NAVEGADORES DE SEGURIDAD ELECTORAL

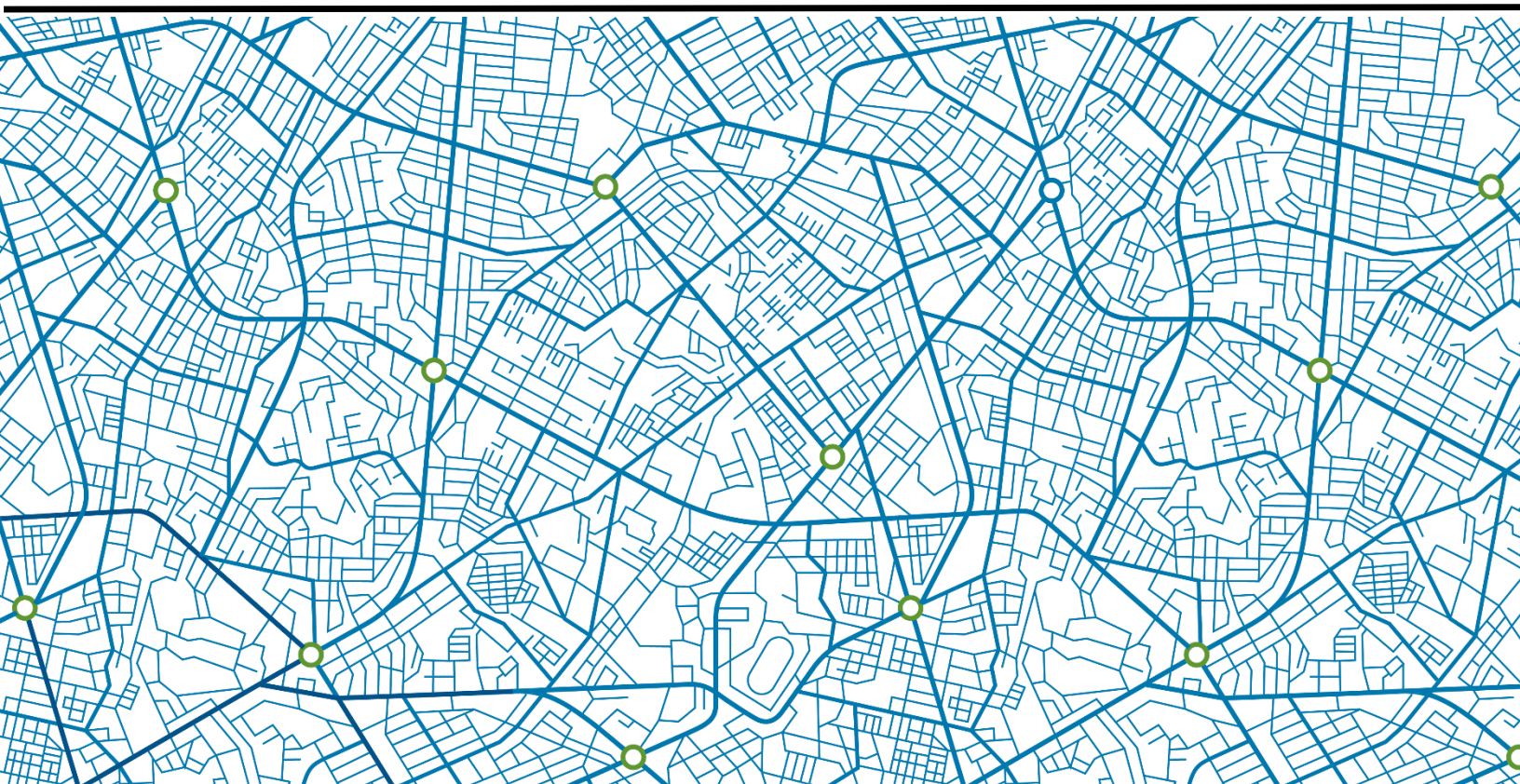
Guía de programa

Septiembre 2023

Agencia de Seguridad de Ciberseguridad e Infraestructura

BORRADOR / PREDECISIVO / DELIBERATIVO / INTERNO

Contenido



RESUMEN GENERAL

Las elecciones se llevan a cabo en un entorno muy visible, pero con recursos limitados, lo que plantea desafíos constantes para garantizar la seguridad. Aunque las oficinas electorales estatales y otras agencias estatales han ampliado el apoyo en seguridad electoral a las jurisdicciones locales desde 2016, los recursos y la experiencia siguen siendo limitados.

