#PROTEGE2024

NUESTRA MISIÓN

Ayudar a los funcionarios electorales y a las partes involucradas en la infraestructura electoral a protegerse contra los riesgos de seguridad cibernética, física y operativa en la infraestructura electoral durante las elecciones de 2024.

NUESTRAS PRIORIDADES

1. Mejorar el nivel de comprensión que las partes involucradas en las elecciones tienen acerca de los riesgos a la infraestructura electoral.
2. Asistir a las partes involucradas en la infraestructura electoral para tomar medidas con el fin de mitigar riesgos.
3. Ayudar a las partes involucradas en las elecciones a garantizar que la infraestructura electoral esté preparada.
4. Proporcionar advertencias y respuestas de inteligencia contra amenazas a las partes involucradas en las elecciones.
5. Facilitar la integración y coordinación operativa por parte del gobierno federal.

APOYO DE CISA A LAS PARTES INVOLUCRADAS EN LA INFRAESTRUCTURA ELECTORAL

En todo el país, CISA está trabajando para ayudar a las partes involucradas en la infraestructura electoral a comprender y manejar el riesgo en las elecciones de 2024. Esto lo logramos de tres maneras: 1) información compartida; 2) servicios de seguridad voluntarios y gratuitos y 3) capacitaciones sin costo alguno. CISA comparte información a través de múltiples medios, desde publicar productos que explican los riesgos cibernéticos, físicos y operativos para la infraestructura electoral y los pasos para mitigarlos, hasta trabajar con la comunidad de inteligencia y otros colaboradores para proporcionar el nivel de comprensión más actualizado acerca del panorama de amenazas. CISA ofrece una gama de servicios voluntarios y gratuitos, como el escaneo continuo de los sistemas y redes de infraestructura electoral, en busca de vulnerabilidades en el Internet y asistencia para la gestión de respuesta a incidentes. También financiamos servicios de seguridad adicionales, como programas de respuesta y para la detección en terminales a través del EI-ISAC. CISA también ofrece capacitaciones sin costo, tales como los ejercicios de simulación y análisis profundos en temas específicos referentes a amenazas.

El equipo de expertos en seguridad de infraestructura crítica de CISA a lo largo del país también ofrece apoyo local personalizado a las partes involucradas en la infraestructura electoral. Los asesores de ciberseguridad de CISA pueden llevar a cabo evaluaciones cibernéticas *in situ* y proporcionar una orientación de ciberseguridad más definida en función de la postura de seguridad específica de una organización. Del mismo modo, los asesores de seguridad de protección de CISA pueden evaluar la infraestructura física y dar opciones que se deben tener en cuenta para reducir la vulnerabilidad a las amenazas físicas. Es importante notar que cada una de las 10 regiones de CISA tiene ahora un Asesor de Seguridad Electoral (ESA, por sus siglas en inglés) que opera tal como un "Navegador CISA" dentro de las partes involucradas en las elecciones. Los ESAs supervisan el apoyo de seguridad electoral de CISA en cada región y trabajan de manera conjunta con las oficinas electorales estatales para garantizar que CISA sea ágil en satisfacer las necesidades únicas de cada estado. Los ESA aprovechan su experiencia como exadministradores electorales, para ayudar a CISA a identificar y priorizar rápidamente los riesgos más serios, y conectar a las partes involucradas (funcionarios estatales, funcionarios locales y proveedores electorales) con los recursos, servicios y herramientas de mitigación apropiados.

PRIMERO LO PRIMERO...

