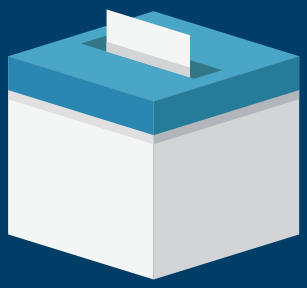
Recursos de seguridad
para el subsector de infraestructura electoral



La **Agencia de Seguridad de Infraestructura y Ciberseguridad** (CISA, por sus siglas en inglés) y el **Buró Federal de Investigaciones** (FBI, por sus siglas en inglés) han elaborado un listado de recursos que están disponibles en todo el gobierno federal para que los funcionarios electorales estatales, locales, territoriales y tribales, y sus socios del sector privado, ayuden a afrontar las amenazas contra la plantilla laboral y brindar orientación sobre la evaluación y mitigación de los riesgos relativos a sus bienes materiales.

Si bien muchos de estos recursos no se centran de manera explícita en la seguridad electoral, es posible que el subsector de la infraestructura electoral los considere útiles en el cumplimiento de su trabajo. Dado que las líneas que separan la seguridad física de la ciberseguridad se vuelven más imprecisas cada vez más, en este documento se han incluido asimismo recursos exclusivos que se focalizan en la ciberseguridad. El usuario puede acceder gratuitamente a todos los recursos aquí mencionados, los que se encuentran en los sitios web que figuran a continuación.

Amenazas contra los funcionarios electorales y la infraestructura electoral

En respuesta al aumento de amenazas de violencia contra funcionarios electorales después de las elecciones estadounidenses de 2020, tanto el FBI como la CISA priorizaron sus esfuerzos para encarar dichas amenazas. Ambos organismos toman en serio todo tipo de amenaza de violencia, incluso aquellas contra los funcionarios electorales a causa de la función fundamental de estos de proteger el proceso electoral en pro de todos los votantes. El Departamento de Justicia (DOJ, por sus siglas en inglés) estableció el "Equipo operativo contra las amenazas a funcionarios electorales" con el objeto de investigar enérgicamente estas amenazas y enjuiciar a los responsables. De usted ser un funcionario electoral víctima de esta amenaza, sírvase seguir los pasos a continuación.

- Si hay una amenaza inminente contra la vida, llame al 911.
- Denuncie las amenazas. Comuníquese con el **coordinador contra los delitos electorales** de la oficina local del FBI (www.fbi.gov/contact-us/field-offices), envíe información en línea por tips.fbi.gov o llame al 1-800-CALL-FBI (225-5324) seleccionando "Prompt 1" [Opción 1] y luego escogiendo "Prompt 3" [Opción 3]. La mejor manera de denunciar las amenazas contra las elecciones es comunicándose con el coordinador contra los delitos electorales de la oficina local del FBI.
- Por último, póngase en contacto con la oficina regional de la CISA para obtener orientación sobre los riesgos a la seguridad física que se adecúe a su jurisdicción e instalaciones. Los asesores en materia de seguridad preventativa (PSA, por sus siglas en inglés) de la CISA pueden realizar evaluaciones, como, por ejemplo, utilizando la herramienta de *Security Assessment and First Entry* [Evaluación de seguridad respecto al primer ingreso, SAFE, por sus siglas en inglés], que ponen de relieve las vulnerabilidades de su infraestructura electoral física, incluidas las oficinas electorales, los sitios donde se procesan las papeletas, los almacenes, los centros de votación y demás instalaciones electorales. Encuentre la PSA local aquí: www.cisa.gov/cisa-regions.

