correo o en ausencia devueltas pueden ser manipulados, robados o destruidos fácilmente.**

Conozca los hechos: Los funcionarios electorales utilizan varias medidas de seguridad para proteger las papeletas devueltas por los votantes a través de los buzones para que no sean manipuladas, robadas o destruidas. Los buzones ubicados al aire libre generalmente están contruidos en metal pesado y de alta calidad, atornillados al suelo e incluyen características de seguridad como candados, sellos a prueba de manipulación, ranuras de inserción de boletas de tamaño mínimo y dispositivos para la prevención contra incendios y daños por agua.

Los buzones ubicados en el interior generalmente cuentan con personal a cargo y están protegidos por las medidas de seguridad existentes en el edificio. Muchas oficinas electorales monitorean sus buzones a través de vigilancia por video las 24 horas del día. Las boletas devueltas a través del buzón son recuperadas por funcionarios electorales o personas designadas, a menudo en equipos bipartidistas, en intervalos frecuentes.

Recursos útiles

- [Ballot Drop Box](#), Election Infrastructure Subsector's Government Coordinating Council and Sector Coordinating Council Joint COVID-19 Working Group
- [Ballot Drop Box Definitions, Design Features, Location, and Number](#), NCSL
- [Voting Outside the Polling Place: Absentee, All-Mail and other Voting at Home Options](#), NCSL
- [Election FAQs](#), NASED
- Sus funcionarios electorales locales o estatales. [EAC state-by-state directory](#)

✓ **Realidad:** El *hardware* y el *software* del sistema de votación son sometidos a pruebas por parte de las autoridades electorales federales, estatales y/o locales.

✗ **Rumor:** El *software* del sistema de votación no se revisa, ni es puesto a prueba, y puede manipularse fácilmente.

Conozca los hechos: Los funcionarios electorales estatales y locales implementan diversas prácticas de prueba para ayudar a garantizar que el *hardware* y el *software* del sistema de votación funcionen según lo previsto. Estas prácticas incluyen pruebas y certificaciones federales y estatales, pruebas antes de la adquisición, pruebas de aceptación y/o pruebas de precisión y lógica antes y después de las elecciones. Dichas pruebas ayudan a detectar y proteger contra problemas de *software* maliciosos o anómalos.

Según los programas de certificación federales y estatales, los fabricantes de sistemas de votación someten a dichos sistemas a pruebas y revisiones por parte de un laboratorio acreditado o de probadores estatales. Estas pruebas están diseñadas para verificar que los sistemas funcionen según lo diseñado y cumplan con los requisitos o estándares estatales y/o federales aplicables en cuestión de precisión, privacidad y accesibilidad, según las pautas del sistema de votación voluntaria establecidas por la Comisión de Asistencia Electoral de EE. UU. Las pruebas de certificación generalmente incluyen una revisión del código fuente de un sistema, así como pruebas ambientales, de seguridad y funcionales. Dependiendo del estado, estas pruebas pueden ser llevadas a cabo por un laboratorio certificado por el estado, una universidad asociada y/o un laboratorio de pruebas certificado por el gobierno federal.

Recursos útiles

- 52 U.S.C. §§ 20971, 21081
- [Voting System Certification Process](#), EAC
- [Voting System Security Measures](#), EAC
- [Election Infrastructure Security](#), CISA
- [Election Infrastructure Cyber Risk Assessment and Infographic](#), CISA
- [Voting System Standards, Testing and Certification](#), NCSL
- [Post-Election Audits](#), NCSL
- [Election FAQs](#), NASED
- Sus funcionarios electorales locales o estatales. [EAC state-by-state directory](#)

✓ **Realidad:** El mantenimiento de la lista de registro de votantes y otras medidas para la integridad electoral protegen contra la votación ilegal en nombre de personas fallecidas.

✗ **Rumor:** Se están emitiendo votos bajo nombres de personas fallecidas y estos votos están siendo contados.

Conozca los hechos: Las leyes estatales y federales prohíben la suplantación de identidad de los votantes, incluida la emisión de votos en nombre de una persona fallecida. Los funcionarios electorales actualizan regularmente sus listas de registro de votantes, eliminando los registros de aquellos que fallecieron, se mudaron, se registraron en otro lugar o no calificaron. La remoción de personas fallecidas se basa en los registros de defunción compartidos por las agencias estatales de estadísticas vitales y la Administración del Seguro Social. Si bien puede haber un lapso entre la muerte de una persona y su eliminación de la lista de registro de votantes, lo que puede llevar a que se envíe algún correo electoral oficial, incluidas las papeletas por correo a las direcciones de las personas fallecidas, los registros de defunción brindan un seguimiento de auditoría sólido para identificar cualquier intento de emitir votos en nombre de

personas fallecidas. Las garantías adicionales de integridad electoral que incluyen la comparación de firmas y la verificación de información protegen aún más contra la suplantación de identidad de los votantes y la votación por parte de personas no elegibles.

En algunos casos, las personas vivas pueden devolver las boletas por correo o dar su voto en persona por anticipado y luego fallecer antes del día de las elecciones. Algunos estados permiten que se cuenten las papeletas de los votantes, mientras que otros las rechazan y siguen procedimientos para identificarlas y rechazarlas durante el procesamiento.

Parte de la información del registro de votantes puede parecer sugerir actividad sospechosa si es tomada fuera de contexto, pero en realidad es el resultado de un error administrativo inocuo o de prácticas de datos previstas.

