Elecciones Federales en EE. UU. 2024: La Amenaza Interna

La Oficina Federal de Investigaciones (FBI, por sus siglas en inglés), en coordinación con la Oficina de Inteligencia y Análisis (I&A, por sus siglas en inglés) del Departamento de Seguridad Nacional (DHS, por sus siglas en inglés), la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA, por sus siglas en inglés)) y la Comisión de Asistencia Electoral de EE.UU. (EAC, por sus siglas en inglés) preparó este resumen general con el fin de ayudar a las partes interesadas a defenderse contra amenazas internas que pudieran materializarse durante el ciclo electoral de 2024. Por años, colaboradores en el sector federal, estatal, local y privado en todo el país han trabajado en estrecha colaboración para respaldar a los funcionarios estatales y locales a proteger la infraestructura electoral contra amenazas cibernéticas, físicas e internas. Gracias a estos esfuerzos, no hay evidencia de que los actores maliciosos hayan cambiado, alterado o eliminado votos o hayan tenido algún impacto en el resultado de las elecciones. En los últimos años, la comunidad involucrada en la infraestructura electoral ha tenido múltiples experiencias donde el control al acceso al sistema electoral se ha visto comprometido debido a amenazas a nivel interno. Si bien no hay evidencia de que actores maliciosos hayan impactado los resultados electorales, es importante que las partes involucradas en las elecciones sean conscientes de los riesgos que las amenazas internas conllevan y de los pasos que se pueden tomar para identificar y mitigar dichas amenazas.

Este documento describe varios ejemplos recientes de amenazas internas a la seguridad electoral, analiza escenarios potenciales que podrían surgir durante el ciclo electoral de 2024 y proporciona recomendaciones para mitigar el riesgo que las amenazas internas representan.[1]

Amenazas internas a las elecciones

En Estados Unidos, las elecciones se administran a nivel del gobierno estatal y local, lo que ha dado lugar a un panorama diverso de sistemas y tecnologías electorales en todo el país. A lo largo del ciclo electoral, muchas personas participan en la administración o la ejecución de responsabilidades que respaldan las elecciones, incluyendo trabajadores electorales, funcionarios de otras divisiones del gobierno, proveedores, contratistas, trabajadores temporales y voluntarios. Entender lo que constituye la condición de informador y cómo los informantes con conocimiento interno de una organización pueden presentar riesgos para una organización, son componentes importantes para desarrollar un programa integral destinado a mitigar amenazas internas.

Una amenaza interna puede ser un individuo o grupo que utiliza su acceso autorizado o conocimiento especializado para causar daño a una organización o entidad. Este daño puede incluir actos maliciosos que afectan la seguridad y la integridad de la información y los sistemas electorales. Las amenazas internas pueden ser empleados actuales o antiguos, trabajadores temporales, voluntarios, contratistas o cualquier otra persona con acceso privilegiado a la información y a los sistemas electorales. Esto podría incluir personas que trabajan fuera de la oficina electoral en funciones que apoyan o interactúan con la infraestructura en la cual depende la oficina electoral.

Ejemplos recientes de amenazas internas relacionadas con la infraestructura electoral

- Un trabajador electoral temporal insertó una unidad de memoria USB personal no autorizada en un libro de votación electrónico que contenía datos de registro de votantes, e incluía información confidencial cuya divulgación está prohibida según la ley estatal. El trabajador electoral temporal extrajo los datos porque quería compararlos con los documentos que iban a recibir después de las elecciones a través de la Ley de Libertad de Información. El equipo electoral afectado fue desmantelado después de que este incidente fue identificado.

- Un Estado identificó una serie de imágenes digitales en un sistema de votación de uno de sus condados y contraseñas confidenciales conectadas con ellas que fueron publicadas en Internet sin autorización alguna. Una revisión a profundidad determinó que un secretario del condado y un empleado a su cargo, supuestamente dieron acceso a las máquinas de votación del condado a una persona no autorizada. Aparentemente, el secretario y el empleado también desactivaron las cámaras de seguridad y dieron credenciales de identificación falsas la persona no autorizada.

[1] El FBI y la CISA le piden al público reportar información sobre actividades sospechosas o delictivas a su oficina local del FBI. (www.fbi.gov/contact-us/field).