PASOS ESENCIALES PARA MEJORAR SU POSICIÓN DE SEGURIDAD EN EL 2024

1. **Habilite la autenticación multifactorial (MFA).** Las contraseñas por sí solas no siempre son eficaces para proteger los datos de su organización. Exigir el uso de MFA es una forma simple de proteger su organización y puede prevenir ataques de riesgo a sus cuentas.
2. **Conozca y maneje sus vulnerabilidades cibernéticas.** Conozca y maneje las vulnerabilidades que los actores maliciosos pueden ver en los sistemas de su organización que se encuentran conectados al internet. Regístrese para el Escaneo Gratuito de Vulnerabilidades de Higiene Cibernética de CISA, enviando un correo electrónico a **vulnerability@cisa.dhs.gov**.
3. **Obtenga una evaluación de seguridad física.** Conozca su posición de seguridad física poniéndose en contacto con los miembros de su equipo regional de CISA o con sus colaboradores en el manejo de emergencias, para hablar sobre la posibilidad de recibir una evaluación de seguridad física sin costo alguno.
4. **Adquiera un dominio .gov.** Haga la transición de su sitio web y correo electrónico a un dominio .gov para que el público pueda identificarlo a usted y su entidad como sitios oficiales del gobierno más fácilmente y para protegerse contra los riesgos de ciberseguridad y suplantación de identidad.
5. **Practique su plan de respuesta a incidentes.** La respuesta a incidentes es un esfuerzo de equipo. Trabaje con su equipo y otros asociados, tales como los organismos de seguridad locales, los proveedores de servicios críticos y otras oficinas gubernamentales, para practicar su plan de respuesta a incidentes, con el fin de evitar que la primera vez que lo use no sea durante una crisis. Póngase en contacto con su equipo regional de CISA para solicitar un ejercicio de simulación de CISA (TTX).
6. **Únase al ISAC de INFRAESTRUCTURA ELECTORAL (EI-ISAC,** por sus siglas en inglés**).** La membresía al EI-ISAC está abierta a todas las organizaciones estatales, locales, tribales y territoriales de los Estados Unidos que apoyen a los funcionarios electorales. La membresía es voluntaria y gratuita para los participantes, y brinda acceso a una variedad de servicios de seguridad sin costo alguno. Únase al IE-ISAC en línea a través de **learn.cisecurity.org/ei-isac-registration**.

PROTEJA SU...

Las siguientes acciones pueden ayudar a mejorar la seguridad de su correo electrónico:

- **Regístrese para bloquear y denunciar dominios maliciosos:** Bloquea los intentos para conectarse a dominios web dañinos reconocidos. Este es un recurso gratuito para los miembros de la IE-ISAC.
- **Implemente la autenticación multifactorial para las cuentas.**
- **Suscríbase a programas de respuesta y para la detección en terminales:** Se implementan en las terminales con el fin de identificar, detectar, responder y remediar incidentes y alertas de seguridad. Este es un recurso gratuito para los miembros de la IE-ISAC.
- **Haga la transición a un dominio .GOV:** Hace que las cuentas de correo electrónico y los sitios web sean fácilmente identificados como parte de una organización gubernamental con el fin de protegerse contra la suplantación de identidad.

Las siguientes acciones pueden ayudar a proteger sus sitios web oficiales:

- **Regístrese para el análisis de aplicaciones web:** Evalúa el estado de sus aplicaciones web con acceso público al buscar vulnerabilidades y configuraciones deficientes.
- **Utilice los servicios de protección DDoS:** Puede encontrar los servicios ofrecidos gratuitamente por parte de los colaboradores de CISA en el sector privado en nuestra página de servicios.
- **Haga la transición a un dominio .GOV:** Hace que las cuentas de correo electrónico y los sitios web sean fácilmente identificados como parte de una organización gubernamental con el fin de protegerse contra la suplantación de identidad.

Las siguientes acciones pueden ayudar a mejorar su red electoral:

- **Regístrese para el escaneo gratuito de vulnerabilidades de higiene cibernética de CISA:** Proporciona a los inscritos un informe recurrente sobre vulnerabilidades y otras condiciones explotables visibles desde Internet, dando prioridad a aquellas que se sabe son explotadas por partes adversarias.
- **Implemente la autenticación multifactorial para las cuentas.**
- **Suscríbase a programas de respuesta y para la detección en terminales:** Se implementan en las terminales con el fin de identificar, detectar, responder y remediar incidentes y alertas de seguridad. Este es un recurso gratuito para los miembros de la IE-ISAC.
- **Utilice los sensores Albert:** El EI-ISAC ofrece sistemas para la detección de intrusos que son administrados y monitoreados las 24 horas del día, los 7 días de la semana, y que permiten la detección de tráfico malicioso dirigido a redes estatales, locales, tribales y territoriales (SLTT, por sus siglas en inglés).

Las siguientes acciones pueden ayudar a proteger sus sistemas electorales:

- **Implemente protocolos y políticas efectivas para la cadena de custodia.**
- **Explore las mejores prácticas de CISA para asegurar los sistemas electorales:** Las organizaciones pueden implementar estas mejores prácticas con el fin de reforzar las redes empresariales y fortalecer la infraestructura electoral, a bajo costo o sin costo alguno.
- **Revise la Guía para la Mitigación de Amenazas Internas a la Infraestructura Electoral de CISA:** Tome medidas para mitigar las posibles amenazas.