En algunos casos, las limitaciones de recursos han impulsado la competencia y aumentado los costos entre las jurisdicciones. Como resultado, varios estados han desarrollado programas para enlaces dedicados, conocidos como "**navegadores**", para reforzar o suplementar los esfuerzos de seguridad electoral tanto a nivel local como estatal.

Basados en las experiencias de los estados que han implementado programas de navegación y esfuerzos similares en los últimos años, esta guía examina las prácticas utilizadas en esta área y ofrece ideas para los estados que están considerando adoptar un programa o mejorar uno existente.

Específicamente, esta guía describe los roles, responsabilidades y capacidades de estos programas, explorando los siguientes temas:

- ¿Qué es un Navegador de Seguridad Electoral?
- Soporte y servicios de navegación
- Creación de un programa de navegación
- Prácticas recomendadas para el programa de navegación

El concepto de navegadores dedicados para los administradores electorales locales no es nuevo y se ha convertido en un modelo altamente apoyado en todo el subsector de infraestructura electoral. Los programas de navegación no son "modelos únicos", y cada estado desarrolla su propio enfoque.

Algunos estados pueden poner énfasis en la ciberseguridad, mientras que otros pueden concentrarse en un manejo más amplio de riesgos en la seguridad electoral.

Los programas de navegación permiten a los estados aplicar de manera amplia la experiencia de un personal pequeño, lo que resulta en un efecto multiplicador de fuerza en todas las jurisdicciones. Estos programas pueden proporcionar una amplia gama de apoyo y servicios a las oficinas electorales locales. Según el estado, el apoyo y los servicios de los programas existentes han incluido el intercambio y análisis de información sobre amenazas, capacitación y ejercicios, evaluaciones de riesgos, orientación e implementación de mitigación, planificación e informes de respuesta a incidentes y participación de las partes interesadas.

Establecer un programa de navegación es un proceso con múltiples pasos. Estos pasos pueden incluir la identificación de financiamiento y autoridades relevantes, la evaluación de necesidades y brechas, la definición del alcance y la escala del programa, el establecimiento de una línea base del programa, el aprovechamiento de los socios, la elección de un navegador y / o equipo de navegadores, y la adopción de un marco para monitorear y evaluar el desempeño del programa.

El intercambio continuo de información y mejores prácticas entre los estados con programas de navegación y esfuerzos similares puede ser útil durante el desarrollo e implementación del programa. Por ejemplo, los materiales existentes, como las herramientas de medición de referencia o los planes de implementación, pueden ser prestados, personalizados y reutilizados. Con esta guía y otras actividades, CISA continuará buscando oportunidades para facilitar el intercambio de información entre los navegadores y toda la comunidad electoral en general.

Los programas de navegación exitosos tienen el potencial de servir como multiplicadores de fuerza crítica, suplementando los recursos locales limitados para fomentar una mayor seguridad y resiliencia en la infraestructura electoral de la nación.

CONTEXTO

Las elecciones estadounidenses son descentralizadas y administradas a nivel estatal, local y territorial bajo marcos, sistemas e infraestructura legales y procesales específicos a cada jurisdicción. También hay una amplia variedad en términos de recursos, especialmente entre las jurisdicciones locales pequeñas y medianas que a menudo deben depender de presupuestos limitados y experiencia interna limitada en ciberseguridad y otras cuestiones de seguridad prioritarias emergentes. Para ayudar a mitigar los desafíos en términos de recursos, las oficinas electorales estatales a menudo apoyan a sus contrapartes locales en el intercambio de información, la capacitación y la administración de infraestructura compartida, como las bases de datos de registro de votantes en todo el estado.

Después de las elecciones de 2016, el apoyo se ha centrado cada vez más en la ciberseguridad y en un manejo más amplio de los riesgos de seguridad electoral. En varios estados, la ampliación en el apoyo en esta área ha incluido la asignación de enlaces estatales dedicados, conocidos en varios estados como "navegadores", que ayudan a movilizar los esfuerzos de seguridad electoral hasta las jurisdicciones más pequeñas.

¿QUÉ ES UN NAVEGADOR DE SEGURIDAD ELECTORAL?

Un navegador de seguridad electoral (en aquí en adelante, "navegador") es cualquier enlace que independientemente de su nombre, es asignado para reforzar o complementar los esfuerzos de seguridad electoral locales y estatales.