La protección de la seguridad física: documentos de orientación y demás recursos

- La publicación de la CISA titulada **Preparación con respecto a la seguridad física en los centros de votación y las instalaciones electorales [Physical Security Preparedness at Voting Locations and Election Facilities]** facilita a los funcionarios electorales adoptar medidas útiles para tomar decisiones que mejoren su postura en cuanto a la seguridad física y la resilencia de las operaciones electorales en su jurisdicción.
  www.cisa.gov/sites/default/files/publications/physical-security-of-voting-location-election-facilities_v2_508.pdf
- Los productos **Última milla [Last Mile]** de la CISA son herramientas que los funcionarios electorales pueden personalizar y emplear para mejorar la seguridad de su infraestructura. Algunos de estos productos son: Election Security Planning Snapshot [Imagen breve para la planificación de la seguridad electoral], Election Emergency Response Guides [Guías para abordar las emergencias electorales], Election Safeguards [Salvaguardias electorales], y otros formularios. Para obtener más información o solicitar un producto Última milla personalizado, póngase en contacto a través de electionsecurity@hq.dhs.gov
- La publicación de CISA titulada **Guía informativa y resumen de un plan de seguridad para sitios que carecen de seguridad y que son accesibles a muchedumbres [Soft Targets and Crowded Places Security Plan Overview and Resource Guide]** proporciona información relevante a socios de los sectores público y privado para mejorar su preparación y seguridad.
  www.cisa.gov/sites/default/files/publications/DHS-Soft-Target-Crowded-Place-Security-Plan-Overview-052018-508_0.pdf
  www.cisa.gov/sites/default/files/publications/19_0424_cisa_soft-targets-and-crowded-places-resource-guide.pdf
- La publicación de la CISA titulada **Protección de la infraestructura durante manifestaciones públicas [Protecting Infrastructure During Public Demonstrations]** ofrece sugerencias de seguridad a empresas que pueden ser víctimas de delitos durante manifestaciones públicas.
  www.cisa.gov/sites/default/files/publications/protecting_infrastructure_during_public_demonstrations_508.pdf
- La publicación de la CISA titulada **Mitigación de los efectos de las publicaciones de mala fe en la infraestructura crítica [Mitigating the Impacts of Doxing on Critical Infrastructure]** define y proporciona ejemplos de publicaciones de mala fe, explica el posible impacto que dichas publicaciones podrían tener en la infraestructura crítica, y ofrece medidas de protección y prevención, opciones de mitigación, y recursos adicionales para personas y organizaciones.
  www.cisa.gov/sites/default/files/publications/cisa_insights_mitigating_the_impacts_of_doxing_508.pdf
- La publicación de la Oficina del Director de Inteligencia Nacional (ODNI, por sus siglas en inglés) titulada **Guía contra el terrorismo para el personal del ámbito de la seguridad pública [Counterterrorism Guide for Public Safety Personnel]** ayuda a los servicios de emergencias a identificar y dar parte de actividades sospechosas, detectar indicadores de que se va a efectuar un acto violento, y responder a ataques terroristas y mitigarlos.
  www.dni.gov/nctc/jcat/index.html