Por ejemplo, en raras ocasiones cuando no se conoce la fecha de nacimiento de una persona registrada (p. ej., un votante que se registró legalmente antes de las prácticas modernas de registro de votantes), los funcionarios electorales pueden usar datos temporales (p. ej., 1/1/1900) hasta que la fecha de nacimiento de la persona registrada pueda ser actualizada. En otros casos, un hijo en edad de votar que tenga el mismo nombre y dirección que su padre fallecido podría malinterpretarse como un votante fallecido o conducir a errores administrativos.

Recursos útiles

- 18 U.S.C. § 1708
- 52 U.S.C. §§ 10307(c), 20507, 20511(2), 21083(a)(2)(A)
- [Mail-in Voting Integrity Safeguards Infographic](#), CISA
- [Election Infrastructure Cyber Risk Assessment](#) and [Infographic](#), CISA
- [Election Infrastructure Security](#), CISA
- [Election Security](#), DHS
- [The National Voter Registration Act of 1993: Questions and Answers](#), DOJ
- [Election Crimes](#), FBI
- [Election Mail Information Center](#), USPS
- Sus funcionarios electorales locales o estatales. [EAC state-by-state directory](#)
- [Maintenance of State Voter Registration Lists](#), NASS
- [What If an Absentee Voter Dies Before Election Day?](#), NCSL
- [Voter List Accuracy](#), NCSL
- [Election FAQs](#), NASED

 **Realidad: Algunos datos del registro de votantes están disponibles públicamente.**

 **Rumor: Si alguien posee o publica datos de registro de votantes significa que las bases de datos de registro de votantes han sido pirateadas.**

Conozca los hechos: Parte de la información del registro de votantes es información pública y está disponible para campañas políticas, investigadores y, a menudo, miembros del público, con frecuencia están a la venta.

De acuerdo con un anuncio de servicio público conjunto entre el FBI y CISA, los actores cibernéticos pueden dar declaraciones falsas sobre información "pirateada" de votantes para socavar la confianza en las instituciones democráticas de EE. UU.

Recursos útiles

- [Availability of State Voter File and Confidential Information](#), EAC
- [FBI-CISA Public Service Announcement: False Claims of Hacked Voter Information Likely Intended to Cast Doubt on Legitimacy of U.S. Elections](#)
- [Access To and Use Of Voter Registration Lists](#), NCSL
- [Election FAQs](#), NASED

✓ **Realidad:** Los sitios web de registro de votantes en línea pueden sufrir interrupciones por motivos no maliciosos.

✗ **Rumor:** Un sitio web de registro de votantes en línea sufre una interrupción y se declara que las elecciones se han visto comprometidas.

Conozca los hechos: Las interrupciones en los sistemas de registro de votantes en línea ocurren por una variedad de razones, incluidos errores de configuración, problemas de *hardware*, desastres naturales, problemas de infraestructura de comunicaciones y ataques de negación de servicio distribuido (DDoS*).

Como advirtieron CISA y el FBI en un [anuncio de servicio público](#), una interrupción del sistema no significa necesariamente que la integridad de la información de registro de votantes o cualquier otro sistema electoral haya sido afectado. Cuando ocurre una interrupción, los funcionarios electorales trabajan para verificar la integridad de la información del registro de votación.

Recursos útiles

- [FBI-CISA Public Service Announcement: False Claims of Hacked Voter Information Likely Intended to Cast Doubt on Legitimacy of U.S. Elections](#)
- [Securing Voter Registration Data](#), CISA
- Your local or state election officials [EAC state-by-state directory](#)

✓ **Realidad:** Que una instancia de un sistema de gobierno estatal o local sea comprometida, no significa necesariamente que la infraestructura electoral o la integridad de su voto se hayan visto comprometidas.

✗ **Rumor:** Si la tecnología de la información (IT*) de la jurisdicción estatal o local se ha visto comprometida, no se puede confiar en los resultados de las elecciones.

Conozca los hechos: los ataques a los sistemas de IT estatales y locales no deben minimizarse; sin embargo, un compromiso de los sistemas de IT estatales o locales no significa que dichos sistemas estén relacionados con las elecciones. Incluso si un sistema relacionado con las elecciones se viera comprometido, el compromiso de un sistema no significa necesariamente que la integridad de la votación haya sido afectada.

Los funcionarios electorales cuentan con múltiples medidas de seguridad y contingencias, que incluyen papeletas electorales provisionales o registros de votación físicos que limitan el impacto de un incidente cibernético con una interrupción mínima de la votación.

Además, el hecho de tener un registro en papel auditable asegura que el conteo de los votos pueda ser verificado y validado.

Recursos útiles

- [FBI-CISA Public Service Announcement: Cyber Threats to Voting Processes Could Slow But Not Prevent Voting](#)
- [Election Infrastructure Cyber Risk Assessment](#) and [Infographic](#), CISA

✓ **Realidad:** Los actores maliciosos pueden falsificar la manipulación de los datos del registro de votación con el fin de difundir desinformación.

✗ **Rumor:** Videos, imágenes o correos electrónicos que sugieran que la información de registro de votación está siendo manipulada significa que los votantes van a poder votar.

Conozca los hechos: Las declaraciones son fácilmente falsificadas y se pueden utilizar con fines de desinformación. Si los datos de registro de votación fuesen manipulados, los estados cuentan diversas medidas de seguridad para permitir que los votantes emitan su voto, incluyendo copias de seguridad fuera de línea de los datos de registro, papeletas de votación provisionales y, en varios estados, la posibilidad de registrarse el mismo día.

Recursos útiles

- [FBI-CISA Public Service Announcement: False Claims of Hacked Voter Information Likely Intended to Cast Doubt on Legitimacy of U.S. Elections](#)
- [Securing Voter Registration Data](#), CISA
- [Election FAQs](#), NASED

✓ **Realidad:** Existen garantías para evitar que se cuenten papeletas impresas en casa o fotocopiadas, como si fuesen papeletas enviadas por correo.

