GUÍA DE SEGURIDAD OPERACIONAL PARA LOS FUNCIONARIOS ELECTORALES

Perspectiva general

La seguridad operativa (OPSEC) es un proceso sistemático para identificar y proteger información, datos o confidencialidad en de una organización.[1] OPSEC no está fuera del alcance de ninguna oficina. Es algo que las personas hacen a diario en su vida personal y profesional cuando toman medidas para proteger información que saben podría crear riesgos si es expuesta, como cuidar su número de seguro social y fecha de nacimiento para protegerse contra el robo de identidad. OPSEC es una parte fundamental para proteger la infraestructura electoral. Sin los cuidados adecuados, la información confidencial puede quedar expuesta, ya sea consciente o inconscientemente, y ser compilada por posibles actores maliciosos, como adversarios extranjeros y delincuentes. Esto puede afectar la capacidad de los trabajadores electorales para llevar a cabo sus deberes oficiales, exponer la información de identificación personal (PII) de los votantes o permitir el acceso no autorizado a sistemas o instalaciones internas. Al incorporar los principios de OPSEC en las operaciones electorales diarias y fomentar una cultura de seguridad en toda su organización, los trabajadores electorales pueden reducir la probabilidad de divulgar información confidencial a partes no autorizadas. Un buen OPSEC al mismo tiempo que se mantiene un proceso electoral transparente y se responde a las consultas públicas es posible.

Ejemplo: Información confidencial compartida de los votantes

Una jurisdicción electoral local compartió accidentalmente una hoja de cálculo en respuesta a una solicitud de registros públicos que incluía los últimos cuatro dígitos de los números de seguro social de los votantes. Cuando se descubrió el error, la jurisdicción le pidió al solicitante que eliminara la información confidencial y pudo confirmar que lo hicieron. Más tarde, la jurisdicción envió cartas a aproximadamente 500,000 votantes registrados afectados para notificarles sobre el incidente y tomar medidas correctivas.

Ejemplo: Las tiendas web de los fabricantes de sistemas de votación y los manuales de capacitación de las jurisdicciones mostraban imágenes de las llaves de los equipos físicos

Utilizando información disponible públicamente, los posibles adversarios podrían haber reproducido o adquirido las llaves físicas de las cerraduras utilizadas para proteger el equipo de votación.

A veces, las imágenes en línea presentan información de llaves físicas, como cortes de llaves o códigos de llaves, que podían ser usados para identificar los tipos de llaves necesarias para acceder a los equipos internos.

La transparencia y el intercambio de información son componentes vitales de la administración electoral, y las recomendaciones incluidas en esta guía son consistentes con estos objetivos.

OPSEC ayuda a las organizaciones a considerar los datos y la información desde el punto de vista de un adversario, lo que permite una evaluación holística de los datos confidenciales y los posibles casos de uso malicioso o no autorizado. Incluso si las piezas individuales de información no parecen particularmente sensibles en su naturaleza, múltiples piezas de información sobre una organización, sus operaciones o su gente pueden potencialmente combinarse para crear un riesgo mucho mayor. Con la capacitación y el conocimiento de los principios de OPSEC, los trabajadores electorales pueden comprender mejor estos riesgos agregados y limitar la exposición potencial de información confidencial.

Este recurso proporciona una visión general de OPSEC en un contexto electoral, destacando los riesgos potenciales y ejemplos del mundo real, y ofrece a los propietarios y operadores de infraestructura electoral actividades de mitigación a considerar.

[1] Instituto Nacional de Estándares y Tecnología, Centro de Recursos de Seguridad Informática (CSRC) Glosario: Seguridad Operacional (OPSEC). https://csrc.nist.gov/glossary/term/operations_security#:~:text=Definitions%3A%20Systematic%20and%20proven%20process%20by%20which%20potential,of%20the%20planning%20and%20execution%20of%20sensitive%20activities.

Implementación de los principios de OPSEC

Los siguientes cinco pasos ayudan a los trabajadores electorales a mejorar los procesos y procedimientos para proteger mejor la información confidencial mediante la implementación de los principios de OPSEC. Para obtener una plantilla de trabajo más detallada, consulte el Apéndice A.