El título y la estructura organizativa de los programas de navegación varían según el estado. Mientras que algunos estados usan el título de "navegador", otros estados usan términos diferentes. Los navegadores en la mayoría de los estados son empleados por la oficina electoral estatal, mientras que otros trabajan para una agencia u oficina estatal diferente, por ejemplo, oficinas de tecnología de la información y seguridad de la información.

En la práctica, los navegadores pueden participar en una amplia variedad de actividades, como administrar el intercambio de información, ofrecer asistencia in situ, desarrollar capacitaciones, coordinar esfuerzos de respuesta y compartir recursos procesales. La misión, el rol y las responsabilidades específicas de un navegador varían según el estado. Finalmente, los programas de navegación pueden ser desarrollados para satisfacer las necesidades de cada jurisdicción electoral y adaptarse para reflejar las operaciones y dependencias electorales únicas dentro de cada estado.

Recuerde: *No existe un "modelo único" de programa de navegación, pero los navegadores de seguridad electoral pueden ser recursos vitales para los funcionarios estatales y locales y pueden abordar una variedad de necesidades.*

TIPOS DE PROGRAMAS DE NAVEGACIÓN

Los programas de navegación pueden diferir en términos de personal, alcance y misión del programa. Consulte *la Tabla 1* para ver algunos modelos de programa. Por ejemplo, algunos estados han empleado hasta 10 navegadores dedicados, mientras que otros utilizan solo uno. Inicialmente, los estados que primero adoptaron programas de navegación se centraron en apoyar los esfuerzos de ciberseguridad para mitigar el riesgo cibernético.

Cada vez más, dependiendo de las necesidades dentro de su jurisdicción, los navegadores están apoyando a las oficinas electorales locales para mitigar un espectro más amplio de amenazas a la seguridad electoral, incluyendo el riesgo físico, el riesgo operativo y la lucha contra las operaciones de influencia extranjera y de desinformación.

Los programas de navegación pueden cubrir una amplia gama de temas de seguridad electoral, pero la mayoría de los programas existentes se han unido en torno a cuatro áreas principales de riesgo:

- **Riesgo cibernético.** Los navegadores se centran en mitigar el riesgo cibernético a través de prácticas de ciberseguridad para proteger las redes, los dispositivos y los datos del uso no autorizado o delictivo y proteger la confidencialidad, integridad y disponibilidad de la información. En el contexto de las elecciones, los esfuerzos de ciberseguridad se centran en las redes, dispositivos y datos utilizados para administrar las elecciones, incluyendo los sitios web de las oficinas electorales, las bases de datos de registro de votantes, el equipo de votación y otros sistemas, así como los datos almacenados y administrados por dichos sistemas.

- **Riesgo físico.** Los navegadores ayudan a abordar el riesgo físico a través del apoyo a la seguridad física que incluye esfuerzos para proteger contra el acceso físico no autorizado de infraestructura sensible y contra actos de violencia u otras actividades nocivas dirigidas en contra de instalaciones, infraestructura o personal. En el contexto de las elecciones, esto puede incluir la protección de las oficinas electorales, las instalaciones de almacenamiento y escrutinio, los lugares de votación, los buzones de votación, los trabajadores electorales y los propios votantes.

- **Riesgo operacional.** Los riesgos operacionales son aquellos que tienen el potencial de impedir la ejecución exitosa de las operaciones. En las elecciones, esto incluye cualquier riesgo que pueda obstaculizar el manejo de las operaciones electorales, como interrupciones en la cadena de suministro de papeletas electorales o la disponibilidad de recursos críticos, como la energía eléctrica.

- **Operaciones de influencia extranjera y desinformación.** Contrarrestar las operaciones de influencia extranjera y la desinformación incluye actividades que crean resiliencia ante el uso de información falsa por parte de actores extranjeros para socavar la seguridad de la infraestructura electoral. Cuando se enfoca en la infraestructura electoral o los votantes, tales esfuerzos pueden sembrar discordia y socavar la confianza en los procesos y resultados electorales, a menudo al amplificar información incorrecta, inflamatoria o engañosa acerca de las elecciones, el proceso de votación o los aspectos de tecnología y seguridad electoral.

