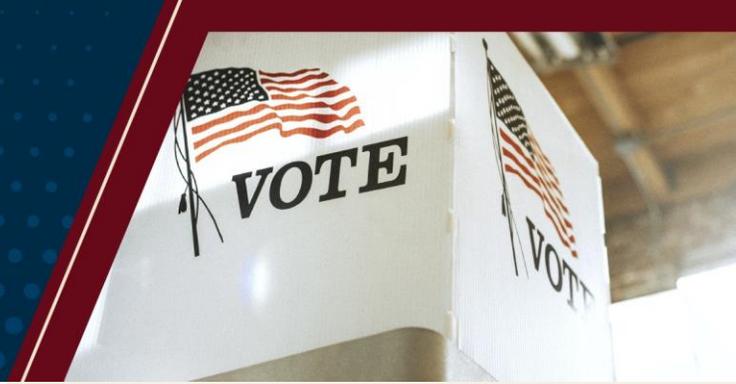




LISTA DE VERIFICACIÓN DE SEGURIDAD FÍSICA PARA OFICINAS ELECTORALES



INTRODUCCIÓN

Garantizar un proceso electoral seguro y resiliente es un interés nacional fundamental y una de las máximas prioridades de la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA, por sus siglas en inglés). La CISA se compromete a trabajar en colaboración con funcionarios electorales y proveedores de tecnología y servicios electorales para gestionar los riesgos de la infraestructura electoral del país. Como parte del amplio conjunto de recursos a disposición de los funcionarios electorales, esta lista de verificación es una herramienta para revisar rápidamente las prácticas establecidas y tomar medidas para mejorar la seguridad física y la resiliencia operativa como preparación para el día de las elecciones.

CÓMO UTILIZAR ESTE RECURSO

Esta lista de verificación proporciona una serie de preguntas diseñadas para ayudar a los funcionarios electorales a identificar áreas a fin de mejorar la seguridad física en las instalaciones de infraestructura electoral y tomar medidas para implementar opciones de bajo costo o sin costo en el corto plazo.

LISTA DE COTEJO DE SEGURIDAD

Planificar y prepararse

SÍ/NO

¿Ha establecido un Plan de Seguridad de las Instalaciones (Facility Security Plan) para su oficina que aborde las tareas clave para mantener la seguridad de la oficina?

- Implemente políticas para asegurar puertas y ventanas exteriores, asegurar áreas sensibles dentro de las instalaciones, utilizar un sistema de alarma en las instalaciones (si está instalado) y observar áreas de estacionamiento para detectar vehículos desatendidos o actividad sospechosa.
- Establezca procedimientos para monitorear el área de estacionamiento y políticas para actuar ante vehículos no autorizados.
- Implemente una campaña de concientización pública "If You See Something, Say Something®" (Si ve algo, diga algo). Esto puede ser tan simple como colocar carteles con información de contacto para que el público pueda denunciar incidentes.
- Establezca políticas y procedimientos de control de acceso para el personal, los voluntarios y el público a fin de permitir únicamente el acceso autorizado a lugares sensibles. Establezca un sólido sistema de rendición de cuentas sobre el control de claves y restrinja la duplicación de claves.
- Practique sus planes de respuesta a incidentes y de continuidad de operaciones para familiarizar al personal con sus responsabilidades. Esto también puede ayudar a identificar lagunas en los planes para que puedan abordarse antes de que ocurra un incidente.

SÍ/NO

¿Ha desarrollado otros planes para apoyar operaciones electorales seguras y resilientes?

- Establezca un **Plan de Respuesta a Incidentes (Incident Response Plan)** que identifique las responsabilidades de seguridad, los contactos de emergencia y los procedimientos de respuesta. Su Plan de Respuesta a Incidentes también debe incluir un **manual de comunicaciones de respuesta a incidentes** que ayude a saber cómo comunicarse de manera clara y transparente con los votantes y el público si ocurre un incidente, y qué medidas se han tomado para garantizar un proceso electoral seguro y protegido.
- Establezca un **Plan de Continuidad de Operaciones (Continuity of Operations Plan)** para garantizar que las funciones electorales esenciales puedan continuar si ocurren interrupciones en las operaciones. Esto podría incluir la planificación de soluciones de energía de respaldo para los lugares de votación u oficinas electorales, o la identificación de sitios alternativos para continuar las operaciones si una instalación es inaccesible o inutilizable.

SÍ/NO

¿Ha establecido procedimientos para el manejo de correo/paquetes sospechosos, como posibles amenazas de bomba?