- **Paso 1 – Identificar la información confidencial:** Tenga conocimiento a nivel organizacional de todos los datos, activos e información personal que proporcionarían información valiosa a un adversario, ya sea por sí mismos o agregados.
- **Paso 2 – Comprender las amenazas:** Comprenda las tácticas utilizadas por los actores de amenazas que pueden representar riesgos físicos, cibernéticos u operativos.
- **Paso 3 – Identificar vulnerabilidades:** Identifique posibles vulnerabilidades en los procedimientos físicos y de ciberseguridad que podrían permitir a un adversario acceder a la información confidencial identificada en el Paso 1.
- **Paso 4 – Evaluar los riesgos:** Considerando las amenazas identificadas en el Paso 2 y las vulnerabilidades identificadas en el Paso 3, evalúe la probabilidad y seriedad de las acciones de un actor de amenazas contra la seguridad de la infraestructura o los procesos electorales si ganara acceso a información confidencial del Paso 1.
- **Paso 5 – Implementar medidas correctivas:** Seleccionar e implementar medidas correctivas que eliminen o reduzcan los principales riesgos identificados en el Paso 4.[2]

Métodos de recopilación del adversario

Al implementar los principios de OPSEC, es importante pensar en cómo los adversarios pueden agregar información confidencial o *indicadores,* para generar una imagen más completa de las vulnerabilidades de la organización. Los indicadores pueden recopilarse a través de una variedad de actividades, entre ellas:

Ver páginas en redes sociales	Observar las oficinas electorales y al personal o escuchar sus conversaciones a escondidas
Inspeccionar el reciclaje o la basura	Revisar los registros públicos en busca de información de seguridad divulgada por error
Agregar información proveniente de múltiples fuentes, como correos electrónicos, sitios web o propuestas de contratos.	Ingeniería social

[2] Instituto Nacional de Estándares y Tecnología, Centro de Recursos de Seguridad Informática (CSRC) Glosario: Seguridad Operacional (OPSEC). https://csrc.nist.gov/glossary/term/operations_security#:~:text=Definitions%3A%20Systematic%20and%20proven%20process%20by%20which%20potential,of%20the%20planning%20and%20execution%20of%20sensitive%20activities.-

Aplicación de medidas correctivas OPSEC

Las medidas correctivas OPSEC reducen la probabilidad de que la información crítica se divulgue involuntariamente a los actores de amenazas y deben aplicarse a todas las áreas de riesgo de seguridad electoral, incluidas las personas, las operaciones, la ciberseguridad y la seguridad física. La siguiente tabla incluye ejemplos de la aplicación de medidas correctivas OPSEC en diferentes áreas de riesgo.

Áreas de riesgo	Aplicación de medidas correctivas OPSEC
 **Gente**	▪ Siempre que sea posible, evite publicar públicamente detalles sobre actividades relacionadas con el trabajo, planes de viaje, horarios o ubicaciones. ▪ Deshabilite los servicios de ubicación en aplicaciones y dispositivos donde no necesite esas funciones para reducir el riesgo de que los adversarios obtengan metadatos que compartirían ubicaciones confidenciales. ▪ No comparta fotos que hagan obvia una ubicación en tiempo real. ▪ Evite discutir información confidencial en público o cerca de espacios con acceso público, que pueda ser escuchada por personas no autorizadas. ▪ Evite mostrar públicamente detalles personales únicos que puedan revelar identidad y ubicación, como calcomanías en los parachoques. ▪ Considere la posibilidad de hacer que las cuentas personales en las redes sociales sean privadas. ▪ Considere solicitar regularmente que se elimine su información personal de los sitios web de registros públicos. ▪ Habilite la autenticación multifactorial en sus cuentas y use frases de contraseña complejas.
 **Operaciones**	▪ Lleve a cabo entrenamientos periódicos con todo el personal para concientizarlos acerca de la protección de la información confidencial y para que comprendan los riesgos de explotación. ▪ Cree o actualice las directrices de la organización para proteger los datos confidenciales y evitar que se publiquen o difundan accidentalmente. ▪ Cree o actualice directrices organizativas para disponer de la información física y digital de forma segura. ▪ Aplique marcas de confidencialidad a todos los documentos para indicar el tipo de información y el nivel de distribución, según corresponda.
 **Ciberseguridad**	▪ Proteja los detalles de infraestructura, como la información de servicios comerciales específicos, diagramas de red e información de seguridad. ▪ Revise minuciosamente y redacte la información confidencial para evitar la divulgación accidental a través de solicitudes de registros públicos, de acuerdo con las leyes estatales aplicables. ▪ Evite el uso de dispositivos personales para asuntos oficiales, lo que abre vectores adicionales de riesgo.
 **Seguridad Física**	▪ Evite que el personal use públicamente insignias u otras formas de identificación fuera del trabajo. ▪ Restrinja el acceso a los planos de las instalaciones, especialmente planos que revelen los puntos de acceso de seguridad y los lugares donde se almacenan equipos confidenciales en una instalación electoral. ▪ Revise periódicamente materiales como manuales, videos de capacitación y contenido educativo, para detectar la divulgación inadvertida de información confidencial de seguridad física.

