
# Guía para mitigar amenazas internas a la infraestructura electoral

## INTRODUCCIÓN

Las personas a quienes se les confía el acceso a la infraestructura electoral pueden, en ocasiones, representar riesgos potenciales para la confidencialidad, integridad y disponibilidad de los sistemas y la información electoral. Esto incluye empleados actuales y previos, voluntarios, contratistas y cualquier otra persona a quien se le haya otorgado acceso privilegiado a los sistemas e información. En todos los sectores de infraestructura crítica y prácticamente en todos los entornos organizacionales, los empleados de confianza pueden causar daños de manera intencional o no intencional.

Las prácticas que disuaden detectan o previenen el daño causado por personas con información privilegiada son parte integral de llevar a cabo elecciones seguras. Esta guía ayuda a quienes trabajan en el subsector de infraestructura electoral a mejorar las prácticas existentes de mitigación de amenazas internas y establecer un programa de mitigación de amenazas internas; resume y amplía guías de recursos que CISA ha emitido anteriormente acerca de la mitigación de amenazas internas para las partes involucradas en la infraestructura crítica.

## DEFINICIÓN DE AMENAZAS INTERNAS[1]

Amenaza interna se refiere a la posibilidad de que una persona infiltrada use su acceso autorizado o su conocimiento acerca de una organización para causarle daño. Esto puede incluir actos maliciosos, complacientes o no intencionales que afecten negativamente la integridad, confidencialidad y disponibilidad de la organización, sus datos, personal o instalaciones.

### Amenazas no intencionales

Las amenazas internas pueden ser no intencionales, incluyendo casos de negligencia o accidentes.

- **Negligente**: El personal interno puede exponer a una organización a daños por su descuido. Este tipo de personal interno generalmente está familiarizado con las políticas de seguridad y/o IT, pero elige ignorarlas, creando un riesgo para la organización. El personal interno negligente suele ser complacientes o muestra un desprecio intencional por las reglas. Exhibe comportamientos que pueden ser presenciados y corregidos.

- **Accidental**: Incluso el mejor empleado puede cometer un error que cause un riesgo indeseable para la organización. Las organizaciones pueden implementar estrategias para limitar el riesgo, pero aún pueden ocurrir accidentes. Si bien los accidentes no se pueden prevenir por completo, el riesgo se puede reducir mediante la capacitación y los controles apropiados.

### Amenazas intencionales

El personal interno puede actuar intencionalmente con el fin de perjudicar a una organización para beneficio personal o para hacer algo respecto a una queja personal. Algunas personas están motivadas por un descontento relacionado con una queja percibida, ambición o presiones financieras. Otros pueden tener un deseo de reconocimiento y buscar atención creando peligro o divulgando información confidencial. Incluso pueden pensar que están actuando en el bien público.

### Otras amenazas

Además de las amenazas internas que tan solo involucran a miembros internos de una organización, las amenazas internas también pueden involucrar a personas externas a la organización. Estas amenazas colusorias por parte de terceros pueden ser intencionales o no intencionales.

- **Colusión**: Esta amenaza ocurre cuando una o más personas infiltradas colaboran con un actor de amenazas externo para poner a una organización en peligro. Estos incidentes involucran con frecuencia a ciberdelincuentes que reclutan a una o varias personas para llevar a cabo fraude, robo de propiedad intelectual, espionaje, sabotaje o una combinación de los mismos.
  Este tipo de amenaza interna puede ser difícil de detectar, ya que los actores externos suelen estar bien

[1] Definiciones extraídas de: " "Insider Threat Mitigation Guide." Cybersecurity and Infrastructure Security Agency, 2020. https://www.cisa.gov/sites/default/files/publications/Insider Threat Mitigation Guide_Final_508.pdf

versados en prácticas y estrategias de seguridad para evitar ser detectados.

- **Amenazas de terceros:** Las amenazas por parte de terceros están asociadas con contratistas o proveedores que no son miembros formales de una organización, pero a quienes se les ha otorgado acceso a las instalaciones, sistemas, redes o personas para llevar a cabo su trabajo. Este tipo de amenaza puede implicar colusión entre múltiples entidades de terceros. Las amenazas por parte de terceros pueden ser directas, donde específicos individuos ponen en peligro a una organización objetivo; o indirectas, donde puede haber fallas o sistemas obsoletos que exponen a la organización a actores de amenazas no intencionales o maliciosos.