- Prepare un área para el manejo seguro del correo con acceso directo al exterior del edificio o en un lugar con puertas que se puedan cerrar.
- Tenga equipo de protección personal disponible para el personal que maneja el correo y fácil acceso al agua.
- Para obtener información adicional, consulte los [Procedimientos de manejo de correo electoral para protegerse contra materiales peligrosos](#) elaborados conjuntamente por la CISA, la Oficina Federal de Investigaciones (Federal Bureau of Investigation), la Comisión de Asistencia Electoral de los EE. UU. (U.S. Election Assistance Commission) y el Servicio de Inspección Postal de los EE. UU. (U.S. Postal Inspection Service), así como la [Guía de amenazas de bombas](#) y la [Lista de verificación de amenazas de bombas](#) de la CISA.

SÍ/NO

¿Se ha coordinado con los servicios de emergencia en su jurisdicción?

- Hable sobre sus planes de seguridad de las instalaciones y respuesta a incidentes con el personal de emergencia con anticipación para que puedan comprender la postura de su organización antes de llegar a la escena durante un incidente.
- Proporcione una lista a los servicios de emergencia o un mapa de ubicaciones de infraestructura electoral, lo que incluye lugares de votación temporales. Revise los planos de las instalaciones y las rutas de evacuación.
- Trabaje con los servicios de emergencia para ver si tienen radios de emergencia para usar durante las operaciones electorales y momentos de mayor amenaza.

SÍ/NO

¿Ha trabajado con el personal de emergencia para mitigar los riesgos potenciales de incidentes fraudulentos como ataques con swatting (denuncias falsas) o amenazas de bombas falsas dirigidas a las instalaciones electorales durante el período de votación?

- Asegúrese de que su sistema de despacho informático de seguridad pública local 9-1-1 tenga identificadas las ubicaciones de las elecciones, incluidas las ubicaciones temporales, para que el sistema alerte a los servicios de emergencia que la ubicación del incidente puede ser un objetivo de llamadas falsas para interrumpir las operaciones electorales.

SÍ/NO

¿Dispone de mecanismos para facilitar la recepción y el intercambio de información sobre amenazas?

- Únase a plataformas de intercambio de información sobre amenazas como el Centro de Análisis e Intercambio de Información sobre Infraestructura Electoral (Election Infrastructure-Information Sharing and Analysis Center).
- Interactúe y comparta información con los Centros de Fusión (Fusion Centers) que tengan cobertura en su jurisdicción.
- Trabaje con sus vecinos (propietarios y operadores de oficinas o edificios vecinos) para compartir conocimientos sobre amenazas y preocupaciones de seguridad, y animarlos a notificar incidentes de seguridad a las autoridades correspondientes. Si es posible, considere compartir imágenes y transmisiones de cámaras de seguridad entre sí.

Implementar

SÍ/NO

¿Realiza controles aleatorios tanto durante como después del horario comercial para asegurarse de que los procedimientos de seguridad se implementan según lo previsto?

SÍ/NO

¿Los puntos de entrada y las ubicaciones o activos sensibles están monitoreados por cámaras de seguridad o sistemas de detección de intrusos?

- Considere implementar sistemas de alerta y monitoreo de seguridad por video que cubran, como mínimo, los puntos de entrada y lugares de almacenamiento de activos sensibles como papeletas y equipos electorales.
- Si las soluciones de seguridad comercial de nivel profesional exceden los recursos disponibles, considere opciones de menor costo disponibles comercialmente, como soluciones de seguridad para el hogar que incluyen cámaras de video con capacidad de detección de movimiento, funciones de alerta por correo electrónico o mensaje de texto y sensores de detección de intrusiones para puertas y ventanas.

SÍ/NO

¿Se utilizan “botones de pánico” fijos o portátiles?

- Muchos sistemas de seguridad de nivel profesional incluyen opciones de alarmas de coacción fijas y portátiles o “botones de pánico” que se integran en el sistema de seguridad más amplio de una instalación.

- Si las soluciones de seguridad comercial de nivel profesional exceden los recursos disponibles, existen “botones de pánico” portátiles de bajo costo disponibles en el mercado que pueden programarse para contactar a la policía local y que vienen en formatos similares a llaveros.

SÍ/NO

¿Existen procedimientos para controlar la entrada de visitantes?

- Asegúrese de que el Plan de Seguridad de las Instalaciones establezca procedimientos para la plena responsabilidad de los visitantes (p. ej., con la implementación de procedimientos de registro de entrada y salida).
- Evite que los visitantes entren por puntos de entrada no autorizados (p. ej., asegúrese de que todas las demás puertas estén cerradas, excepto la entrada pública).
- Implemente mecanismos para informar a los demás empleados de la presencia de visitantes dentro de las instalaciones. Para las oficinas donde el monitoreo continuo de los lugares de entrada de visitantes es un desafío, considere colgar un timbre en la puerta o instalar algún tipo de sensor de movimiento o timbre comercial que alerte cuando se abre una puerta.