Conclusión

Al igual que las elecciones son operaciones continuas, el ciclo de revisión y actualización de las prácticas OPSEC debe aplicarse continuamente en todos los aspectos de una organización para evitar la divulgación de información confidencial. A través de una cuidadosa planificación, documentación y capacitación, la aplicación de los principios de OPSEC puede ayudar a los funcionarios electorales a salvaguardar aún más la infraestructura electoral de posibles actores de amenazas. Los principios de OPSEC también deben evolucionar para hacer frente a un entorno de amenazas cambiante y a las nuevas tácticas de los actores de amenazas.

Más recursos relacionados con OPSEC

La información proporcionada en este documento se complementa con recursos adicionales sobre OPSEC de CISA y los socios federales de CISA que se vinculan a continuación. Se alienta a las partes interesadas en las elecciones a revisar estos recursos para prepararse aún más y mitigar los riesgos asociados con posibles incidentes de OPSEC.

- Guía de mitigación de amenazas internas de CISA: https://www.cisa.gov/resources-tools/resources/election-infrastructure-insider-threat-mitigation-guide
- CISA Seguridad Física de los Lugares de Votación e Instalaciones Electorales: https://www.cisa.gov/resources-tools/resources/physical-security-voting-locations-and-election-facilities
- Guía de acción y consideraciones de seguridad personal de CISA: https://www.cisa.gov/resources-tools/resources/personal-security-considerations-action-guide
- Mejores Prácticas de la Comisión de Asistencia Electoral de los Estados Unidos (EAC): Solicitud de Registros Públicos: https://www.eac.gov/election-officials/best-practices-public-records-request
- Centro Nacional de Contrainteligencia y Seguridad OPSEC posters y plantillas: https://www.dni.gov/index.php/ncsc-what-we-do/operations-security
- Definición de seguridad operativa del Instituto Nacional de Estándares y Tecnología (NIST): https://csrc.nist.gov/glossary/term/operations_security