**Ejemplos de amenazas no intencionales**

- Permitir que alguien le siga a través de un punto de entrada seguro
- Extraviar o perder dispositivos de almacenamiento portátiles o medios que contienen información confidencial
- Ignorar mensajes para instalar nuevas actualizaciones de software o parches de seguridad
- Escribir mal una dirección de correo electrónico y enviar externamente un documento confidencial por accidente
- Hacer clic en un hipervínculo o correo electrónico de phishing inadvertidamente
- Eliminar incorrectamente documentos o datos confidenciales

**Ejemplos de amenazas intencionales**

- Intentar alterar o destruir papeletas, sobres de boletas por correo, formularios de registro u otros documentos electorales básicos
- Intentar violar el secreto electoral
- Intentar alterar o destruir los datos electorales, incluidos los datos de registro de votantes
- Permitir que una persona no autorizada acceda a equipos, sistemas, activos o datos electorales
- Apagar cámaras de seguridad o sistemas de control de acceso
- Robo de equipos o datos electorales
- Filtrar información confidencial a la prensa o al público
- Intimidar o amenazar a otros miembros del personal

## Ejemplos de amenazas internas

Las amenazas internas se manifiestan de diversas maneras, tales como violencia, espionaje, sabotaje, robo e incidentes de ciberseguridad.

- **Incidentes de ciberseguridad**: Estos incluyen una variedad de acciones, que pueden incluir robo, espionaje, violencia o sabotaje, que se relacionan con cualquier cosa referente a tecnología, realidad virtual, computadoras, dispositivos o internet. Estas acciones se llevan a cabo utilizando una variedad de vectores, como virus, filtración de datos, negación de ataques al servicio, malware o software sin parches, y pueden ser intencionales o no intencionales.
- **Violencia**: Un acto de violencia, amenazas de violencia u otro comportamiento amenazante que crea un entorno intimidante, hostil o abusivo. La violencia interna incluye amenazas criminales o destructivas, que preceden a un ataque físico y dañan la infraestructura o dañan la salud y la seguridad de un individuo u organización. Esto puede incluir terrorismo o violencia en el lugar de trabajo/organización.
- **Espionaje**: La práctica de espiar a un gobierno, organización, entidad o persona extranjera para obtener de manera encubierta o ilícita información confidencial o sensible para obtener beneficios militares, políticos, estratégicos o financieros. Esto incluye espionaje criminal, económico o gubernamental.
- **Sabotaje**: Implica acciones deliberadas destinadas a dañar la infraestructura física o virtual de una organización, incluido el incumplimiento de los procedimientos de mantenimiento o de IT, la contaminación de espacios limpios, el daño físico a las instalaciones o la modificación o eliminación de código para interrumpir las operaciones.
- **Robo**: Involucra múltiples tipos de robo, más a menudo relacionados con finanzas o propiedad intelectual. El delito financiero es la toma no autorizada o el uso ilícito del dinero o la propiedad de una persona, empresa u organización con la intención de beneficiarse de ello. El robo también incluye el robo de propiedad intelectual o el robo de ideas, invenciones y/o expresiones creativas de una persona u organización.
  Los sistemas digitales que contienen grandes cantidades de datos de clientes o propiedad intelectual pueden ser más atractivos para los actores maliciosos.

### ¿QUÉ ES MDM?

CISA utiliza las siguientes definiciones de la información errónea, la desinformación y la información maliciosa (MDM, por sus siglas en inglés). MDM puede originarse a partir de fuentes tanto extranjeras como nacionales.

- **La información errónea** es falsa, pero no se crea ni se comparte con la intención de causar daño.
- **La desinformación** se crea deliberadamente para engañar, dañar o manipular a una persona, grupo social, organización o país.
- **La información maliciosa** se basa en hechos, pero se usa fuera de contexto para engañar, dañar o manipular.

### Amenazas internas y la información errónea, la desinformación y la información maliciosa

El entorno de información que rodea a las elecciones y, en particular, la diseminación de información errónea, desinformación e información maliciosa (MDM) relacionada con las elecciones, puede proporcionar una motivación adicional para las amenazas internas.
El contenido de MDM a menudo está diseñado para provocar una fuerte respuesta emocional por parte del consumidor y eludir el razonamiento lógico para incitar a la acción, ya sea que la acción sea simplemente difundir el contenido en las redes sociales o tomar medidas en el mundo real, incluidos actos o amenazas de violencia.
Una táctica común desplegada por los actores de MDM nacionales y extranjeros es reforzar un fuerte sentido de pertenencia, comunidad y mentalidad de grupo entre aquellos que consumen regularmente su contenido.
En los casos cuando un individuo ya tiene una queja con una organización o está experimentando otros factores estresantes en su vida, las narrativas de MDM pueden proporcionar una interpretación alternativa de la realidad que parece ser mejor que la vida real. Esta vulnerabilidad puede generar o exacerbar amenazas internas.