Las siguientes acciones pueden ayudar a proteger su oficina electoral:

- **Solicite una evaluación de seguridad física:** Una evaluación de seguridad de primer acceso (SAFE, por sus siglas en inglés) ayuda a identificar vulnerabilidades de seguridad física de alto nivel y proporciona opciones de mitigación.
- **Solicite capacitaciones de CISA sobre diversos temas de amenazas a la seguridad:** CISA ofrece capacitaciones presenciales o virtuales sobre una variedad de temas de amenazas físicas y cibernéticas, tales como la preparación contra tiradores activos y amenazas de bombas.
- **Solicite un Ejercicio de Simulación (TTX) de CISA para practicar su Plan de Respuesta a Incidentes:** CISA ofrece TTX presenciales o virtuales sin costo alguno, adaptados a las partes interesadas en las elecciones estatales y locales.

Las siguientes acciones pueden ayudar a proteger su oficina electoral:

- **Revise las Guías de mejores prácticas de seguridad de CISA en el sitio web de #PROTECT2024** que cubren la seguridad individual y la seguridad personal.
- **Establezca estrictos controles de seguridad** en todas las cuentas profesionales y personales.
Limite la información de identificación personal disponible públicamente. Encuentre más información en la guía de CISA para "Mitigar los impactos del *doxing* en la infraestructura crítica".

#PROTECT2024 CAPACITACIONES Y SERVICIOS DE CISA

Capacitaciones de CISA para la Seguridad Electoral

Capacitaciones sin costo alguno y que se pueden dictar en persona o virtualmente. Cada una suele durar entre 30 y 90 minutos.
Para obtener más información o solicitar una capacitación, envíe un correo electrónico a electionsecurity@cisa.dhs.gov.

Capacitaciones específicas de seguridad

- Descripción CISA de la seguridad electoral
- Generar confianza a través de prácticas seguras
- Técnicas de no confrontación para trabajadores electorales
- Mantener seguras las oficinas electorales locales
- Amenazas internas
- Inteligencia Artificial Generativa y Operaciones de Influencia Maliciosa Extranjera

Capacitaciones en riesgos cibernéticos

- Phishing
- Ransomware

Capacitaciones en riesgo físico

- Preparación ante tiradores activos
- Preparación ante amenazas de bombas
- Identificación y respuesta de artículos sospechosos

Capacitaciones en resiliencia operativa

- Preparación en Comunicaciones de Emergencia
- Planificación en comunicaciones "PACE"

Ejercicios de Simulación CISA para la Seguridad Electoral (TTXs)

TTXs estatales y locales en persona o virtuales sin costo para ayudar a las partes interesadas a practicar sus planes de respuesta a incidentes. Para solicitar un ejercicio, envíe un correo electrónico a **cisa.exercises@cisa.dhs.gov** o comuníquese con el personal de CISA en su región.

Seguridad electoral "*TTX in a Box*": Escenarios de seguridad electoral actualizados para el entorno de amenazas electorales en 2024 que están listos para ser utilizados por los funcionarios electorales con el fin de entrenar a sus equipos. Para obtener más información, visite **cisa.gov/CTEPS**

7ª Simulacro anual de votación: Únase a nosotros en agosto de 2024 para el séptimo simulacro anual de seguridad electoral nacional de CISA que brinda la oportunidad para que los gobiernos SLTT, los miembros electorales en el sector privado, los comités políticos nacionales y otros miembros de la comunidad electoral se reúnan, planifiquen para diversos escenarios y mejoren los planes de respuesta. Póngase en contacto con su ESA de CISA o diríjase a **TTXvote@cisa.dhs.gov regional** para obtener más información.

Evaluaciones físicas y de ciberseguridad

Los asesores de seguridad de CISA están disponibles en todas las regiones de CISA para llevar a cabo evaluaciones de seguridad cibernética y física con el fin de ayudar a las organizaciones SLTT a crear programas de seguridad cibernética y física que sean robustos y firmes. Póngase en contacto con el personal regional de CISA para solicitar una evaluación: **cisa.gov/about/regions**.

Servicios CISA de Ciberseguridad

Regístrese en los servicios cibernéticos voluntarios y sin costo de CISA, tales como: Escaneo de vulnerabilidades de higiene cibernética para conocer las vulnerabilidades que los actores maliciosos pueden ver en los sistemas conectados a internet en su organización. CISA también ofrece análisis de aplicaciones web para evaluar las aplicaciones web de acceso público y descubrir vulnerabilidades y configuraciones incorrectas que puedan ser explotadas. Inscríbase aquí: **cisa.gov/cyber-hygiene-services.**

Productos “Última Milla” personalizados en mejores prácticas de seguridad

La iniciativa CISA de “Última Milla” proporciona a los administradores electorales y a sus colaboradores una gama de recursos personalizables basados en las mejores prácticas de seguridad y los estándares de la industria con el fin de proteger la infraestructura electoral en todo el país.
Póngase en contacto con **electionsecurity@cisa.dhs.gov** para desarrollar sus propios productos de última milla y visite **cisa.gov/last-mile-products** para descargar el "Kit de herramientas de última milla", que proporciona una descripción general de los esquemas de productos personalizables.