✗ **Rumor:** Un actor malicioso puede defraudar fácilmente una elección imprimiendo y enviando papeletas adicionales por correo.

Conozca los hechos: Esto es falso. Cometer fraude a través de boletas fotocopiadas o impresas en casa sería algo muy difícil de hacer exitosamente. Esto se debe a que cada oficina electoral local cuenta con medidas de seguridad para detectar ese tipo de actividad maliciosa. Si bien las medidas específicas varían, de acuerdo con las leyes y prácticas electorales estatales y locales, dichas medidas de seguridad incluyen comparación de firmas, verificación de información, códigos de barra, marcas de agua y peso de papel exactos.

Recursos útiles

- [Mail-in Voting Election Integrity Safeguards Infographic](#), CISA
- [Election FAQs](#), NASED

✓ **Realidad:** Existen garantías para proteger contra la votación fraudulenta utilizando la papeleta federal de voto por escrito en ausencia (FWAB*).

✗ **Rumor:** Un actor malicioso puede defraudar fácilmente una elección utilizando la papeleta federal de voto por escrito en ausencia (FWAB).

Conozca los hechos: Cambiar una elección usando FWAB presentados de manera fraudulenta sería muy difícil de hacer. Esto se debe a que las oficinas electorales cuentan con medidas de seguridad para detectar dicha actividad.

La FWAB se utiliza principalmente como papeleta de respaldo para votantes militares y en el extranjero que hayan solicitado, pero aún no hayan recibido su papeleta de voto en ausencia. Los usuarios de FWAB deben proporcionar su firma y cumplir con diversos requisitos estatales de registro de votantes y solicitud de papeleta de voto en ausencia, que pueden incluir el suministro de un número de seguro social completo o parcial, número de identificación estatal, prueba de identificación y/o firma de testigo.

Dado que solo los votantes militares y en el extranjero son elegibles para usar el FWAB, relativamente pocos de ellos se presentan en cada elección. En 2016, los estados informaron que solo se envió un total de 23.291 FWAB en todo el país, y todos, a excepción de seis de esos estados, recibieron menos de 1.000 FWAB. Dado que el uso es relativamente raro, los picos en el uso de FWAB se detectarían como anómalos.

Recursos útiles

- 52 U.S.C. § 20303
- [Voting Assistance Guide](#), FVAP
- [Election Forms and Tools for Sending](#), FVAP
- [Election Administration and Voting Survey Comprehensive Report](#), EAC

DÍA DE ELECCIONES

✓ **Realidad:** El uso de papeletas y otras medidas adicionales, garantizan que los votos puedan contarse cuando un escáner no funcione correctamente o no pueda escanear las papeletas por otras razones.

✗ **Rumor:** Problemas con los escáneres de papeletas en mi sitio de votación significan que mi boleta no será contada.

Conozca los hechos: Como todos los sistemas digitales, los escáneres de papeletas pueden fallar en su funcionamiento. De manera similar, es posible que los escáneres de papeletas que funcionen correctamente no puedan escanear papeletas que estén dañadas, mal impresas o que tengan marcas ambiguas. Cuando una papeleta no puede ser leída por un escáner en un sitio de votación, los funcionarios electorales proceden a almacenarla de forma segura hasta que pueda ser contada más adelante. Debido a que la papeleta en sí es el registro oficial de los votos, no hay ningún impacto en la precisión o integridad de los resultados electorales.

Recursos útiles:

- [Voluntary Voting System Guidelines](#), EAC
- Your local or state election officials [EAC state-by-state directory](#).

✓ **Realidad:** Los funcionarios electorales proporcionan utensilios para escribir aprobados para marcar papeletas a todos los votantes en persona que usan papeletas de papel marcadas a mano.

✗ **Rumor:** Los trabajadores electorales dieron utensilios para escribir específicos, como *Sharpies*, solamente a ciertos votantes para que sus boletas fueran rechazadas.

Conozca los hechos: Las jurisdicciones electorales permiten a los votantes marcar las papeletas con diversos tipos de utensilios para escribir, según la ley estatal y otras consideraciones, como los requisitos del sistema de tabulación. Los trabajadores electorales deben proporcionar a los votantes utensilios para escribir aprobados. Aunque marcadores como *Sharpies*, pueden traspasar las boletas, algunos funcionarios electorales han declarado que el equipo de tabulación de boletas en sus jurisdicciones aún puede leer estas boletas. Muchas jurisdicciones incluso diseñan sus boletas con columnas desplazadas para evitar que cualquier posible traspaso afecte la capacidad de escanear fácilmente ambos lados de las boletas.

Si una papeleta tiene problemas que impidan la capacidad para ser escaneada, puede ser contada a mano o duplicada, o adjudicada por funcionarios electorales, quienes utilizan procedimientos definidos como cadena de custodia para garantizar la protección al secreto e integridad de la papeleta. Además, muchos estados tienen leyes de "Intención del votante" que permiten que se cuenten papeletas incluso cuando existen problemas como filtraciones o marcas perdidas, siempre i cuando se pueda determinar la intención del votante.

Recursos útiles

- [After the Voting Ends: The Steps to Complete an Election](#), NCSL
- [Ballot Duplication blog series](#), Council of State Governments Overseas Voting Initiative
- Sus funcionarios electorales locales o estatales. [EAC state-by-state directory](#)

✓ **Realidad:** Las leyes estatales y federales protegen a los votantes contra amenazas o intimidación en las urnas, incluso por parte de los observadores electorales.