- Un funcionario del condado alertó acerca de un intento para obtener acceso no autorizado a la red electoral del condado durante las elecciones estatales primarias que tuvieron lugar en la primavera. Según el funcionario, alguien recibió acceso a una oficina gubernamental donde pudo conectar una computadora portátil no autorizada a una red gubernamental. Los datos de esa red electoral aparecieron más tarde en una reunión pública en la que se discutían temas percibidos como fraude electoral.

- Dos funcionarios del condado permitieron a usuarios no autorizados acceder a sus sistemas electorales durante un proceso de auditoría, lo que provocó que el director electoral del estado descertificara las máquinas y prohibiera su uso en futuras elecciones.

Explotación potencial de amenazas internas por parte de adversarios extranjeros

Hasta la fecha, los ejemplos de actividades de amenazas internas relacionadas con el proceso electoral han sido de naturaleza interna, tanto en términos de actor como de motivos. Sin embargo, al menos desde 2016, un número creciente de adversarios extranjeros han seguido monitoreando las redes electorales y han intentado influir o interferir en las elecciones gubernamentales en Estados Unidos. Si bien se estima que el peligro de que un adversario extranjero obtenga acceso a la infraestructura electoral a través de un informante con acceso privilegiado es mínimo, la idea de normalidad (o país estable) frente a la influencia o interferencia electoral podría impulsar a algunos adversarios a cruzar ciertos límites o "líneas rojas" en Estados Unidos, como atacar y explotar a personas o trabajadores electorales en Estados Unidos con el fin de interferir en las elecciones. Una manera en que esta amenaza originada en el extranjero podría manifestarse es mediante intentos de explotar el acceso interno para interferir con la infraestructura o los procesos electorales. Los adversarios extranjeros al igual que otros actores maliciosos, tales como redes criminales, podrían intentar obtener acceso interno a través de diversos métodos.

- Los adversarios pueden intentar obtener acceso interno explotando las opiniones ideológicas de un objetivo interno, proporcionando incentivos financieros o utilizando organizaciones relacionadas o presencia diplomática para establecer contacto con un individuo que ya se encuentra en una posición de confianza o que estaría dispuesto a buscar y obtener una posición a favor del actor extranjero.

- Los adversarios pueden intentar chantajear o coaccionar a un objetivo interno para aprovechar su acceso, recopilar información sobre los esfuerzos y vulnerabilidades de seguridad electoral, o dirigir al individuo para que lleve a cabo actividades maliciosas. Antes de iniciar el contacto, los adversarios extranjeros posiblemente recopilarán información acerca de dicho individuo con el fin de descubrir cualquier cosa que pudiera ser utilizar para chantajearlo o coaccionarlo. El tipo de información podría incluir deudas financieras y actividades potencialmente vergonzosas o ilegales.

En caso de que un adversario obtuviera acceso a la infraestructura electoral a través de un informante con acceso privilegiado, este podría utilizar ese acceso para interrumpir procesos y/o difundir información falsa en un intento de desacreditar el proceso electoral y socavar la confianza en las instituciones democráticas de EE. UU.

- Si un adversario obtuviera acceso a través de un informante con acceso privilegiado a los sistemas electorales en una jurisdicción en particular, dicha actividad podría exponer la información personal de los votantes, obstaculizar la capacidad de los votantes para acceder a información exacta el día de las elecciones o hacer que estos sistemas estén temporalmente inaccesibles para el público o los trabajadores electorales, situaciones que podrían retrasar, pero no impedir la votación o la presentación de resultados.

- Los adversarios también podrían emplear personal interno para que les ayuden en sus operaciones de influencia maliciosa con el fin de socavar la confianza del público estadounidense en la seguridad y la integridad del proceso electoral. Una persona con información privilegiada podría proporcionar a un adversario material para desarrollar o difundir mensajes que ponen a prueba la seguridad, los resultados o las operaciones del sistema electoral. Esto incluye la filtración coordinada de datos o la publicación de información en la que se alegue que la infraestructura electoral se ha visto comprometida por acciones de un adversario.