SÍ/NO

¿Las ventanas de la planta baja y las grandes puertas de entrada de vidrio tienen medidas de privacidad instaladas?

- Instale una película de contacto o de privacidad en las puertas y ventanas de vidrio de la planta baja si no tienen otras características para oscurecer la visibilidad exterior. Se pueden comprar películas de contacto o de privacidad en la ferretería local y algunos tipos pueden brindar cierta resistencia a la rotura.
- Si no es posible modificar las ventanas del edificio, utilice tratamientos de ventanas o cortinas que se puedan ajustar fácilmente para ocultar la observación visual hacia la oficina.
- Si está permitido, considere prohibir el estacionamiento junto al edificio de la oficina electoral durante las operaciones de las elecciones y épocas de mayor amenaza.

SÍ/NO

¿Existen barreras físicas delante de las entradas para mitigar las vías de aproximación de alta velocidad o los caminos rectos sin obstáculos para los vehículos?

- Instale bolardos de seguridad (normalmente hechos de metal o cemento) frente a las instalaciones para ayudar a proteger a los peatones y prevenir daños vehiculares accidentales o deliberados.
- Si las soluciones permanentes, como los bolardos, exceden los recursos, comuníquese con su departamento de transporte para consultar sobre posibles barreras temporales que puedan estar disponibles. Otra alternativa podría ser llenar jardineras exteriores extra grandes para usarlas como barrera.

SÍ/NO

¿Hay extintores de incendios previamente colocados en lugares sensibles?

- Instale un extintor de incendios en cada habitación donde se guarden papeletas, equipos electorales y suministros electorales.
- Asegúrese de que haya un extintor de incendios en cada lugar de votación.

SÍ/NO

¿Las urnas electorales están ubicadas en áreas bien iluminadas y monitoreadas continuamente?

- Coloque las urnas en lugares que proporcionen buena iluminación, permitan una videovigilancia continua y sean observables por el personal de la instalación.

Informar

Sepa cómo notificar incidentes de seguridad física o cibernética a las autoridades estatales y locales pertinentes, la CISA y otros socios federales.

- Aproveche la iniciativa Última Milla (Last Mile) de la CISA para documentar la guía de informes.
- Imprima [Ciclo de elecciones generales de 2024: Guía de notificación voluntaria de incidentes para las partes interesadas en la infraestructura electoral](#) de la CISA.

RECURSOS

#Proteger2024 | CISA

cisa.gov/topics/election-security/protect2024

Recursos fundamentales para los funcionarios electorales estatales y locales que ocupan puestos esenciales.

Ciclo de elecciones generales de 2024: Guía de notificación voluntaria de incidentes para las partes interesadas en la infraestructura electoral | CISA

cisa.gov/resources-tools/resources/2024-general-election-cycle-voluntary-incident-reporting-guidance-election-infrastructure

Se anima a las partes interesadas en la infraestructura electoral a compartir información relacionada con incidentes de seguridad física y cibernética entre sí, con los centros de fusión estatales, con las fuerzas del orden locales y con los socios federales.

Seguridad física de los lugares de votación y las instalaciones electorales | CISA

cisa.gov/resources-tools/resources/physical-security-voting-locations-and-election-facilities

Esta guía general proporciona recursos y pasos prácticos para conectar, planificar, capacitar y notificar que los funcionarios electorales deben considerar para mejorar su postura de seguridad física y la resiliencia de las operaciones electorales en su jurisdicción.

Qué hacer: amenaza de bomba | CISA

cisa.gov/resources-tools/resources/what-do-bomb-threats

Este documento de orientación proporciona una descripción general de las amenazas de bombas y algunas prácticas recomendadas para mitigar los impactos asociados con estas amenazas.

Correo sospechoso | USPIS

uspis.gov/tips-prevention/suspicious-mail

Siga y comparta estos consejos para protegerse y proteger a otros contra el correo sospechoso.

Procedimientos de manipulación de correo electoral para protegerse contra materiales peligrosos | CISA

cisa.gov/resources-tools/resources/election-mail-handling-procedures-protect-against-hazardous-materials

Esta guía proporciona una descripción general para los funcionarios electorales sobre cómo prepararse para manipular el correo de manera segura, identificar correo potencialmente sospechoso y responder a la posible exposición a materiales peligrosos durante la manipulación del correo.

Productos de Última Milla | CISA

cisa.gov/resources-tools/services/last-mile-products

La iniciativa “Última Milla” (Last Mile) de la CISA ofrece a los administradores electorales y a sus socios una serie de recursos personalizables basados en las prácticas recomendadas de seguridad y en los estándares de la industria para ayudar a proteger la infraestructura electoral en todo el país.