Si bien las partes involucradas en la infraestructura electoral no pueden predecir o controlar por completo el entorno de información acerca de las elecciones, estas pueden educar a su personal, voluntarios y proveedores sobre las narrativas y tácticas de MDM. Las oportunidades de capacitación y educación continuas son especialmente importantes para personal que no sea de tiempo completo, ya que pueden unirse a la organización sin pleno conocimiento de los procesos electorales o de cómo pueden verse afectados por el contenido de MDM.
De manera similar, las partes interesadas en la infraestructura electoral pueden mitigar el impacto de las narrativas de MDM manteniendo una comunicación proactiva y consistente con el público sobre los procesos electorales. Tal comunicación puede ayudar a evitar alimentar las narrativas de MDM y desarrollar la resiliencia organizacional contra ellas. Cuando se comunica acerca de los procesos electorales, las partes involucradas en la infraestructura electoral deben tratar de proporcionar información directa y concisa sin demasiados detalles, y sin causar más confusión.
El entorno actual de MDM, a nivel local, nacional e internacional, debe tenerse en cuenta al evaluar las amenazas internas. La comunicación transparente, junto con las medidas de prevención y detección que se describen a continuación, puede ayudar al personal a comprender y desempeñar su función, conectarla con la misión de la organización de administrar elecciones seguras y mantenerse resiliente frente a las posibles narrativas de MDM que socavan esa misión y potencialmente incitan al personal interno a causar daño intencional.

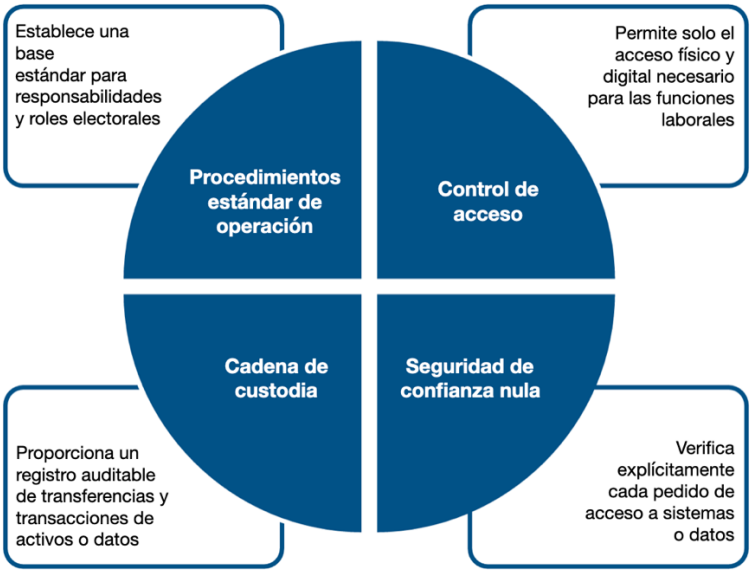
## CREAR UN PROGRAMA PARA MITIGAR AMENAZAS INTERNAS

Los funcionarios electorales y sus socios del sector privado emplean regularmente prácticas diseñadas para disuadir, detectar o prevenir actos dañinos por parte del personal interno, ya sea que usen o no el término "amenaza interna" o hayan articulado su enfoque y prácticas en un programa documentado. Desde el manejo de papeletas en equipos de dos hasta los estrictos procedimientos de cadena de custodia y la presencia de observadores durante la votación y el conteo, muchas prácticas electorales básicas arraigadas se han diseñado teniendo en cuenta la mitigación de amenazas internas. Sin embargo, las partes involucradas en la infraestructura electoral pueden beneficiarse al documentar su enfoque y establecer un programa de mitigación de amenazas internas más formal. Tales acciones pueden ayudar a identificar brechas en las prácticas actuales e informar el enfoque más amplio de la organización para el manejo de riesgos.
Los programas exitosos para mitigación de amenazas internas emplean prácticas, estrategias y sistemas comprobados que limitan y rastrean el acceso a través de funciones, servicios y aplicaciones organizacionales. Esas prácticas y sistemas limitan la cantidad de daño que puede causar el personal interno, sea el acto intencional o no.
Un enfoque holístico de varios niveles para la mitigación de amenazas internas combina la seguridad física y digital con la participación del personal. Un programa de mitigación efectivo tiene como objetivo comprender la interacción

del personal interno dentro de una organización, rastrear la interacción según corresponda y lo permita la ley, e intervenir si la interacción representa una amenaza para la organización. El programa de mitigación de amenazas internas de una organización es un componente esencial del plan más amplio de manejo de riesgos de la organización.
Una base sólida para la prevención y mitigación de amenazas internas proviene de un conjunto de valores compartidos y aplicados por todos en la organización. **Las organizaciones deben promover un clima positivo de responsabilidad, transparencia y confianza.** La cultura organizacional también debe alentar a los empleados a reportar incidentes como componente integral para proteger el ambiente.

## Elementos clave de los programas para mitigación de amenazas internas en la infraestructura electoral

Desde una cultura proactiva y de apoyo, las partes involucradas en la infraestructura electoral pueden implementar varias medidas proactivas y preventivas para reducir el riesgo y el impacto de las amenazas internas. Si bien cada aspecto es importante individualmente, son más efectivos cuando se implementan juntos para crear un entorno de administración electoral integral y resiliente. Los elementos clave de los programas para mitigación de amenazas internas de la infraestructura electoral incluyen: Establecimiento de procedimientos estándar de operación (SOP, por sus siglas en inglés), administración del control de acceso físico y digital, implementación de principios de seguridad de confianza nula e implementar procesos de cadena de custodia.