Posibles indicadores de actividad de amenazas internas

Los individuos en riesgo de convertirse en amenazas internas a menudo exhiben indicadores o señales de advertencia.[2] La siguiente lista a pesar de no ser exhaustiva, contiene posibles indicadores a los cuales los funcionarios electorales deben prestar atención y pedir a las autoridades que los investiguen cabalmente.

- Intentar alterar o destruir papeletas de votación, sobres de papeletas enviadas por correo, documentación administrativa o permitir que otros accedan a estos materiales sin autorización previa.
- Sin necesidad o autorización alguna, acceder a sistemas, equipos y/o instalaciones que no requieren acceder o proporcionar acceso a personal no autorizado.
- Apagar cámaras de seguridad o sistemas de control de acceso o ignorar protocolos que exigen la presencia de dos personas.
- Sin necesidad ni autorización alguna, llevar a casa material alguno así sea o no privado, a través de documentos, memorias USB, discos de computadora o correo electrónico. Copiar material innecesariamente, especialmente si es privado o confidencial.
- Acceder de forma remota a la red informática en períodos de tiempo inusuales o inesperados, fuera de las horas típicas de operación.
- Ignorar los reglamentos de la agencia para la instalación de software o hardware personal, el acceso a sitios web restringidos, las búsquedas no autorizadas o la descarga de información confidencial.
- Intimidar o amenazar a otros miembros del personal.

Proteja su organización: Creación de un programa para la mitigación de amenazas internas

Los trabajadores electorales y sus contrapartes en el sector privado emplean regularmente mecanismos diseñados para disuadir, detectar o prevenir acciones nocivas por parte del personal interno, ya sea que utilicen o no el término “amenaza interna” o hayan articulado su enfoque y manejo en un programa documentado. Desde el manejo de papeletas en grupos de dos (a menudo bipartidistas), hasta los robustos procedimientos de cadena de custodia, la presencia de observadores durante la votación y el recuento de votos, muchas de las principales prácticas electorales utilizadas por largo tiempo, han sido diseñadas con el fin de mitigar las amenazas internas. Sin embargo, las partes involucradas en la infraestructura electoral podrían beneficiarse de documentar su enfoque y establecer un programa más formal para mitigar las amenazas internas. Tales acciones pueden ayudar a identificar brechas en las prácticas actuales y orientar el enfoque más amplio de la organización para el manejo de riesgos.

La cultura organizacional también debe fortalecer el reporte proactivo de las inquietudes de los empleados y de los problemas de seguridad como componente central para proteger el entorno. A partir de esta base, un programa exitoso para la mitigación de amenazas internas debe implementar prácticas, estrategias y sistemas que limiten y rastreen el acceso a lo largo de las funciones organizacionales. Siempre y cuando reciban la supervisión necesaria para garantizar su adecuada aplicación, las medidas preventivas contra amenazas internas también ayudan a detectar amenazas mediate la implementación de sistemas y procesos electorales transparentes y auditables y la identificación de valores atípicos o fuera de rango para su investigación. Los elementos clave de los programas de mitigación de amenazas internas a la infraestructura electoral incluyen:

- **Procedimientos Operativos Estándar (**SOP, por sus siglas en inglés) describen la serie de pasos o requisitos para completar una tarea. Algunos ejemplos pueden incluir la necesidad de señales visuales para identificar al personal autorizado en áreas específicas o exigir el "sistema de compañeros" o un mínimo de dos personas para manejar tareas delicadas. Las listas de verificación son herramientas útiles para promover el cumplimiento de los SOP.

- **Sistemas de Control de Acceso Físico y Digital** pueden detectar y prevenir amenazas internas. Los sistemas de control de acceso deben aplicar el principio de privilegio mínimo, dando a las personas acceso sólo a los sistemas necesarios para realizar sus funciones esenciales. **Los privilegios de acceso pueden cambiar a medida que se acerca una elección u otras fechas clave.** Los controles de acceso físico pueden incluir limitar el acceso a instalaciones, equipos, dispositivos, sellos y bolsas a prueba de manipulaciones y otros activos, además de proporcionar vigilancia de activos físicos en video. Los controles de acceso digital otorgan acceso solo a los sistemas, activos, datos o aplicaciones necesarios relacionados con el trabajo o función de un individuo.
  En ambos casos, los registros de acceso, los formularios de control y los videos de vigilancia proporcionan registros auditables para saber quién y cuándo un activo físico o digital fue accedido.