✗ **Rumor:** Se permite que los observadores en el lugar de votación intimiden a los votantes, hagan campaña e interfieran con la votación.

Conozca los hechos: Si bien la mayoría de los estados tienen un proceso para permitir que un número limitado de observadores acreditados o registrados en los lugares de votación en persona observen el proceso de votación, las

leyes estatales y federales ofrecen a los votantes protección general contra amenazas e intimidación, incluso por parte de los observadores. Los estados usan diferentes términos para los observadores, tales como "observadores electorales", "retadores" y "agentes electorales". En general, los observadores tienen prohibido violar el derecho al voto secreto, hacer campaña, recopilar información privada de los votantes y obstruir o interferir con el proceso de votación. Los observadores en algunos estados pueden alertar acerca de problemas potenciales a los funcionarios electorales, como el cuestionamiento de la elegibilidad de un votante, el comportamiento sospechoso o las sospechas de violaciones de reglas. La intimidación o el comportamiento amenazante nunca están permitidos.

Bajo ciertas circunstancias, la División de Derechos Civiles del Departamento de Justicia de los EE. UU. (DOJ) puede monitorear los procedimientos en los lugares de votación para la protección de los votantes bajo las leyes federales de derecho al voto. Los observadores internacionales, incluidas las delegaciones de la Organización para la Seguridad y la Cooperación en Europa o la Organización de los Estados Americanos, que han sido invitados por el Departamento de Estado de los EE. UU., también pueden observar los procesos de votación en persona en algunos estados.

Si cree que ha sido víctima o ha sido testigo de amenazas o intimidación de votantes, reporte dicha situación a la Sección de Votación de la División de Derechos Civiles del DOJ al teléfono 800-253-3931 o a través de su portal de quejas en línea <https://civilrights.justicia.gov/>. En caso de emergencia, llame al 911.

Recursos útiles

- 18 U.S.C. § 245(b)(1)(A), 18 U.S.C. § 594, 52 U.S.C. § 20511, 18 U.S.C. §§ 241 and 242
- [Election Crimes and Security](#), FBI
- [Federal Prosecution of Election Offenses](#), DOJ
- [About Federal Observers and Election Monitoring](#), DOJ
- [State Laws on Poll Watchers and Challengers](#), NASS
- [Poll Watchers and Challengers](#), NCSL
- [Policies for Election Observers](#), NCSL
- [OSCE/ODIHR Elections in the United State of America](#), OSCE
- [Election FAQs](#), NASED

 **Realidad: Existen garantías para proteger el voto secreto.**

 **Rumor: Alguien dice saber por quién voté.**

Conozca los hechos: La confidencialidad de las papeletas de votación está garantizada por ley en todos los estados. Los funcionarios electorales implementan varias medidas de seguridad para que terceros, incluidos los propios funcionarios electorales, no puedan ver o conocer las selecciones hechas por los votantes. Con pocas excepciones, estas medidas de seguridad aseguran que las papeletas individuales, una vez emitidas, no puedan rastrearse e identifiquen a los votantes que las emitieron. Para la votación en persona, las medidas de privacidad incluyen divisores entre las mesas de votación y requisitos de que los trabajadores electorales se mantengan alejados de los votantes mientras emiten sus votos. Para la votación por correo y provisional, los funcionarios electorales siguen estrictos procedimientos para garantizar la confidencialidad de las papeletas cuando éstas se reciben en los sobres de papeletas enviadas por correo y provisionales.

Los votantes pueden renunciar voluntariamente a los derechos de confidencialidad de las papeletas en determinadas circunstancias, y es posible que se requiera la renuncia en algunas de ellas, como los votantes militares y en el extranjero que votan por fax o por correo electrónico.

Si bien las selecciones en la papeleta son secretas en casi todas las circunstancias, la afiliación partidaria de un votante y su historial de votación generalmente no lo son. La información contenida en los registros de registro de votantes, como el nombre, la dirección, el número de teléfono y la afiliación a un partido político (en los estados con registro de votantes basado en un partido), generalmente está disponible para los partidos políticos y otros. Estos datos también contienen información sobre si un votante votó en una elección en particular, pero no sobre sus selecciones de voto.

Recursos útiles

- [Voting Outside the Polling Place: Absentee, All-Mail and other Voting at Home Options](#), NCSL
- [Secrecy of the Ballot and Ballot Selfies](#), NCSL
- [States that are Required to Provide Secrecy Sleeves for Absentee/Mail Ballots](#), NCSL
- [Access To and Use of Voter Registration Lists](#), NCSL
- [Election FAQs](#), NASED

✓ **Realidad:** Los sitios de búsqueda de lugares de votación pueden tener interrupciones por razones no maliciosas.

✗ **Rumor:** Si los sitios de búsqueda de lugares de votación tienen una interrupción, la infraestructura electoral debe haber sido comprometida.

Conozca los hechos: Los sitios de búsqueda de lugares de votación, como todos los sitios en línea, pueden tener interrupciones por una variedad de razones, lo que afecta su disponibilidad para los votantes. Los sitios de búsqueda de lugares de votación no están conectados a la infraestructura que cuenta los votos y, por lo general, están segmentados fuera de la infraestructura que permite la votación, tales como la base de datos de registro de votantes. Los funcionarios electorales indicarán a los votantes potenciales herramientas y recursos alternativos para esta información en caso de que exista algún un problema.