## Procedimientos estándar de operación

El establecimiento e implementación de SOPs ayuda principalmente a prevenir amenazas internas no intencionales debido a negligencia o accidentes. Los SOPs describen cómo se deben realizar las funciones organizacionales y estandarizan las diversas tareas y responsabilidades asociadas con los diferentes roles, aumentando la calidad y la coherencia del trabajo entre el personal. Especialmente en un entorno electoral, donde los voluntarios y los proveedores externos rotan regularmente, los SOPs pueden ayudar a los empleados a incorporarse rápidamente, comprender las expectativas de su función y desempeñar sus funciones con éxito. Además, los SOPs crean una base para medir los resultados e identificar áreas de mayor eficiencia y mejoramiento.

Los SOPs para cada función o responsabilidad deben documentar claramente los pasos necesarios para realizar la actividad con éxito. Esto incluye proporcionar pasos secuenciales para completar tareas, mostrar imágenes y ejemplos, y especificar las listas de verificación y los registros necesarios para la verificación. Los SOPs incompletos o inexistentes pueden hacer que el personal desarrolle sus propios procedimientos, lo que puede generar un riesgo adicional. Por lo tanto, los SOP limitan toma de decisiones *ad hoc* y ayudan a remediar rápidamente problemas que puedan surgir.

## Control de acceso

Los sistemas de control de acceso físico y digital previenen y detectan amenazas internas. Los controles de acceso

físico pueden incluir límite de acceso a las instalaciones, los equipos, los dispositivos, los sellos y bolsas a prueba de manipulaciones y otros activos, así como vigilancia por video de los activos físicos. Los controles de acceso digital otorgan acceso solo a los sistemas, activos, datos o aplicaciones necesarios relacionados con el trabajo o la función de una persona. En ambos casos, los registros de acceso, los formularios de control y el video de vigilancia brindan registros auditables de quién accedió a un activo físico o digital, así como cuándo se accedió. En general, los sistemas de control de acceso evitan que cualquier individuo obtenga acceso a todos los activos dentro de una organización, lo que reduce el daño potencial a los sistemas físicos o digitales. Si se sospecha de un incidente, los registros de acceso y los formularios de control pueden ayudar a identificar quién es responsable del comportamiento potencialmente dañino.

Los sistemas de control de acceso deben aplicar el **principio de acceso con privilegios mínimos** para otorgar a todas las personas (personal de tiempo completo, voluntarios y proveedores) acceso solo a los sistemas y datos necesarios para realizar sus funciones esenciales. Los privilegios de acceso pueden cambiar antes de una elección u otras fechas clave. Además, las organizaciones deben asegurarse de que el acceso se revoque de inmediato cuando una persona finaliza su trabajo o deja la organización (p. ej., desactivar el acceso a las instalaciones para los proveedores una vez que completan el mantenimiento de rutina).

Un desafío clave en torno al control de acceso para los funcionarios electorales es el acceso al sistema estatal de base de datos de registro de votantes. Es posible que el estado no sepa quién tiene acceso dentro de cada oficina electoral local, por lo que es importante que las jurisdicciones y las oficinas estatales trabajen juntas para confirmar y actualizar regularmente una lista de usuarios autorizados y privilegios asociados.

## Principios de seguridad de confianza nula

Un enfoque de seguridad de confianza nula se basa en el principio de “siempre verificar". En lugar de asumir que todo lo que sucede en las redes y sistemas de una organización es seguro, el enfoque de confianza nula asume que se ha producido o se producirá una infracción y verifica cada solicitud como si no estuviera autorizada. Anteriormente, en muchas organizaciones, la seguridad de los activos digitales estaba estrechamente ligada a la ubicación física donde se almacenaban y la confianza universal en todos los miembros de la organización. En otras palabras, todos los dispositivos de una oficina y todos los usuarios del personal pueden acceder a la mayoría de la información, los sistemas y los datos. Esta confianza implícita de los dispositivos o usuarios facilitó que las amenazas internas se manifestaran en una organización sin ser detectadas. Por el contrario, el enfoque de confianza cero verifica explícitamente cada solicitud de acceso, independientemente de dónde se origine o a qué recurso acceda. Muchos sistemas digitales ahora incluyen funciones de seguridad de confianza cero que se pueden activar, como solicitar siempre a los usuarios que ingresen su contraseña en lugar de almacenarla en la memoria del dispositivo. Las partes interesadas en la infraestructura electoral también pueden considerar procedimientos como implementar la "regla de dos personas" (requiere que al menos un observador esté presente) o trabajar en equipos bipartidistas al acceder a recursos confidenciales.

Visite https://zerotrust.cyber.gov/ para obtener orientación adicional sobre la implementación de confianza cero de CISA y la Oficina de Administración y Presupuesto (OMB).