[2] (U) La amenaza interna: una introducción a la detección y disuasión de un espía interno | FBI | 21 de mayo de 2016 | https://www.fbi.gov/file-repositorio/folleto_de_amenazas_internas.pdf/view

En general, los sistemas de control de acceso impiden que un individuo acceda a todos los activos dentro de una organización y reducen el daño potencial a los sistemas físicos o digitales. En caso de que se sospeche un incidente, los registros de acceso y los formularios de control pueden ayudar con las investigaciones posteriores al incidente e incluso servir como evidencia.

Un desafío clave en torno al control de acceso para los trabajadores electorales es el acceso al sistema de base de datos de registro de votantes estatal. Es posible que el estado no siempre 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 periódicamente una lista de usuarios autorizados y privilegios asociados.

- **Procedimientos de Cadena de Custodia** rastrean el movimiento y el control de activos físicos y digitales documentando cada vez que se usa o transfiere un activo y la persona responsable del mismo. Esto puede ayudar a prevenir el acceso no autorizado a sistemas confidenciales, detectar la presencia de una amenaza interna, proporcionar evidencia y mejorar el tiempo de remediación si ocurre un incidente. También genera un registro auditable de las transferencias y transacciones de un activo, lo que permite detectar una amenaza potencial si hubiera una brecha en la cadena.
- **Enfoque de Seguridad de Confianza Nula** se basa en el principio de "verificar siempre". En vez de asumir que todo lo que sucede en las redes y sistemas de una organización es seguro, el enfoque de confianza nula supone que se ha producido o se producirá una infracción y verifica cada solicitud como si no estuviera autorizada. Un enfoque de confianza nula verifica explícitamente cada solicitud de acceso, independientemente de dónde se origina o a qué recurso accede. Muchos sistemas digitales ahora incluyen funciones de seguridad de confianza nula que se pueden activar, como exigir siempre a los usuarios que ingresen su contraseña en lugar de almacenarla en la memoria del dispositivo. Las partes involucradas en la infraestructura electoral también pueden considerar implementar protocolos como la “regla de dos personas” (exigir que al menos un observador esté presente) o trabajar en equipos bipartidistas cuando se accedan recursos confidenciales.
- **Monitoreo Continuo** es una práctica clave para detectar comportamientos anómalos, incluyendo posibles amenazas internas. Involucra una combinación de herramientas humanas y digitales, como registros de acceso, videovigilancia, detección de terminales y software de respuesta, respaldados por una cultura organizacional sólida que promueve el reporte proactivo.
- **Auditoría** de todos los procesos electorales y comerciales debe ser una constante en el manejo electoral antes, durante y después de una elección. Las auditorías validan si medidas tales como el control de acceso y la cadena de custodia funcionan correctamente, recopilan y mantienen los datos necesarios y si son utilizadas adecuadamente por parte del personal. También dan la oportunidad de revisar registros (registros de acceso, imágenes de seguridad, formularios de cadena de custodia, etc.) e identificar posibles brechas o áreas para su mejoramiento. Se recomienda incorporar auditorías en los SOP de una organización.
- **Adherencia a las Mejores Prácticas en Ciberseguridad** para sistemas y redes para implementar un enfoque de defensa en profundidad que evite que puntos únicos de falla sean suficientes para comprometer el sistema. Estas mejores prácticas de seguridad también están diseñadas con la expectativa de que un actor malicioso ya haya obtenido acceso a un sistema o software similar para intentar identificar vulnerabilidades. Las mejores prácticas de ciberseguridad, como la autenticación multifactorial, la aplicación de parches y actualizaciones, y la segmentación de la red, ayudan a minimizar el posible impacto en la seguridad si ocurriera un incidente, como una amenaza interna.
- **Reporte** de todos los incidentes a las autoridades correspondientes para que puedan ser investigados y documentados puede prevenir o reducir la probabilidad de que ocurran incidentes similares en el futuro.