Recursos útiles

- [Election Infrastructure Cyber Risk Assessment](#) and [Infographic](#), CISA
- Your local or state election officials [EAC state-by-state directory](#)

PERÍODO POSELECTORAL

✓ **Realidad:** La existencia de una vulnerabilidad en la tecnología electoral no es evidencia de que la vulnerabilidad haya sido explotada o de que los resultados de una elección se hayan visto afectados. Identificar y mitigar vulnerabilidades es una práctica de seguridad importante.

✗ **Rumor:** Las vulnerabilidades en la tecnología electoral significan que las elecciones han sido pirateadas y los piratas informáticos pueden cambiar los resultados electorales.

Conozca los hechos: Como todos los sistemas digitales, las tecnologías utilizadas para administrar las elecciones tienen vulnerabilidades. Los funcionarios electorales utilizan diversos controles tecnológicos, físicos y procesales para ayudar a salvaguardar estos sistemas y la integridad de los procesos electorales que respaldan. Las vulnerabilidades identificadas deben tomarse en serio y las mitigaciones deben implementarse de manera oportuna. Identificar y mitigar vulnerabilidades es una parte clave de las prácticas habituales de ciberseguridad.

Las mitigaciones incluyen la instalación de parches de software, la implementación de salvaguardias físicas y de procedimiento y la aplicación de controles técnicos compensatorios. Estas salvaguardas y controles de compensación incluyen medidas que buscan identificar y mitigar vulnerabilidades antes de su posible explotación, así como aquellas que ayudan a detectar y recuperarse de un mal funcionamiento o una explotación real o intentada de vulnerabilidades conocidas o de día cero. Es importante tener en cuenta que no hay indicios de que las vulnerabilidades cibernéticas hayan contribuido a que algún sistema de votación elimine, pierda o cambie votos.

Recursos útiles

- [Intelligence Community Assessment on Foreign Threats to the 2022 U.S. Elections](#), ODNI
- [Joint Statement from the Department of Justice and Homeland Security Assessing the Impact of Foreign Interference During the 2022 U.S. Mid-Term Election](#), DHS and DOJ
- [CISA Insights: Chain of Custody and Critical Infrastructure Systems](#), CISA
- [Chain of Custody Best Practices](#), EAC

- [Voting Testing and Certification Program](#), EAC
- [Voting System Standards, Testing and Certification](#), NCSL
- [Post-Election Audits](#), NCSL
- Sus funcionarios electorales locales o estatales. [EAC state-by-state directory](#)

✓ **Realidad:** Los procedimientos de manejo de papeletas de votación protegen contra la destrucción intencional o no intencional de papeletas y la manipulación.

✗ **Rumor:** Las papeletas se pueden quitar, agregar, reemplazar o destruir fácilmente sin ser detectadas, lo que altera el conteo oficial de votos.

Conozca los hechos: Los funcionarios electorales implementan distintas medidas de protección de tabulación y procesamiento de boletas diseñadas para garantizar que cada papeleta emitida en la elección pueda contarse correctamente. Estas medidas de seguridad incluyen procedimientos de cadena de custodia, requisitos de registro auditable y procesos de sondeo. Los funcionarios electorales utilizan estas medidas de seguridad para verificar que los votos sean tabulados con precisión durante el procesamiento y el conteo.

La ley federal y diversas leyes y reglamentos estatales rigen las prácticas de retención de papeletas y otros registros electorales por parte de los funcionarios electorales. Según la ley federal, las papeletas, las solicitudes, los registros y otros récords relacionados con las elecciones para cargos federales, como los de presidente y vicepresidente, miembros del Senado o la Cámara de Representantes de los EE. UU., deben conservarse y guardarse durante 22 meses a partir de la fecha de la elección. Aparte de su preservación, muchas jurisdicciones estatales, locales y territoriales requieren protocolos de seguridad específicos para las papeletas electorales almacenadas y otros registros electorales, como el almacenamiento en una bóveda segura con sistemas de doble bloqueo que solo se pueda abrir cuando los representantes autorizados de ambos partidos políticos estén presentes. Este tipo de requisito común tiene por objeto garantizar que todas las papeletas y los registros pertinentes se conserven intactos luego de las elecciones en caso de que se necesiten para recuentos, auditorías u otros procesos posteriores a las elecciones.

Los funcionarios electorales pueden destruir o desechar las papeletas y otros registros electorales que deban conservarse después de los períodos de conservación aplicables establecidos en los requisitos federales, estatales y/o locales. Los funcionarios electorales pueden descartar otros materiales electorales que no estén sujetos a requisitos de retención en cualquier momento.

Las imágenes o videos de funcionarios electorales descartando papeles pueden parecer sospechosos cuando se ven fuera de contexto, pero es probable que representen el manejo legal de materiales electorales.

Recursos útiles

- 52 U.S.C. § 20701
- [Federal Law Constraints on Post-Election "Audits"](#), DOJ
- [CISA Insights: Chain of Custody](#), CISA
- [Chain of Custody Best Practices](#), EAC
- [Task force of Vote Verification: Post-election Audit Recommendations](#), NASS
- [Retention Chart for Boards of Elections](#), State of Ohio
- [Election Infrastructure Security](#), CISA
- [Election Infrastructure Cyber Risk Assessment and Infographic](#), CISA
- [Election FAQs](#), NASED
- Sus funcionarios electorales locales o estatales. [EAC state-by-state directory](#)

✓ **Realidad:** Las variaciones en los totales de votos para diferentes contiendas en la misma papeleta ocurren en cada elección y por sí mismas no indican fraude o problemas con la tecnología de votación.

✗ **Rumor:** Más votos en una contienda que en otras contiendas en la papeleta significa que no se puede confiar en los resultados.

Conozca los hechos: En cada elección se producen variaciones en los totales de votos para diferentes contiendas en la misma papeleta. Por ejemplo, esto puede ocurrir como resultado de "votos insuficientes".