## Cadena de custodia

La cadena de custodia es un proceso transparente para rastrear el movimiento y el control de activos físicos y digitales mediante la documentación de cada persona y organización que manejó un activo, equipo sensible o datos; la fecha y hora en que fue recolectado, transportado o transferido; y por qué se manejó el activo. Si bien no es exclusivo de las elecciones, la cadena de custodia desempeña un papel vital para garantizar la integridad de una elección y proporcionar evidencia en caso de que se detecte una amenaza interna, así como mejorar el tiempo de reparación si ocurre un incidente. Sin prácticas sólidas de cadena de custodia, los equipos de sistemas electorales, los activos o los datos en reposo o en tránsito podrían ser accedidos y manipulados sin saberlo por los actores de amenazas.

Las elecciones son complejas y hay muchas funciones que componen el intrincado proceso de llevar a cabo una elección. En cada punto donde se ingresan, acceden, transfieren, transmiten o almacenan datos, medios o equipos, existe una oportunidad de error o riesgo. Las prácticas sólidas de cadena de custodia reducen este riesgo al crear un rastro auditable de activos a lo largo del proceso electoral.

Con el fin de evaluar el riesgo y mejorar la seguridad y la resiliencia,

Ejemplo: un procedimiento de cadena de custodia podría requerir que al menos dos personas firmen todos los equipos, materiales transportados o registros de acceso a los medios: el usuario principal y un testigo que garantice que el equipo, los medios u otros activos se manejaron adecuadamente. En ausencia de este requisito, puede ser difícil verificar quién accedió o transportó el equipo, los medios u otros activos y para qué propósito.

las partes interesadas en la infraestructura electoral pueden utilizar marco de seguridad cibernética del Instituto Nacional de Estándares y Tecnología (NIST) para establecer estándares, pautas y prácticas de cadena de custodia. NIST describe un proceso de cinco pasos para identificar activos y riesgos, proteger sistemas, detectar incidentes, responder a infracciones y recuperarse.
Establecer y mantener los procedimientos estándar de operación necesarios, los controles de acceso, la seguridad de confianza nula y los procedimientos de cadena de custodia son facetas de la administración electoral necesarias. Además, deben ser revisados, puestos a prueba y auditados antes, durante y después de las elecciones. En conjunto, estas medidas respaldan la integridad, confiabilidad y seguridad de una elección, brindando evidencia para generar confianza pública en el proceso.

## LAS AMENAZAS INTERNAS DE LAS ELECCIONES EN EL PUNTO DE MIRA

En la mayoría de las jurisdicciones, los funcionarios electorales administran las elecciones con la asistencia de personal temporal o estacional, voluntarios, proveedores y contratistas. Al igual que las amenazas potenciales planteadas por el personal de tiempo completo, estas personas pueden representar una amenaza interna. Por lo tanto, los funcionarios electorales deben asegurarse de que todas las personas involucradas en las elecciones sean consideradas, según sus funciones y responsabilidades específicas, al desarrollar un programa parta mitigar las amenazas internas.

### Proveedores y contratistas

Los proveedores y contratistas deben cumplir con el mismo nivel de estándares de seguridad que los empleados. Los funcionarios electorales deben asegurarse de incorporar en sus procesos de adquisición y requisitos de contratación las mismas salvaguardas que tienen para sus propios empleados. Al adquirir nuevos servicios contratados, los requisitos de seguridad y las calificaciones mínimas deben incorporarse en las solicitudes de propuestas y en los acuerdos contractuales finales, como las verificaciones de antecedentes obligatorias para todas las personas que trabajarán en el contrato.

Es probable que los proveedores y contratistas tengan el mismo o mayor acceso físico y/o digital a ciertos datos críticos que el personal de tiempo completo y, por lo tanto, conllevan un riesgo similar, si no mayor, para la infraestructura electoral. Los funcionarios electorales deben considerar restringir o eliminar el acceso remoto a los sistemas o activos electorales por parte de los contratistas, limitar el acceso solo a los sistemas y datos requeridos para realizar el servicio contratado y, cuando sea posible, tener un funcionario del gobierno presente cuando los contratistas accedan a sistemas o datos críticos (pero como mínimo siempre requieren que al menos dos personas estén presentes). Cuando sea posible, separe las cuentas de proveedores y contratistas de las de los empleados regulares y utilice dispositivos administrados por la organización para prohibir los dispositivos que no son de confianza en la red. Considere proporcionar a las personas un cordón de color, placa, chaleco o artículo similar cuando trabajen en instalaciones gubernamentales para que sea fácil para todos identificar quién debe o no debe estar en áreas seguras.