Establecer y mantener los procedimientos operativos estándar necesarios, los controles de acceso, la seguridad de confianza nula y los procedimientos de cadena de custodia son facetas necesarias de la administración electoral. Además, deben ser revisados, comprobados y auditados antes, durante y después de las elecciones. En conjunto, estas medidas respaldan la integridad, confiabilidad y seguridad de una elección, proporcionando evidencia para generar confianza pública en el proceso.

Para ayudar a las partes involucradas en sus esfuerzos para la mitigación de amenazas internas, CISA desarrolló un "Formulario para el reporte de amenazas internas" y un "Formulario para la investigación de amenazas internas" como herramientas que las organizaciones pueden descargar, revisar e incorporar en sus programas de mitigación de amenazas internas. Estos formularios y la "Guía del usuario del formulario para el reporte de amenazas internas" son anexos de esta guía y se pueden encontrar en el sitio web de CISA #PROTEGE2024 con sus vínculos listados a continuación.

Recursos y contactos adicionales de seguridad electoral

El FBI y CISA alientan al público a reportar información sobre actividades sospechosas o criminales a su oficina local del FBI. (www.fbi.gov/contact-us/field).

Para obtener asistencia adicional, mejores prácticas y términos comunes, visite los siguientes sitios web:

- Protected Voices - FBI
- #Protect2024 - CISA
- Election Security – U.S. Election Assistance Commission (eac.gov)
- Election Security - Dept of Homeland Security
- Election Crimes and Security — FBI

Formulario para Reporte de Amenazas Internas

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) creó estos formularios como una herramienta para que las organizaciones interesadas las descarguen, revisen e incorporen en sus programas de mitigación de amenazas internas. El ***Formulario para Reporte*** y el ***Formulario para investigación*** son archivos PDF en blanco que se pueden utilizar con cualquier programa para amenazas internas. Al igual que otros formularios desarrollados por CISA, las partes interesadas pueden utilizarlos en su formato actual o utilizarlos como ejemplo para desarrollar sus propios productos internos.

El ***Formulario para Reporte*** permite a las personas presentar inquietudes relacionadas con una posible amenaza interna al punto de contacto apropiado dentro de su organización. Este formulario incluye un botón de "enviar" que las organizaciones pueden editar para generar automáticamente un correo electrónico a la dirección postal adecuada dentro de la organización. Una organización que desee utilizar el formulario de informes deberá editar el botón "enviar" como se describe en este documento antes de que el formulario esté disponible para uso de los empleados. Esto ayuda a garantizar que todos los informes sean recopilados de forma centralizada por los destinatarios o la bandeja de entrada seleccionados adecuados.

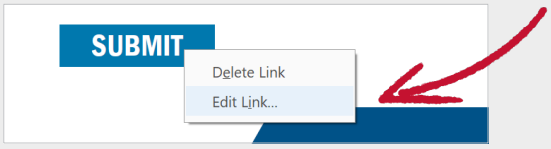
El ***Formulario para investigación*** está diseñado para ayudar a las organizaciones a documentar incidentes y determinar los próximos pasos apropiados, incluidos, entre otros, la revisión por parte del equipo de gestión de amenazas de una organización, la derivación a las autoridades policiales u otras acciones de seguimiento necesarias para proteger a la organización y a sus empleados. Esto ayudará a las partes interesadas a mantener un registro de las acciones organizacionales relacionadas con un incidente de amenaza interna, promover la responsabilidad de los pasos necesarios para proteger los activos e identificar vulnerabilidades en el esfuerzo de mitigar futuras amenazas internas.

Los formularios se pueden descargar y los datos recopilados están controlados y gestionados por las políticas y protocolos de las organizaciones interesadas.