APÉNDICE A: PASOS PARA MEJORAR LA SEGURIDAD OPERATIVA

Paso OPSEC	Mejores Prácticas/Detalles de Implementación
Paso 1 – Identificar la información confidencial: Tenga conocimiento a nivel organizacional de todos los datos, activos e información personal que proporcionarían información valiosa a un adversario, ya sea por sí mismos o agregados.	**Identifique y revise toda la información confidencial rutinariamente.** • Forme un equipo multidisciplinario para identificar la información confidencial. • Desarrolle una lista que proporcione un inventario de información confidencial. • Confirme los registros o documentos que deben evaluarse para su inclusión en la lista de información confidencial. • Si utiliza un nuevo servicio o un nuevo proveedor de servicios, revise su información para detectar cualquier posible inclusión en la lista de información confidencial. • Capacite a los miembros del equipo, e incluya las partes clave y su equipo legal (dentro y fuera de su oficina), sobre la lista de información confidencial. • Establezca un proceso de enrutamiento para que el equipo multidisciplinario pueda revisar la información o el material de solicitud de datos antes de compartirlo con el solicitante, como con las solicitudes de registros públicos.
Paso 2 – Comprender las amenazas: Comprenda las tácticas utilizadas por los actores de amenazas que pueden representar riesgos físicos, cibernéticos u operativos.	**Evalúe las amenazas potenciales y revise esta evaluación periódicamente.** • Identificar quién es el actor de la amenaza (adversarios extranjeros, actores criminales, etcétera) y cuál es su objetivo. • Considere qué sistemas o información puede un actor de amenazas atacar para cumplir su objetivo. • Comprenda las capacidades y el nivel de sofisticación del actor de amenazas. ¿Pueden hacerlo ellos mismos o necesitan ayuda, posiblemente una ayuda a nivel interno?
Paso 3 – Identificar vulnerabilidades: Identifique posibles vulnerabilidades en los procedimientos físicos y de ciberseguridad que podrían permitir a un adversario acceder a información confidencial crítica.	**Evalúe las amenazas que puedan existir para la información confidencial identificada en el paso 1.** • Identificar los riesgos potenciales y las vulnerabilidades en la infraestructura y los procesos electorales que pueden llevar a la exposición de información confidencial identificada en el Paso 1, en contraste con las capacidades adversarias identificadas en el Paso 2. • Al revisar el riesgo potencial, considere un enfoque ante todo tipo de riesgo (por ejemplo, ataques físicos, cibernéticos, de información).
Paso 4 – Evaluar los riesgos: Considere la probabilidad y la gravedad de las acciones de un actor de amenazas sobre la seguridad de la infraestructura o los procesos electorales si tuviera acceso a información confidencial.	**Evalúe los riesgos que presentan las vulnerabilidades documentadas en el paso 3.** • Revise la probabilidad de que ocurra la amenaza y, a continuación, la gravedad del impacto (bajo, significativo, catastrófico, etcétera) si esa amenaza ocurriera. • Considere las vulnerabilidades/impacto/probabilidad desde la perspectiva de la tríada de seguridad de información: Confidencialidad, Integridad y Disponibilidad. • Priorizar los riesgos e implementar un plan de acción.
Paso 5 – Implementar medidas correctivas: Seleccione e implemente medidas correctivas que eliminen o reduzcan el riesgo.	**Configure políticas/procesos/controles/dispositivos que se puedan implementar para mitigar los riesgos del paso 4.** • Si no puede tomar acción a todo nivel, comience con los riesgos prioritarios. • Cree procesos para verificar las entidades que solicitan recibir información; implemente el control/monitoreo bipartidista de las operaciones y activos críticos; utilice métodos de verificación de identidad físicos y electrónicos. • Desarrolle procedimientos de notificación para informar sobre posibles violaciones de OPSEC y pasos para responder y recuperarse si una posible

	violación se convierte en un incidente. • Lleve a cabo entrenamientos regulares para poner a prueba los planes de mitigación y responder a la divulgación no autorizada de información confidencial. • Desarrolle y esté listo a utilizar comunicados de prensa y otros materiales de comunicación preparados previamente en el evento de un incidente. • Revise las listas de contactos de las partes involucradas para verificar que sean precisas. • Revise los procedimientos de verificación de identificación para asegurarse de que los planes de mitigación sean resistentes a la ingeniería social (es decir, ¿todos conocen las "frases de contraseña" actuales y cada cuándo cambian?). • Utilice escenarios para probar la capacidad de su plan para responder adecuadamente y mitigar las consecuencias de una divulgación. Por ejemplo: ○ Una lista de nombres de usuario y contraseñas administrativas del sistema de votación es robada. ○ La información de identificación personal de una lista de registro de votantes se envía erróneamente a una parte no autorizada. ○ Una lista de votantes confidenciales se envía erróneamente a una organización de medios de comunicación. ○ Se descubre que los informes de análisis de vulnerabilidades de un análisis de ciberseguridad reciente o los resultados de una prueba de penetración reciente se han enviado por correo electrónico a una parte que no es confiable.