### Personal temporal, personal estacional y voluntarios

La mayoría de las oficinas electorales dependen de trabajadores temporales, estacionales y/o voluntarios para llevar a cabo las operaciones electorales, incluida la operación de equipos electorales y el transporte de medios o materiales electorales sensibles, procesar formularios de registro de votantes, manejar formularios de solicitud de papeletas por correo, administrar papeletas por correo y otras tareas de administración electoral. La construcción de un equipo exitoso de personal temporal y voluntario comienza con el reclutamiento de personas que entienden la misión de la organización y poseen un alto grado de responsabilidad por su función. Al unirse a la organización, se debe exigir a todos los nuevos miembros que firmen un código de conducta que articule claramente el comportamiento esperado y describa las consecuencias de las violaciones.

## DETECCIÓN E IDENTIFICACIÓN DE AMENAZAS INTERNAS

Incluso las medidas preventivas y de protección más sólidas no pueden eliminar por completo el riesgo de amenazas internas intencionales o no intencionales. Por lo tanto, es importante que las partes interesadas en la infraestructura electoral prueben y auditen sus procedimientos de manera rutinaria, lo que ayudará a identificar las brechas procesales y responder a las amenazas cambiantes en las elecciones. La detección de amenazas se lleva a cabo mediante revisión humana y herramientas técnicas que monitorean la presencia de indicadores de amenazas.
Como aquellos que cometen actos de violencia o roban datos suelen compartir sus planes o quejas con otros antes de actuar, los compañeros de trabajo, compañeros, amigos, vecinos, familiares u observadores ocasionales suelen estar posicionados para conocer y ser conscientes de las predisposiciones, los factores estresantes y los comportamientos de los demás. internos que están considerando actos maliciosos.
Cada individuo tiene una base de comportamiento y desviarse de su norma podría ser una indicación de que algo en ellos ha cambiado fundamentalmente. Importante para el proceso de identificación de indicadores de amenazas potenciales es comprender que el **comportamiento es lo que más importa**, no la motivación. La presencia de motivaciones políticas, religiosas, ideológicas, financieras o basadas en la venganza ayuda a comprender qué impulsa a un individuo a actuar, pero los indicadores de comportamiento del individuo son la clave para determinar si merecen consideración, monitoreo o evaluación adicionales como una amenaza potencial.

### Medidas preventivas contra amenazas internas como mecanismos de detección

Las medidas preventivas contra amenazas internas, incluidos SOP, sistemas de control de acceso, seguridad de confianza nula y cadena de custodia, también contribuyen a detectar e identificar amenazas al establecer sistemas y procesos electorales transparentes y auditables. Sin embargo, la detección efectiva a través de estas medidas requiere la comprensión y supervisión humana para garantizar que se apliquen adecuadamente y se auditen de forma rutinaria para identificar valores atípicos para una mayor investigación. Disponer de medidas preventivas significa poco si no se utilizan de manera sistemática.

Cada medida puede ayudar a la detección de amenazas de las siguientes maneras:

- **Procedimientos operativos estándar**: Los SOPs y las mejores prácticas proporcionan una base común para que un equipo mida y detecte cuándo no se están siguiendo las mejores prácticas.
- **Sistemas de control de acceso**: Estos sistemas generan registros de acceso y filmaciones de seguridad que se pueden revisar para verificar el acceso a los sistemas físicos y digitales y detectar si se ha producido un acceso no autorizado.
- **Seguridad de confianza nula**: Al igual que los sistemas de control de acceso, las medidas de seguridad de confianza nula proporcionarán un registro de acceso a los sistemas y datos digitales. Al validar la identidad de un usuario en cada solicitud de acceso, las medidas de confianza cero brindan información granular sobre el acceso.
- **Cadena de custodia**: La cadena de custodia produce un registro auditable de las transferencias y transacciones de un activo, lo que permite detectar una amenaza potencial si hay una brecha en la cadena.

### Monitoreo continuo

El monitoreo de amenazas internas, así como de cualquier problema con los sistemas implementados, debe ser continuo. Esto implica una combinación de herramientas humanas y digitales, respaldada por una sólida cultura organizacional de informes proactivos. Todos los empleados tienen un papel que desempeñar en el proceso para responsabilizarse a sí mismos y a los demás por seguir los procedimientos establecidos. A través de un monitoreo proactivo y continuo, incluso la oficina electoral más organizada y con mejores recursos puede encontrar prácticas que están desactualizadas o que no se siguen de manera consistente, dejando a la organización expuesta a riesgos si no se abordan adecuadamente. Finalmente, todos los procedimientos y prácticas, incluidos los programas de monitoreo, deben revisarse y actualizarse regularmente para cumplir con las leyes federales, estatales y locales aplicables.