SOPORTE Y SERVICIOS DE NAVEGACIÓN

Los programas de navegación pueden proporcionar una amplia gama de apoyo y servicios a las oficinas electorales locales, personalizados para alinearse con el marco legal y la infraestructura únicos del estado. El apoyo y los servicios de los programas existentes han incluido variaciones de los siguientes elementos:

Área de soporte del Navegador	Importancia para los funcionarios electorales
Intercambio y análisis de información	Evaluar, analizar y compartir información sobre amenazas a la seguridad electoral (por ejemplo, alertas de ciberseguridad) para garantizar que los funcionarios reciban información clara, concisa, oportuna y procesable
Evaluación de riesgos	Facilitar evaluaciones de riesgos que identifiquen posibles brechas de seguridad y vulnerabilidades
Análisis de riesgos y priorización	Analizar evaluaciones de riesgos y datos de informes de servicio técnico; recomendar priorización para mitigaciones
Guía de mitigación	Recomendar recursos y servicios técnicos disponibles para los funcionarios electorales que reduzcan el riesgo y generen resiliencia
Implementación Técnica	Implementar medidas de mitigación, como establecer procedimientos operativos, iniciar reuniones con soporte de IT y redactar planes de mejoramiento
Planificación e informes de respuesta a incidentes	Actualizar o desarrollar planes personalizados de respuesta a incidentes para garantizar la coordinación y respuesta adecuadas entre las partes locales, estatales, federales y del sector privado; proporcionar orientación sobre los requisitos de presentación de informes
Desarrollo del Plan de Continuidad de Operaciones (COOP)	Actualizar o desarrollar planes personalizados para garantizar la continuidad de las operaciones durante posibles incidentes
Entrenamiento y ejercicios	Proporcionar a los funcionarios electorales capacitación en seguridad electoral o facilitar ejercicios y simulaciones para probar planes y procedimientos de respuesta a incidentes, y garantizar la preparación operativa general
Participación de las partes interesadas	Crear conciencia y generar confianza en los procesos electorales en las comunidades locales a través de la participación de las partes interesadas
Desarrollo de plantillas	Desarrollar y usar plantillas para estandarizar materiales, como procedimientos operativos estándar (SOP), listas de verificación de seguridad o planes de recuperación

CONSTRUYENDO UN PROGRAMA DE NAVEGACIÓN DE SEGURIDAD ELECTORAL

Cuando los funcionarios electorales estatales comienzan a construir un programa de navegador, es crucial considerar primero los posibles casos de uso, los beneficios y si el estado puede asignar los recursos adecuados para implementar y administrar el programa de manera efectiva. Tales deliberaciones por adelantado pueden aumentar el éxito y la viabilidad a largo plazo de un programa. A continuación, describimos algunas consideraciones para informar el proceso de planificación inicial.

Explorar la autoridad y la supervisión administrativa

A medida que las jurisdicciones trabajan en la planificación inicial, es importante identificar quién tiene la autoridad o el poder regulatorio para establecer el programa y quién asumirá la administración, el riesgo y los costos para proporcionar servicios. En algunos casos, como en Illinois,[1] la legislación era necesaria para establecer el programa. En otros casos, como Minnesota, la legislación no era necesaria.[2]

Identificar brechas entre el apoyo de seguridad electoral estatal existente y las necesidades locales

Identificar las brechas entre el apoyo y los servicios de seguridad electoral estatales y las necesidades de las jurisdicciones locales es un paso crucial antes de elaborar un plan de implementación y puede aumentar la probabilidad de éxito del programa. Por ejemplo, en un estado donde muchas oficinas electorales locales carecen o poseen planes de respuesta a incidentes obsoletos, el estado puede buscar crear un programa de navegación con líneas de esfuerzo que aborden la coordinación de respuesta a incidentes, el desarrollo de planes de respuesta a incidentes y ejercicios que incluyan escenarios de respuesta a incidentes.

Después de realizar una evaluación de necesidades y personalizar el programa para beneficiar tanto a las jurisdicciones estatales como locales, puede ser útil comenzar a investigar los modelos existentes de los estados que ya han implementado programas de navegadores. *La Tabla 1* presenta ejemplos de cómo algunos estados y localidades organizan sus programas.