Estas variaciones por sí mismas indican que existan problemas con la tecnología de votación o la integridad de los procesos o resultados electorales. Un voto negativo ocurre cuando un votante, intencionalmente o no, no selecciona ninguna opción en una contienda dada en su papeleta (por ejemplo, un votante vota por un candidato presidencial, pero no por ningún candidato en otras contiendas en su boleta) o, cuando un votante selecciona menos que el número máximo permitido para un concurso en particular. Los votos inferiores ocurren comúnmente en las llamadas contiendas de "votación negativa".

Por ejemplo, un votante puede optar por votar por presidente, senador y gobernador, pero no por otros cargos o iniciativas de ley que se encuentran más abajo en su boleta. Incluso si una papeleta incluye un voto negativo en una contienda en particular, se cuentan los votos debidamente marcados en su boleta.

Recursos útiles

- Sus funcionarios electorales locales o estatales. [EAC state-by-state directory](#)
- [Voter Intent Laws](#), NCSL
- [Post-Election Audits](#), NCSL
- [Election FAQs](#), NASED

 **Realidad: Sólidas garantías que incluyen procedimientos de escrutinio y auditoría ayudan a garantizar la precisión de los resultados oficiales de las elecciones.**

 **Rumor: Un actor malicioso podría cambiar los resultados de las elecciones sin ser detectado.**

Conozca los hechos: Los sistemas y procesos utilizados por los funcionarios electorales para tabular los votos y certificar los resultados oficiales están protegidos por varias medidas de seguridad que ayudan a garantizar la precisión de los resultados electorales. Estas salvaguardas incluyen medidas que ayudan a garantizar que los sistemas de tabulación funcionen según lo previsto, protegen contra *software* malicioso y permiten la identificación y corrección de cualquier irregularidad.

Cada estado tiene salvaguardas en el sistema de votación para garantizar que cada papeleta emitida en la elección pueda contarse correctamente. Los procedimientos estatales a menudo incluyen pruebas y certificación de los sistemas de votación, registros auditables y verificaciones de *software*, como pruebas de lógica y precisión, para garantizar que las papeletas se cuenten correctamente antes de que los resultados de las elecciones se hagan oficiales. Con estas medidas de seguridad, los funcionarios electorales pueden verificar y determinar si los dispositivos ejecutan el *software* certificado y funcionan correctamente.

Cada estado también tiene leyes y procesos para verificar los recuentos de votos antes de que los resultados se certifiquen oficialmente. Los procesos estatales incluyen procedimientos de cadena de custodia firmes, registros auditables y procesos de sondeo. La gran mayoría de los votos emitidos en esta elección se emitirán en boletas de papel o utilizando máquinas que producen un registro de auditoría en papel, lo que permite realizar auditorías de tabulación a partir del registro en papel en caso de que surja algún problema con el *software* del sistema de votación, los récords de auditoría o la tabulación. Estos procedimientos de sondeo y certificación generalmente se llevan a cabo a la vista del público, ya que normalmente se permite la presencia de representantes de partidos políticos y otros observadores, para agregar un nivel adicional de verificación. Esto significa que el *software* del sistema de votación no es un punto único de falla y dichos sistemas están sujetos a múltiples auditorías para garantizar su precisión y confiabilidad. Por ejemplo, algunos condados realizan múltiples auditorías, incluida una prueba de precisión y lógica poselectoral del sistema de votación, y un conteo manual bipartidista de papeletas.

Recursos útiles

- [Election Results Reporting Risks and Mitigations Infographic](#), CISA
- [Election Infrastructure Cyber Risk Assessment](#) and [Infographic](#), CISA
- [Mail-in Voting Integrity Safeguards Infographic](#), CISA
- [Mail-in Voting Processing Factors Map \(Updated October 29, 2020\)](#), CISA
- [Post-Election Process Mapping Infographic](#), CISA

- Sus funcionarios electorales locales o estatales. [EAC state-by-state directory](#)
- [Post-election audits](#), NCSL
- [Policies for Election Observers](#), NSCL
- [Election FAQs](#), NASED

✓ **Realidad: El Departamento de Seguridad Nacional (DHS) y la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) no diseñan ni auditan papeletas, ya que son procesos administrados por funcionarios electorales estatales y locales.**

✗ **Rumor: DHS o CISA imprimieron papeletas con medidas de seguridad y están auditando los resultados como una medida contra la falsificación de papeletas.**

Conozca los hechos: Aunque DHS y CISA ayudan a los estados y a las localidades a asegurar la infraestructura electoral, DHS y CISA no diseñan, imprimen, ni auditan las papeletas. Los funcionarios electorales estatales y locales administran el diseño y la impresión de las papeletas, así como la auditoría de los resultados.

Las oficinas electorales locales cuentan con medidas de seguridad y detección que hacen que sea muy difícil cometer fraude a través de papeletas falsificadas. Si bien las medidas específicas varían, de acuerdo con las leyes y prácticas electorales estatales y locales, las medidas de seguridad de las papeletas pueden incluir comparación de firmas, verificación de información, códigos de barra, marcas de agua y peso de papel exactos.

DHS y CISA operan en apoyo de los funcionarios electorales estatales y locales, y no administran elecciones ni manipulan papeletas. El papel de CISA en la seguridad electoral incluye compartir información, como indicadores de amenazas cibernéticas, con funcionarios electorales estatales y locales, así como brindar servicios técnicos de ciberseguridad (por ejemplo, análisis de vulnerabilidades) a pedido de dichos funcionarios. CISA dio fondos a una tercera parte independiente para desarrollar una herramienta de auditoría electoral de código abierto para uso voluntario de los funcionarios electorales estatales y locales. (Nota: La frase anterior se actualizó el 9 de noviembre de 2020). CISA no audita elecciones y no tiene acceso a la herramienta tal como la usan los estados.