### Auditoría

Las auditorías internas de todos los procesos comerciales y electorales deben ser una parte rutinaria de la administración electoral antes, durante y después de una elección. Las auditorías validan si las medidas, como el control de acceso y la cadena de custodia, funcionan correctamente, recopilan y mantienen los datos o el equipo necesarios, y si el personal los utiliza correctamente. También brindan la oportunidad de revisar registros (registros de acceso, imágenes de seguridad, formularios de cadena de custodia, etc.) e identificar posibles lagunas o áreas de

mejora. Las auditorías deben usarse para buscar evidencia que demuestre la efectividad y durabilidad de los procedimientos, procesos, sistemas y prácticas de capacitación.
Se anima a las partes involucradas en la infraestructura electoral a identificar un cronograma para auditorías periódicas que tenga sentido para su flujo de trabajo y capacidad; las auditorías internas más pequeñas y frecuentes de diferentes procesos pueden ser menos perturbadoras que una gran auditoría de fin de año. Se recomienda incorporar auditorías en los SOPs de una organización. Los interesados en la infraestructura electoral no deben esperar solicitudes externas para realizar auditorías de sus sistemas y procesos.
Transparencia
El proceso electoral es transparente y está abierto al escrutinio público, lo que brinda una fortaleza única en comparación con muchas otras áreas de infraestructura crítica. Permitir que el público ayude y observe el proceso electoral puede ayudar a iluminar los puntos en los que el proceso no está claro y brindar oportunidades para realizar mejoras. Desde la perspectiva de las amenazas internas, la participación pública puede resultar en la detección de "falsos positivos" debido a la falta de claridad o comprensión. Esto subraya la importancia de documentar los procedimientos minuciosamente, probarlos y auditarlos, y educar al público sobre ellos.

## EVALUACIÓN DE AMENAZAS

La evaluación de amenazas internas es el proceso de recopilación y análisis de información sobre una persona de interés que puede tener el interés, el motivo, la intención y la capacidad de causar daño a una organización o personas, con el objetivo de prevenir un incidente interno en cualquier de sus expresiones. El equipo de gestión de amenazas internas que realiza la investigación debe responder varias preguntas clave:

1. *¿Existe evidencia que sugiera que la persona de interés representa una amenaza?*
2. *¿Qué tipo de amenaza plantea la persona de interés?*
3. *¿Se está moviendo la persona de interés hacia la comisión de un acto malicioso?*

### Intervención que no es de emergencia

Si la evaluación inicial de estas tres preguntas indica que no existe un potencial inmediato de amenaza, entonces la organización debe comenzar, en la medida autorizada por la ley, una investigación más profunda para recopilar información, evaluar el riesgo y determinar próximos pasos. Durante la etapa de investigación, es posible que el equipo de gestión de amenazas internas deba considerar consultar con un profesional externo de evaluación de amenazas, consultar con un asesor legal y/o iniciar la coordinación con las fuerzas del orden, según sea necesario.

El propósito de la investigación es recopilar evidencia (incluso de los sistemas de control de acceso, registros de seguridad y formularios de cadena de custodia), determinar el comportamiento de referencia de la persona de interés y los cambios a partir de él, analizar el riesgo de avanzar hacia un acto malicioso y documentar los resultados.
Con base en la investigación, el equipo puede determinar los próximos pasos, que pueden incluir, entre otros, observar y esperar, cambiar o restringir los privilegios de acceso, tomar medidas administrativas como suspensión o despido, ayudar a encontrar asesoramiento o apoyo externo y /o informar a la policía.

### Intervención de emergencia

Si se determina que se requiere una intervención de emergencia en función de la evaluación inicial, entonces la organización debe tomar medidas inmediatas, lo que incluye pedir ayuda a los socorristas o a las fuerzas del orden si es necesario.
En caso de violencia física o sabotaje, el equipo debe iniciar el Plan de respuesta a incidentes de la organización, omitir la evaluación inicial, comunicarse con las autoridades correspondientes y comenzar una investigación tan pronto como sea seguro hacerlo. En casos de violencia dirigida o sabotaje, la intervención de emergencia a veces puede resultar en la necesidad de evacuar un lugar o instalación, iniciar un cierre o refugiarse en el lugar. La organización debe tener planes establecidos para cada respuesta y coordinarse en toda la organización para la acción inmediata.

## MANEJO DE LAS AMENAZAS INTERNAS

Como se mencionó anteriormente, la mitigación efectiva de las amenazas internas requiere que las organizaciones fomenten una cultura positiva y de apoyo que aliente a los empleados a denunciar comportamientos inusuales. Una parte integral de este objetivo es un proceso transparente y coherente para la presentación de informes, donde tanto el personal como el público saben que sus informes serán reconocidos, tomados en serio y manejados de manera adecuada. Las partes interesadas en la infraestructura electoral deben enfatizar que la contribución hacia este objetivo es compartida por todos en la comunidad, incluido el personal, los proveedores y los voluntarios envueltos en la administración de las elecciones. Los programas que fomentan la notificación y la intervención tempranas aumentan la probabilidad de que una amenaza pueda mitigarse o reducirse.

Una vez que se haya resuelto o mitigado un problema, considere la posibilidad de organizar una sesión informativa para que las partes apropiadas discutan el problema, los pasos que se tomaron para mitigarlo y las áreas de mejora. Esto ayuda a reforzar una cultura de compromiso y conciencia y permite que todo el equipo esté mejor preparado en el futuro.