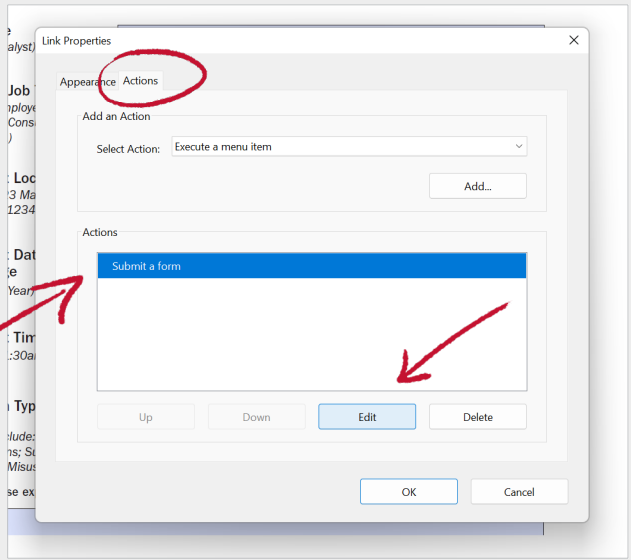
Si le preocupa una amenaza inmediata en el lugar de trabajo, comuníquese con la policía local. *Las plantillas de informes e investigación no pretenden otorgar a ninguna organización la autoridad para realizar actividades que de otro modo no podrían realizar según las leyes, regulaciones y políticas aplicables. Consulte con su asesor legal antes de implementar estos formularios en su organización.*

EDITE EL FORMULARIO PARA REPORTE ESPECÍFICAMENTE PARA SU ORGANIZACIÓN:

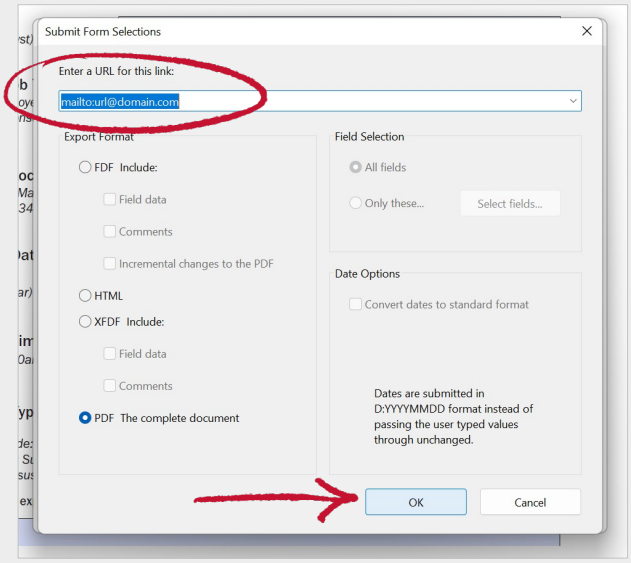
1. Haga clic derecho en el botón *SUBMIT* y haga clic en "*Edit Link...* "



2. Navegue a la pestaña "*Actions*" y edite la acción de "*Submit a form*" para enviar un formulario



3. Edite el "*Mailto*: url@domain.com" con la dirección de correo electrónico que desee y haga clic en *Ok* para aceptar



Formulario para Reporte de Amenazas Internas
REPORTE EN SU SITIO DE TRABAJO

Las plantillas de informes e investigación no pretenden otorgar a ninguna organización la autoridad para realizar actividades que de otro modo no podrían realizar según las leyes, regulaciones y políticas aplicables. Consulte con su asesor legal antes de implementar estos formularios en su organización.

Utilice esta sección para informar cualquier actividad sospechosa en el lugar de trabajo, centrándose en documentar el incidente y proporcionar detalles relevantes sobre el comportamiento/incidente observado:

1 Descripción del incidente

Proporcione tantos detalles como pueda sobre el incidente y sus observaciones.

2 Ubicación del incidente

Ejemplo: 123 Main Street, Anytown, ST 12345

3 Fecha del incidente o rango:

4 Hora(s) del incidente

Ejemplo: 11:30 a.m.

5 Tipo de preocupación

Los ejemplos incluyen: amenazas verbales/escritas; terrorismo/extremismo violento; Conducta personal; Situaciones financieras; Abuso de sustancias; Situaciones de Comportamiento; Conducta criminal; Manejo inadecuado de la información protegida; Mal uso de la tecnología de la información; Delitos Cibernéticos; Espionaje; Robo de propiedad financiera/intelectual; Violencia en el trabajo

Comparta detalles sobre las personas asociadas con la actividad sospechosa en la siguiente sección:

6 Nombre (o descripción si se desconoce)

Ejemplo: John Doe

7 Título profesional

Ejemplo: analista, representante de ventas, ingeniero de software

8 Función o tipo de trabajo

Ejemplo: Empleado, Contratista, Consultor, Proveedor, etc.