Establecer una línea base y un alcance del programa

Una vez completada la evaluación de las necesidades, las **organizaciones deben tratar de establecer medidas o indicadores de referencia a partir de los cuales medir el progreso.** Recursos como la Herramienta de Perfil de Riesgo de Seguridad Electoral de CISA o la Lista de Verificación de Objetivos de Desempeño de Ciberseguridad Intersectorial pueden ser útiles para desarrollar puntos de referencia, que las jurisdicciones pueden personalizar en función de sus necesidades únicas, infraestructura y postura de seguridad existente. Los programas de navegación de seguridad electoral permiten a los funcionarios electorales locales adaptar el programa inherentemente para que se ajuste a sus perfiles de riesgo únicos y necesidades de seguridad localizadas. **El papel del navegador es ayudar a identificar esos riesgos, evaluar las áreas de mejora y, cuando corresponda, ayudar a crear un plan de acción para abordarlos.** En los programas de exploración de navegadores, algunos estados se han enfocado principalmente en la ciberseguridad, mientras que otros brindan apoyo en múltiples áreas de riesgo. El apoyo puede variar desde compartir información y recursos hasta ir físicamente al sitio para implementar soluciones técnicas y otras mitigaciones. Finalmente, las organizaciones deben tratar de determinar si el programa tendrá

[1] PARTE 213 PROGRAMA CYBER NAVIGATOR: Listado de secciones. (s.f.). https://www.ilga.gov/commission/jcar/admincode/026/02600213sections.html

[2] Si bien Minnesota no requirió legislación para crear su Programa de Navegadores, el estado sí requirió aprobación legislativa para gastar fondos de HAVA en el programa. Para obtener más información, consulte: Oficina del Secretario de Estado del Estado de Minnesota. (6 de marzo de 2019). https://www.sos.state.mn.us/about-the-office/

roles o servicios de cara al público. Los compromisos públicos que crean conciencia sobre las medidas de seguridad electoral existentes pueden ayudar a infundir una mayor confianza pública en las operaciones electorales. Los eventos públicos también podrían ser una oportunidad para solicitar comentarios sobre la evolución de las preocupaciones u oportunidades para una mayor participación o desarrollo de productos / servicios para los funcionarios electorales.

Identificar soporte financiero

La financiación es una consideración clave para implementar un programa de navegador sostenible. Si bien algunos estados pueden dirigir o redirigir los fondos existentes para lanzar un programa de navegador, otros pueden necesitar buscar nuevos fondos o autorización de la legislatura estatal u otras autoridades gubernamentales estatales y locales relevantes. La identificación de fondos también puede ser complicada por los ciclos presupuestarios y de financiamiento que pueden no alinearse con los ciclos electorales. Cuando los fondos disponibles son limitados, algunos estados lanzaron primero un programa piloto de navegador, para poner en marcha el programa rápidamente y demostrar su propuesta de valor para futuras solicitudes de autorización de presupuesto o programa.

Las subvenciones federales pueden proporcionar una fuente de financiamiento adicional para los programas de navegador. Los fondos de la Ley Help America Vote **(HAVA),** distribuidos por la Comisión de Asistencia Electoral de los Estados Unidos a las oficinas electorales estatales, han sido utilizados por los estados para implementar programas de navegación y otras iniciativas de seguridad electoral. Las subvenciones del Departamento de Seguridad Nacional (DHS), incluido el Programa de Subvenciones de Seguridad Nacional **(HSGP), administrado por la Agencia Federal para el Manejo de Emergencias (FEMA), y el Programa de Subvenciones de Seguridad Cibernética Estatal y Local** (SLCGP), **administrado por** CISA y FEMA, también se pueden usar para avanzar en los esfuerzos de seguridad electoral. DHS designó la seguridad electoral como un Área de Prioridad Nacional para la última ronda de financiamiento de HSGP e incluyó programas de navegadores como ejemplo en el aviso de oportunidad de financiamiento.[3]

Ley Help America Vote (HAVA)	Programa de Subvenciones para la Seguridad Nacional (HSGP)	Programa de subvenciones de ciberseguridad estatal y local (SLCGP)
•Proporciona fondos a estados y territorios de EE. UU. para mejorar la administración de las elecciones para cargos federales, incluyendo el mejoramiento de la tecnología y la implementación de ciertas mejoras de seguridad. •HAVA ofrece subvenciones de fórmula, subvenciones discrecionales y subvenciones de seguridad electoral. En particular, las **subvenciones discrecionales** pueden ser una fuente útil de financiación inicial para poner en marcha o ampliar un programa de navegación.	•Proporciona financiación para apoyar el desarrollo y la continuidad del **Objetivo de Preparación Nacional** de una nación segura y resiliente. •El HSGP del año fiscal 2023 identificó las elecciones como **área de prioridad nacional** y requirió que los destinatarios asignaran el 3% del premio a la seguridad electoral.	•Proporciona subvenciones para abordar los riesgos y amenazas de ciberseguridad a los sistemas de información utilizados o propiedad de (o en nombre de) gobiernos estatales, locales y territoriales. •El propósito es ayudar a los gobiernos estatales, locales y territoriales a **manejar y reducir el riesgo cibernético sistémico.**

Figura 1: Oportunidades de subvenciones federales

Las oportunidades de financiamiento pueden provenir de una variedad de fuentes federales, estatales e incluso privadas, dependiendo de la disponibilidad, la necesidad y la ley estatal. Asegúrese de investigar todas las opciones potenciales para ver qué se adapta mejor a las necesidades específicas del programa de navegación.