Recursos útiles

- [Election Infrastructure Security](#), CISA
- [Election Security](#), DHS
- [Federal Role in U.S. Campaigns and Elections: An Overview](#), CRS
- [Mail-in Voting Integrity Safeguards Infographic](#), CISA
- [Mail-in Voting 2020 Risk Assessment](#), CISA
- [Risk-Limiting Audits with Arlo](#), Voting Works
- Sus funcionarios electorales locales o estatales. [EAC state-by-state directory](#)

✓ **Realidad: Los resultados de las elecciones no son definitivos hasta ser certificados. Los informes en la noche de las elecciones no son oficiales y esos resultados pueden cambiar a medida que se completa el conteo de votos.**

✗ **Rumor: Si los reportes de resultados en la noche de las elecciones cambian en los días o semanas siguientes, el proceso está pirateado o comprometido, por lo que no puedo confiar en los resultados.**

Conozca los hechos: El cronograma para informar los resultados de las elecciones puede verse afectado por una serie de factores, incluidos los cambios en las políticas estatales o locales que afectan la forma en que se manejan las elecciones, los cambios en el momento en que se pueden procesar las papeletas o la implementación de protocolos adicionales para facilitar la votación y procesamiento seguro de votos durante la pandemia.

Los resultados de las elecciones que se reportan en la noche de elecciones no son siempre oficiales y se entregan únicamente para la conveniencia de los votantes. De hecho, ningún estado exige que los resultados oficiales se certifiquen la misma noche de las elecciones. Fluctuaciones en los informes de resultados no oficiales durante y

después de la noche de las elecciones a medida que se procesen y cuenten más boletas van a suceder, a menudo incluyen papeletas de votantes militares, y en el extranjero, y papeletas provisionales validadas.

Las variaciones en los procesos estatales también pueden significar que las papeletas emitidas a través de diferentes métodos (p. ej., votación anticipada en persona, votación por correo y votación el día de las elecciones) se cuenten y se notifiquen extraoficialmente en orden diferente. Los resultados oficiales se publican después de un riguroso escrutinio (verificación) y certificación por parte de los funcionarios electorales locales y estatales.

Recursos útiles

- [FBI-CISA Public Service Announcement: Foreign Actors and Cybercriminals Likely to Spread Disinformation Regarding 2020 Election Results](#)
- [Election Results Reporting Risks and Mitigations](#), CISA
- [Mail-in Voting 2020 Risk Assessment](#), CISA
- [Mail-in Voting Integrity Safeguards Infographic](#), CISA
- [Mail-in Voting Processing Factors Map \(Updated October 29, 2020\)](#), CISA
- [Post-Election Process Mapping Infographic](#), CISA
- [Checklist for Securing Election Night Results Reporting](#), EAC
- [USPS Election Mail Information Center](#), USPS
- [Federal Election Results FAQs](#), CRS
- [State Election Canvassing Timeframes and Recount Thresholds](#), NASS
- [After the Voting Ends: The Steps to Complete an Election](#), NCSL
- [Voting Outside the Polling Place: Absentee, All-Mail and Other Voting at Home Options](#), NCSL
- [Election FAQs](#), NASED

 **Realidad: Los votos provisionales se cuentan en todas las elecciones independientemente de los márgenes de resultado.**

 **Rumor: Las papeletas provisionales solo se cuentan si hay una contienda reñida.**

Conozca los hechos: Los funcionarios electorales revisan todas las boletas provisionales en cada elección, independientemente de los márgenes de resultados. Se cuentan los votos provisionales emitidos por personas cuya elegibilidad pueda ser verificada. Además, los funcionarios electorales deben proporcionar a las personas que emitieron votos provisionales información por escrito sobre cómo pueden determinar si su voto fue contado y, si no lo fue, el motivo de su rechazo.

Recursos útiles

- 52 U.S.C. § 21082
- [Post-Election Process Mapping Infographic](#), CISA
- [Provisional Ballots](#), NCSL
- [State Policies on Voting In-Person or Changing Vote After Requesting a Mail/Absentee Ballot](#), NASS
- [Election FAQs](#), NASED
- Sus funcionarios electorales locales o estatales.. [EAC state-by-state directory](#)

 **Realidad: En algunas circunstancias, a los funcionarios electorales se les permite “duplicar” las papeletas para asegurarse de que se puedan contar correctamente.**

 **Rumor: Presenciar a los funcionarios electorales marcando papeletas significa que se está realizando una votación fraudulenta.**

Conozca los hechos: Los votantes no siempre envían papeletas que puedan ser interpretadas con precisión por un escáner de papeletas debido a problemas, como daños, errores de imprenta y/o marcas ambiguas en la papeleta. Los funcionarios electorales aplican las reglas de la jurisdicción para determinar la intención del votante según las marcas en dichas boletas y capturan los votos válidos de las boletas en los resultados de las elecciones a través de diversos procesos electrónicos y/o manuales.

La duplicación de boletas es un proceso mediante el cual los funcionarios electorales transfieren cuidadosamente las selecciones de un votante en una papeleta que no se pueda escanear, a una papeleta duplicada para que pueda ser leída por un escáner de papeletas. Tanto la papeleta original como la duplicada se etiquetan y registran para que las dos boletas se puedan rastrear y auditar.