Esta plantilla de informes está destinada a documentar actividades y comportamientos sospechosos o que indican actividad delictiva. Tales actividades o comportamientos deben denunciarse sólo cuando existan hechos articulables que respalden una conclusión racional de que el comportamiento es sospechoso o sugiere una actividad delictiva. No informe basándose en actividades protegidas constitucionalmente o por motivos de raza, etnia, religión, género, orientación sexual, discapacidad u otras características similares, y no informe basándose únicamente en una combinación de dichos factores. ***Si le preocupa una amenaza inmediata en el lugar de trabajo, comuníquese con la policía local.***

ENVIAR

Plantilla de informe de amenazas internas

NUMERO DE REPORTE

Las plantillas de informes e investigación no pretenden otorgar a ninguna organización la autoridad para realizar actividades que de otro modo no podrían realizar según las leyes, regulaciones y políticas aplicables. Consulte con su asesor legal antes de implementar estos formularios en su organización.

DETALLES DEL INCIDENTE

1 **Descripción del incidente** *Explique el incidente detalladamente (p.ej., declaración de un testigo, etc.). ¿Qué sistemas de TI se vieron comprometidos? ¿Qué tecnología identificó la infracción (si aplica)*

2 **Tipo de inquietud** *Los ejemplos incluyen: amenazas verbales/escritas; terrorismo/extremismo violento; Conducta personal; Consideraciones financieras; Abuso de sustancias; Consideraciones de Comportamiento; Conducta criminal; Manejo inadecuado de la información protegida; Mal uso de la tecnología de la información; Espionaje; Robo de propiedad financiera/intelectual;Otro*

3 **¿Se ha notificado al profesional de seguridad adecuado?** ◯ *Sí* ◯ *No* ◯ *N / A*

4 **¿Se ha notificado al equipo de manejo de amenazas internas?** ◯ *Sí* ◯ *No* ◯ *N / A*

INFORMACIÓN SOBRE LA PERSONA DE INTERÉS

5	Nombre	
6	Título profesional	
7	Categoría Laboral	
8	Nivel de autorización/Acceso especial	
9	Privilegios de red	
10	Equipo utilizado en el incidente	
11	Localización de la oficina	
12	Fecha del incidente o rango de fechas	
13	Hora(s) del incidente	

INFORMACIÓN DEL INVESTIGADOR/OFICIAL DE ADMISIÓN

14	Nombre	
15	Información del contacto	
16	Posición	

INFORMACIÓN ADICIONAL

17 **Recomendaciones iniciales** *¿Es necesario involucrar a las autoridades? ¿Qué medidas deben tomarse para mantener a las personas seguras?*

18 **¿Cómo se detectó la actividad sospechosa?** *¿Qué actividad ocurrió? ¿Cuál fue la principal motivación del individuo (si se conoce)? ¿Se violó alguna política organizacional? ¿Cómo se eludieron las políticas/procedimientos de seguridad, si fue posible? ¿Qué medidas tomó la organización para mitigar y prevenir un incidente?*

19 **Siguientes pasos, rastreo y conclusión** *¿Qué acciones tomó la organización? ¿Se recomendaron consecuencias para el individuo a RR.HH., como una advertencia formal, sugerencia de asesoramiento o despido? ¿Se envió el asunto a las autoridades para una mayor investigación? ¿Se realizaron entrevistas a los testigos? ¿Qué acción debe seguirse a continuación en este caso particular?*

20 **Recomendaciones/Actualizaciones/Cambios** *¿Qué cambios en seguridad debería considerar la organización? ¿Qué cambios deben realizarse para proteger los activos de la organización? ¿El reporte condujo a una mitigación o prevención exitosa? En caso negativo, ¿qué brecha de seguridad es necesario analizar? ¿Es necesario un mayor seguimiento del individuo?*

INFORME REVISADO POR

Nombre

Título

Número de investigación policial (si aplica)

Oficina Investigadora (si aplica)

Fecha