Biblioteca de recursos de seguridad electoral

La biblioteca de recursos de seguridad electoral de CISA proporciona recursos informativos voluntarios para ser usados por los gobiernos estatales, locales, tribales y territoriales (SLTT, por sus siglas en inglés), las organizaciones del sector privado que colaboran con la infraestructura electoral y el público en general.

#PROTECT2024 LISTA DE VERIFICACIÓN

PRIMERO LO PRIMERO: SI NO HACE NADA MÁS, PRIORICE ESTO:

- [ ] Implemente la autenticación multifactorial para todas las cuentas oficiales de red, cuentas de correo electrónico y cuentas de redes sociales.
- [ ] Regístrese para el escaneo de vulnerabilidades de higiene cibernética y el escaneo de aplicaciones web gratuitos de CISA. Coordine con su asesor de ciberseguridad (CSA) local de CISA para ayudar a garantizar que su oficina solucione cualquier vulnerabilidad identificada.
- [ ] Solicite una evaluación de seguridad física de CISA sin costo para sus instalaciones electorales, si aún no ha tenido una.
- [ ] Haga la transición de su correo electrónico y sitio web a un dominio .gov. Configúrelos para que cualquier tráfico a sus direcciones de correo electrónico y sitio web existentes se reenvíe al nuevo correo electrónico o dirección .gov. Así no pueda hacer la transición a .gov este año, aún puede reservar el dominio de su jurisdicción.
- [ ] Regístrese en un simulacro de CISA para practicar su plan de respuesta a incidentes.
- [ ] Únase al EI-ISAC para acceder a información sobre amenazas que se comparte en tiempo real y a otros recursos y servicios gratuitos.

CIBERNÉTICA

- [ ] Solicite capacitaciones CISA en persona o virtuales acerca de *phishing* y *ransomware*.
- [ ] Solicite una sesión informativa por parte de su CSA local sobre los servicios de ciberseguridad de CISA y cómo estos podrían ayudar a su oficina.
- [ ] Obtenga el programa para respuesta y detección en terminales para los sistemas de su oficina. Este es un recurso gratuito para los miembros del IE-ISAC.
- [ ] Implemente el bloqueo y la generación de informes de dominios maliciosos para ayudar a protegerse contra el acceso no intencional a sitios maliciosos. Este es un recurso gratuito para los miembros del IE-ISAC.
- [ ] Lea las publicaciones CISA más recientes acerca de amenazas cibernéticas para comprender mejor el panorama de amenazas en 2024.
- [ ] Asegúrese de que todas las cuentas, incluidas las cuentas en redes sociales, tengan la configuración de seguridad más sólida posible y elimine la información de identificación personal acerca de usted, su personal o su familia que pueda estar disponible en línea.

FÍSICA

- [ ] Solicite capacitaciones CISA en persona o virtuales acerca de amenazas físicas.
- [ ] Utilice la “Lista para Verificación de Seguridad Física en los Centros de Votación" de CISA para ayudar a mitigar el riesgo en los lugares de votación.

RESILIENCIA OPERATIVA

- [ ] Solicite una capacitación CISA en persona o virtual acerca de las Comunicaciones de Emergencia y Planificación "PACE".
- [ ] Solicite productos personalizados de "Última Milla" para su estado.
- [ ] Participe en el simulacro de votación (*Tabletop the Vote*), el ejercicio anual de seguridad electoral a nivel nacional de CISA.
- [ ] Desarrolle y practique su plan para continuidad de operaciones.
- [ ] Establezca relaciones con las fuerzas del orden público a nivel estatal y local para saber a quién contactar cuando denuncie actividades delictivas.
- [ ] Desarrolle e implemente un plan de comunicaciones públicas para aumentar la comprensión que el público tiene sobre sus procesos electorales y medidas de seguridad.
- [ ] Desarrolle y practique un plan de comunicaciones de respuesta a incidentes: asegúrese de que incluya cómo responder a las tácticas comunes utilizadas en las operaciones de influencia maliciosa extranjera dirigidas a la infraestructura electoral (consulte la guía de CISA "Asegurar la infraestructura electoral contra las tácticas de operaciones de influencia maliciosa extranjera")