[3] El Programa de Subvenciones de Seguridad Nacional del Año Fiscal 2023 del Aviso de Oportunidad de Financiamiento (NOFO) del Departamento de Seguridad Nacional (DHS). (s.f.). FEMA.gov. https://www.fema.gov/grants/preparedness/homeland-security/fy-23-nofo

Elegir un navegador

Al igual que los propios funcionarios electorales, los navegadores exitosos necesitarán una variedad de habilidades técnicas, interpersonales y organizacionales para lograr los objetivos del programa. Los navegadores también deben ser capaces de establecer confianza dentro de su comunidad e iniciar nuevas asociaciones o colaboraciones según corresponda para el programa.

A medida que cambia el panorama de riesgos, es fundamental encontrar un navegador que pueda entender y apoyar eficazmente una cartera dinámica de seguridad electoral. Los navegadores siempre pueden ser entrenados para que posean un nivel suficiente de competencia técnica en todos los sectores de riesgo; sin embargo, ciertas "competencias sociales", como la comunicación efectiva, la resolución de problemas y la adaptabilidad, también son importantes. Los estados pueden tratar de reclutar exfuncionarios electorales o asociados en infraestructura electoral como navegadores, para aprovechar su conocimiento institucional, relaciones y experiencia. Si bien las personas sin experiencia electoral previa aún pueden ser navegadores efectivos, pueden requerir una mayor inversión inicial de capacitación para trabajar en el sector de infraestructura electoral. Estas personas pueden aportar otros conjuntos de habilidades deseadas al programa en áreas técnicas específicas que ayudan alcanzar los objetivos del programa.

Factores clave

Al elegir un Navegador de Seguridad Electoral, considere estos factores clave:

- ☐ ¿Cuáles son los principales objetivos y prioridades de su programa?
- ☐ ¿Cuáles son los principales factores de riesgo de sus jurisdicciones? ¿Existe un área específica de especialización que sería mas apropiada para manejarlos?
- ☐ ¿Qué conjuntos de habilidades son más importantes para lograr los objetivos de su programa?
- ☐ ¿Hay alguna persona con relaciones existentes o familiaridad con sus sistemas electorales que fácilmente podría asumir este rol?

Medir el rendimiento y la eficacia

Finalmente, cada estado debe determinar medidas de efectividad para evaluar el programa e identificar áreas de mejora. Cuando se trabaja con un nuevo programa, las evaluaciones tempranas pueden provenir de informes anecdóticos y estadísticas del programa de conteo (p. ej., el número de casos o incidentes manejados, el número de capacitaciones proporcionadas sobre cada tema relevante, cuántos trabajadores electorales recibieron esas capacitaciones, etc.). **Con el tiempo, a medida que el programa madura, las localidades pueden comenzar a establecer objetivos cada vez más ambiciosos para el programa y sus participantes, centrándose no solo en los productos del programa, sino también en los resultados.** Esta también puede ser una forma efectiva de identificar qué componentes del programa son más impactantes o de más alta demanda. Por ejemplo, si una capacitación o recurso en particular demuestra ser particularmente efectivo, puede ampliarse y ampliarse para futuras necesidades del programa. Idealmente, las jurisdicciones pueden confiar en estas evaluaciones para ayudar a identificar áreas de mejora y dirigir cambios incrementales.

PRÁCTICAS RECOMENDADAS PARA EL PROGRAMA DE NAVEGACIÓN

El intercambio de información es uno de los elementos más importantes de un programa de navegación. Los nuevos programas pueden beneficiarse de la identificación de competencias básicas para los navegadores y las mejores prácticas o recursos existentes utilizados en otros estados y jurisdicciones.

Los funcionarios electorales locales probablemente solicitarán asistencia en una amplia variedad de desafíos **y todos los navegadores pueden beneficiarse al compartir información con otros navegadores y funcionarios electorales en todos los estados.** El poder y el valor de compartir información y mejores prácticas es la razón por la cual CISA elaboró esta guía, para aumentar el conocimiento y la comprensión de los programas de navegadores en todo el país. A medida que los navegadores buscan aprovechar los recursos estatales y locales disponibles, también deben recordar que los socios federales, incluidos el FBI, CISA y EI-ISAC, también pueden ayudar a facilitar las conexiones y compartir información a nivel nacional.