Sitios web clave/Información de contacto

- La página web de la CISA **Seguridad electoral [Election Security]** contiene todos los recursos y herramientas de seguridad electoral de la CISA, incluso todos los recursos del gobierno federal que se detallan en este documento: www.cisa.gov/election-security.
- El sitio web de la CISA **Programa de seguridad de nuestras ciudades natales [Hometown Security Program]** proporciona herramientas y recursos para respaldar la seguridad y la resilencia comunitarias. Visite www.cisa.gov/hometown-security.
- La página web de la CISA **Comisión interinstitucional en materia de seguridad [Interagency Security Committee]** aborda la seguridad continua en todo el gobierno para las instalaciones federales y ha elaborado muchas normas, políticas y documentos de mejores prácticas que las personas y las organizaciones pueden examinar en www.cisa.gov/isc.
- La página web de la CISA de la **Oficina para la prevención de atentados con bomba [Office for Bombing Prevention]** proporciona toda clase de recursos, capacitaciones, herramientas y productos para ayudar a las autoridades estatales y locales, los socios privados, y demás personas a entender y mitigar la amenaza que suponen los artefactos explosivos improvisados y proteger la infraestructura crítica. Visite www.cisa.gov/obp.
- **CISA Central** es el núcleo de CISA donde los socios y las partes interesadas pueden pedir asistencia y servicios relacionados a la infraestructura crítica. CISA Central opera las 24 horas del día y los siete días de la semana. Póngase en contacto escribiendo a Central@cisa.gov o llamando al 888-282-0870.
- Por medio de la línea de información del FBI, **FBI Tip Line**, se pueda dar parte de amenazas y delitos relacionados con las elecciones o de cualquier otra índole. Visite https://tips.fbi.gov o llame al 1-800-CALL-FBI (225-5324).
- La página web del FBI **Delitos y seguridad electorales [Election Crimes and Security]** proporciona información con relación al reconocimiento y denuncia de delitos electorales. Visite www.fbi.gov/elections.
- La iniciativa del FBI **Voces protegidas [Protected Voices]** proporciona herramientas y recursos a campañas políticas, compañías y personas para protegerse de las operaciones de influencia por parte de gobiernos extranjeros y de ciberamenazas. Visite www.fbi.gov/protectedvoices.
- La página web **Herramientas para los servicios de emergencia [First Responder Toolbox]** del Centro Nacional contra el Terrorismo (NCTC, por sus siglas en inglés) de la ODNI brinda información que ayuda a prepararse, coordinar y reaccionar, y a fortalecer la seguridad, la protección y las investigaciones de las partes interesadas que laboran en contra del terrorismo. Visite www.dni.gov/index.php/nctc-how-we-work/joint-ct-assessment-team/first-responder-toolbox.
- **La Comisión de Asistencia Electoral de los EE. UU. (EAC, por sus siglas en inglés)** es la oficina de información a nivel nacional sobre la administración electoral. Tiene recursos adicionales con respecto a la seguridad electoral, los que pueden accederse en www.ac.gov/election-officials/election-security.

Capacitación y ejercicios

- Las **sesiones de capacitación en seguridad electoral por parte de la CISA** proporcionan más orientación a las partes interesadas electorales en el manejo del riesgo y el fortalecimiento de la resilencia de la infraestructura electoral. Para programar sesiones de capacitación u obtener más información, envíe un correo electrónico a electionsecurity@hq.dhs.gov.
- La **Comisión interinstitucional en materia de seguridad de la CISA** se centra en la seguridad de todas las instalaciones federales y proporciona cursos de capacitación en línea e interactivos que pueden ser útiles para la seguridad de su infraestructura física. Visite www.cisa.gov/interagency-security-committee-training.
- La **Oficina para la prevención de atendados con bomba de la CISA (OBP por sus siglas en inglés)** imparte capacitaciones en persona, virtuales y de estudio independiente en línea. Estos cursos ayudan a las partes interesadas públicas y privadas a mejorar su percatación de la amenaza que representan los artefactos explosivos improvisados, y su respuesta a estos. Visite tripwire.dhs.gov/training-education/counter-ied-training-0.
- Los **ejercicios de la CISA**, incluidos los ejercicios de simulación, proporcionan entrenamientos que se basan en situaciones hipotéticas para ayudar a identificar áreas a mejorarse, compartir las mejores prácticas y mejorar la preparación contra amenazas a la infraestructura y la plantilla laboral electorales. Visite www.cisa.gov/critical-infrastructure-exercises.

Advertencias y anuncios de servicio público

- El **Centro para analizar e intercambiar información sobre la infraestructura electoral [Elections Infrastructure Information Sharing and Analysis Center, EL-ISAC, por sus siglas en inglés]** ofrece un conjunto de recursos sobre la seguridad electoral, entre estos, productos de inteligencia sobre amenazas, seguimiento de amenazas y vulnerabilidades, reacción y remedio en conexión a casos, y otros productos y servicios. Visite www.cisecurity.org/ei-isac/.
- El **Centro de denuncias de delitos en línea [FBI Internet Crime Complaint Center, IC3, por sus siglas en inglés]** acepta denuncias en línea de víctimas de delitos en internet y publica alertas, tanto de la industria como de los consumidores, sobre cuestiones relacionadas con delitos en internet. Visite www.ic3.gov.
- El **Sistema nacional de ciberconcienciación [National Cyber Awareness System, NCAS, por sus siglas en inglés]** almacena las alertas de la CISA con respecto a cuestiones y vulnerabilidades de seguridad actuales. Visite www.cisa.gov/uscert/ncas/alerts.