Muchas jurisdicciones requieren equipos bipartidistas de dos o cuatro personas para completar este proceso y verificar que los votos se transfieran con precisión a las papeletas duplicadas. El proceso a menudo está abierto a la observación pública.

En algunas jurisdicciones, la duplicación de papeletas se denomina reelaboración de papeletas, réplica de papeletas o transcripción de papeletas.

Recursos útiles

- [After the Voting Ends: The Steps to Complete an Election](#), NCSL
- [Ballot Duplication blog series](#), Council of State Governments Overseas Voting Initiative
- Sus funcionarios electorales locales o estatales. [EAC state-by-state directory](#).

✓ Realidad: Los resultados que se muestran a través de los sitios en línea que reportan los resultados electorales no son oficiales y están sujetos a cambios hasta que se certifiquen dichos resultados. Una interrupción, degradación u otro problema que afecte la integridad o disponibilidad de la información que se muestra en dichos sitios no afecta el conteo de votos ni la precisión de los resultados oficiales certificados.

✗ Rumor: Si un sitio de reportes en la noche de las elecciones experimenta una interrupción, se degrada o muestra resultados incorrectos, los conteos de votos se perderán o manipularán.

Conozca los hechos: Los funcionarios electorales utilizan sitios en línea para compartir resultados no oficiales con el público a medida que se van contando los votos y se llevan a cabo otros procesos de gestión de resultados.

Los resultados que se muestran en estos sitios no son oficiales y pueden actualizarse, según sea necesario, hasta que los resultados oficiales sean certificados. Estos sitios pueden experimentar interrupciones debido a una variedad de problemas, incluido un alto volumen de tráfico de Internet o incidentes cibernéticos. Los incidentes cibernéticos, así como los errores humanos o tecnológicos, también pueden dar lugar a que se muestre información inexacta en estos sitios. Como estos sitios en línea no están conectados a ninguna parte del sistema de votación, dichas interrupciones no afectan la capacidad de los funcionarios electorales para contar las papeletas o la precisión de los resultados oficiales certificados.

Recursos útiles

- [FBI-CISA Public Service Announcement: Foreign Actors and Cybercriminals Likely to Spread Disinformation](#)
- [Election Results, Canvass, and Certification](#), EAC
- [Post-Election Process Mapping Infographic](#), CISA
- [Federal Election Results FAQs](#), CRS
- [Election FAQs](#), NASED

✓ Realidad: Los actores maliciosos pueden usar identidades falsas y hacerse pasar por cuentas reales.

✗ Rumor: Si una cuenta de redes sociales se atribuye una identidad, la cuenta debe ser administrada por esa persona u organización.

Conozca los hechos: Los actores maliciosos a menudo usan identidades falsas y se hacen pasar por cuentas reales con el fin de engañar al público para hacerle creer la desinformación, incluyendo la desinformación relacionada con

temas electorales. La suplantación de identidad por parte de los adversarios no es una táctica nueva. Por ejemplo, los delincuentes cibernéticos maliciosos a veces intentan falsificar sitios web y direcciones de correo electrónico para engañar a las personas y lograr que hagan clic en enlaces o compartan información personal. Crear identidades falsas en las redes sociales es simplemente otro enfoque para engañar a los usuarios.

Algunas plataformas de redes sociales ofrecen herramientas de verificación de identidad para ayudar a los usuarios a identificar las cuentas verificadas por la plataforma. Estos sistemas pueden ser útiles para hallar cuentas que sean fuentes oficiales de información. La mayoría de las plataformas de redes sociales también ofrecen métodos para que los usuarios sepan si una cuenta ha violado las normas de la plataforma en lo referente a perfiles suplantados.

Como práctica recomendada, busque fuentes confiables tales como su oficina electoral local, para obtener información relacionada con las elecciones.

Recursos útiles

- [#TrustedInfo2024](#), NASS
- Voter Resources: [State Voter Information](#), NASED
- [Voting and Elections Information](#), usa.gov
- Su directorio de funcionarios electorales locales o estatales. [EAC state-by-state directory](#)

✓ **Realidad: Los actores cibernéticos pueden "suplantar" o falsificar direcciones de remitentes de correo electrónico para que parezca que provienen de otra persona.**

✗ **Rumor: Recibí un correo electrónico relacionado con las elecciones que parece provenir de cierta organización, por lo que la organización debe haberlo enviado.**

Conozca los hechos: Los actores cibernéticos pueden falsificar correos electrónicos para que parezca que provienen de otra persona. Esta táctica común se denomina falsificación de correo electrónico, en la que los atacantes envían un correo electrónico que aparenta ser de un dominio u organización específicos en un intento de capturar datos personales o propagar *malware*. Dichos correos electrónicos falsificados también pueden ser utilizados para difundir información falsa o incendiaria.

Para enviar correos electrónicos que parezcan realistas, los ciberdelincuentes pueden falsificar la dirección del remitente para ocultar el origen de un correo electrónico o configurar dominios falsificados que tienen un nombre ligeramente diferente del dominio real. Siempre tenga cuidado con correos electrónicos inusuales y busque fuentes confiables para verificar, como el sitio en línea oficial de la organización. Nunca proporcione información personal ni descargue archivos de correos electrónicos sospechosos. Si recibe un correo electrónico sospechoso relacionado con las elecciones, considere informarlo a su funcionario electoral local o a la oficina local del FBI.

Recursos útiles

- [FBI-CISA Public Service Announcement: Spoofed Internet Domains and Email Accounts Pose Cyber and Disinformation Risks to Voters](#)
- [Actions to Counter Email-based Attacks on Election-Related Entities](#), CISA
- [Enhanced Email and Web Security](#), CISA