CONSIDERACIONES PARA IMPLEMENTAR DIFERENTES MODELOS DEL PROGRAMA DE NAVEGACIÓN

Si bien todos los programas de navegación difieren según las necesidades y los recursos, los programas existentes se pueden agrupar en dos modelos generales.

Modelos de programa

Modelo de programa especialmente diseñado: algunos estados han creado programas de navegación desde cero, abordando las necesidades de seguridad electoral o las brechas que antes no se cumplían. En comparación con los programas modificados (explicados a continuación), los programas especialmente diseñados pueden tener más flexibilidad y autonomía para determinar los roles y responsabilidades del navegador, pero también pueden requerir más fondos iniciales.

- **Recursos altos**: dos o más navegadores dedicados
- **Recursos bajos**: un navegador dedicado
- **Recursos para voluntarios o pasantes**: programas que dependen del apoyo de voluntarios o pasantes, generalmente en asociación con una o más universidades

Modelo de programa modificado: algunos estados han redirigido recursos de otras áreas existentes para crear programas de navegador. Es posible que estos estados ya tengan una o más personas que sirven en una capacidad similar a la de un navegador. En comparación con los programas especialmente diseñados, los programas modificados pueden ser más fáciles de iniciar inicialmente, pero también pueden requerir que los navegadores hagan "doble sombrero" con sus otros roles.

- **Asesoramiento Intensivo**: programas que se basan principalmente en asociaciones con otras entidades para proporcionar navegadores
- **Cambio de enfoque**: cambiar uno o más roles existentes dentro de la organización para incluir actividades de navegador

Consideraciones acerca del programa

- **Alcance del programa y actividades**
  - **Alcance:** los dominios de riesgo que el programa puede admitir, incluidos los dominios de riesgo de ciberseguridad, seguridad física, operacional y / o desinformación.
  - **Área de servicio**: según el modelo y el alcance, el programa podrá proporcionar servicios a algunos o a todos los funcionarios electorales dentro del estado.
  - **Participación local**: los funcionarios electorales pueden participar en el programa de manera requerida o voluntaria.
  - **Actividades de servicio**: actividades potenciales que un programa de navegador puede llevar a cabo

- Creación y gobernanza de programas
    - **Autoridad de Creación de Programas:** algunos programas especialmente diseñados pueden requerir la aprobación regulatoria para ser establecidos, mientras que los programas modificados pueden ser establecidos directamente por el liderazgo organizacional.
    - **Opciones de financiamiento**: posibles vías para financiar programas de navegadores (no exhaustivo)
    - **Gobernanza**: la mayoría de los programas de navegación se alinean con el principal funcionario electoral del estado
    - **Socios de gobernanza**: socios potenciales para la gobernanza del programa

- Personal del programa y asociados
    - **Contratación de personal**: los candidatos para los programas de navegador pueden provenir de profesionales de IT existentes; voluntarios, estudiantes o pasantes con experiencia en IT y / o ciberseguridad; o enlaces o coordinadores de seguridad electoral existentes dentro del estado
    - **Dependencia / escala del personal primario**: el número anticipado de personal, voluntarios, pasantes o socios necesarios para implementar el programa
    - **Enfoque del personal**: los candidatos para los programas de navegación pueden enfocarse en experiencia técnica, experiencia previa en elecciones o redes profesionales, o una combinación de estos.
    - **Socios proveedores de servicios**: socios potenciales para la implementación del programa