## RECURSOS ADICIONALES

### Mitigación de Amenazas Internas

- CERT Insider Threat Center en el Software Engineering Institute de Carnegie Mellon: ofrece productos escritos para la mitigación de amenazas internas en una variedad de entornos organizacionales.
- I Recursos de mitigación de amenazas internas | CISA: comparte una guía general para ayudar a las personas, organizaciones y comunidades a comprender las amenazas internas y mejorar o establecer un programa de mitigación de amenazas internas.
- Guía de mitigación de amenazas internas | CISA: proporciona una guía integral para organizaciones de todos los tamaños en apoyo del establecimiento o mejora de un programa de mitigación de amenazas internas. La información de la guía es escalable y permite considerar el nivel de madurez y el tamaño de la organización.
- Autoevaluación de riesgos internos | CISA: una herramienta para ayudar a los propietarios y operadores u organizaciones, especialmente las pequeñas y medianas que pueden no tener departamentos de seguridad internos, a medir su vulnerabilidad ante un incidente de amenaza interna. La herramienta es un PDF descargable que hace a los usuarios preguntas clave sobre su empresa actual, centrándose en los dominios de gestión de programas, personal y formación, y recopilación y análisis de datos.
- National Insider Threat Task Force (NITTF): ayuda a los departamentos y agencias federales a identificar las mejores prácticas para detectar, disuadir y mitigar las amenazas emergentes. NITTF también proporciona una variedad de productos y recursos aplicables a entidades estatales, locales, tribales, territoriales y de infraestructura crítica.
- Amenaza interna del FBI: una introducción a la detección y disuasión de un espía interno: una introducción para gerentes y personal de seguridad sobre indicadores de comportamiento, señales de advertencia y formas de detectar y disuadir a los internos de comprometer los secretos comerciales organizacionales y los datos confidenciales de manera más efectiva.

### Información errónea, desinformación e información maliciosa (MDM)

- Biblioteca de recursos de MDM: El equipo de información errónea, desinformada y maliciosa (MDM) de CISA se encarga de desarrollar la resiliencia nacional a las actividades de influencia extranjera y MDM. A través de estos esfuerzos, CISA ayuda al pueblo estadounidense a comprender el alcance y la escala de las actividades de MDM dirigidas a las elecciones y la infraestructura crítica y les permite tomar medidas para mitigar los riesgos asociados.

### Ciberseguridad para Infraestructuras Críticas

- Marco para Mejorar la Ciberseguridad de Infraestructuras Críticas | NIST: proporciona un marco y un camino a seguir para que las partes interesadas de la infraestructura crítica evalúen los riesgos de ciberseguridad, mejoren la gestión de riesgos y prioricen y alcancen los objetivos de ciberseguridad.
- Prácticas de gestión de riesgos de la cadena de suministro para organizaciones y sistemas de información federales | NIST: amplía la guía de gestión de riesgos de seguridad cibernética al profundizar en los riesgos de la cadena de suministro de tecnología de la información y las comunicaciones (TIC) y cómo identificarlos, evaluarlos y mitigarlos.

### Cadena de Custodia

- Cadena de Custodia y Sistemas de Infraestructura Crítica | CISA: descripción general de lo que es la cadena de custodia, los posibles impactos y riesgos de una cadena de custodia rota, y un marco inicial para asegurar los activos físicos y digitales para quienes trabajan en sistemas de infraestructura crítica.
- Mejores Prácticas de Cadena de Custodia | EAC: Mejores prácticas en prácticas de cadena de custodia específicamente para funcionarios electorales.
- Cadena de Custodia – Terminología General y Modelos: Guía de la Organización Internacional de Normalización (ISO 22095:2020) sobre procesos de cadena de custodia.

### Realización de Auditorías Internas

- Aspectos Únicos de la Auditoría Interna en el Sector Público | IIA: esta guía permitirá a los auditores internos planificar y realizar trabajos de auditoría interna con una comprensión de los roles y principios únicos de las organizaciones del sector público.
- Evaluación de la Gobernanza Organizacional en el Sector Público | IIA: Descripción general de cómo los auditores internos pueden evaluar y hacer recomendaciones apropiadas para mejorar las actividades y procesos de gobierno para las organizaciones del sector público.
- Creación de un Proceso de Competencia de Auditoría Interna para el Sector Público | IIA: esta guía ayuda a garantizar que la función de auditoría de una organización tenga el conocimiento colectivo, las habilidades y otras competencias necesarias para completar las auditorías planificadas.

### Adquisición de tecnología electoral

- Una guía para garantizar la seguridad en las adquisiciones de tecnología electoral | CIS: una guía sobre la adquisición de hardware, software y servicios informáticos para la administración electoral.
- Gestión de los riesgos de la cadena de suministro de ciberseguridad en la tecnología electoral | CIS: Esta guía para proveedores de tecnología electoral proporciona las mejores prácticas para áreas problemáticas específicas identificadas por la comunidad electoral.