Tabla 1: Tipos de programas de navegación

Detalles del programa	Programas especialmente diseñados Nuevos programas creados con el propósito específico de abordar las brechas de seguridad electoral			Programas modificados Los programas existentes redirigen los recursos para abordar las brechas de seguridad electoral	
	Recursos altos (2+ personal)	**Recursos bajos** (1 personal)	**Recursos para voluntarios o pasantes**	**Asesoramiento Intensivo**	**Cambio de enfoque**
Alcance del programa	Soporte básico a intensivo en múltiples dominios de riesgo	Soporte básico en un número limitado de dominios de riesgo	Soporte intensivo para un único dominio de riesgo (cibernético)	Soporte intermedio en múltiples dominios	Soporte básico en múltiples dominios
Área de Servicio	Todos los funcionarios electorales locales	Todos los funcionarios electorales locales	Algunos funcionarios electorales locales	Todos los funcionarios electorales locales	Todos los funcionarios electorales locales
Participación local	Estatutario o Voluntario, pero impulsado por fondos de subvención	Voluntario	Estándares de seguridad requeridos con apoyo voluntario	Voluntario	Voluntario
Actividades de servicio	Intercambio de información Conexión con proveedores de servicios Colaboraciones Evaluaciones de las necesidades Entrenamientos y ejercicios Responder a preguntas Análisis y priorización de riesgos Subvención Guía de mitigación Implementación técnica Planificación de la respuesta a incidentes COOP Participación de las partes interesadas Desarrollo de plantillas	Intercambio de información Conexión con proveedores de servicios Colaboraciones Evaluaciones de las necesidades Entrenamientos y ejercicios Responder a preguntas Guía de mitigación Planificación de la respuesta a incidentes COOP Desarrollo de plantillas	Intercambio de información Conexión con proveedores de servicios Colaboraciones Evaluaciones de las necesidades Responder a preguntas Guía de mitigación Desarrollo de plantillas	Intercambio de información Conexión con proveedores de servicios Colaboraciones Entrenamiento y ejercicios Responder a preguntas Guía de mitigación	Intercambio de información Conexión con proveedores de servicios Colaboraciones Entrenamiento y ejercicios Responder a preguntas Guía de mitigación
Autoridad de creación de programas	Estatutario / Regulatorio	Regulatorio / Gestión	Administración	Administración	Administración
Opciones de financiación	Estímulo HAVA / Presupuesto operativo	Estímulo HAVA / Presupuesto operativo	Presupuesto operativo / Financiamiento de subvenciones	Presupuesto operativo	Presupuesto operativo
Gobernanza	Jefe Estatal Oficial Electoral	Jefe Estatal Oficial Electoral	Jefe Estatal Oficial Electoral	Jefe Estatal Oficial Electoral	Jefe Estatal Oficial Electoral
Socios de gobernanza	Oficial Estatal de Seguridad de la Información de IT (ISO)	ISO de IT estatal	Líder del Programa Universitario	ISO de IT estatal	ISO de IT estatal
Dotación de personal	Profesionales de IT	Profesionales de IT	Voluntarios Pasantes / Estudiantes	Enlaces existentes con soporte de IT	Enlaces existentes

Detalles del programa	Programas especialmente diseñados Nuevos programas creados con el propósito específico de abordar las brechas de seguridad electoral			Programas modificados Los programas existentes redirigen los recursos para abordar las brechas de seguridad electoral	
	Recursos altos (2+ personal)	**Recursos bajos** (1 personal)	**Recursos para voluntarios o pasantes**	**Asesoramiento Intensivo**	**Cambio de enfoque**
Dependencia / Escala de personal primario	Personal diverso	Individuo	Voluntario	Asociados	Personal diverso
Enfoque en la dotación de personal	Experiencia técnica / Red profesional	Experiencia técnica / Red profesional	Experiencia técnica	Experiencia en Elecciones / Red Profesional	Experiencia en Elecciones / Red Profesional
Socios proveedores de servicios	IT estatal Gobierno Federal (CISA) Guardia Nacional Sector privado	IT estatal Gobierno Federal (CISA) Guardia Nacional Sector privado	Universidades TI estatal Gobierno Federal (CISA) Guardia Nacional Sector privado	IT estatal Gobierno Federal (CISA) Guardia Nacional Sector privado	IT estatal Gobierno Federal (CISA) Guardia Nacional Sector privado

CONCLUSIÓN

Ahora más que nunca, los estados deben recurrir a todos los elementos en su conjunto de herramientas de seguridad para garantizar la resiliencia de la infraestructura electoral de la nación. Los programas de navegación pueden servir como un poderoso multiplicador de fuerza para mejorar la seguridad electoral a nivel local. Muchos estados han tenido éxito en la implementación de programas de navegación que se adaptan a sus necesidades de seguridad electoral y a los matices de sus prácticas de administración electoral. El equipo de Seguridad y Resiliencia Electoral de CISA está disponible para apoyar a los estados interesados en establecer o expandir su programa de navegadores y facilitar el intercambio de las mejores prácticas en todo el país.

Para obtener más información sobre los programas de navegadores u otros recursos de seguridad electoral de CISA, comuníquese con ElectionSecurity@cisa.dhs.gov