PRINCIPIOS BÁSICOS SOBRE AMENAZAS DE AGENTES INTERNOS: LO QUE NECESITA SABER

DESCRIPCIÓN GENERAL

Las organizaciones de todos los tamaños son vulnerables a ser víctimas de una amenaza de agentes internos. Una amenaza de agentes internos es la posibilidad de que un agente interno utilice su acceso autorizado o conocimiento especial de una organización para dañar a dicha organización. Este daño puede incluir actos maliciosos, de exceso de confianza o no intencionales que afecten negativamente la integridad, la confidencialidad y la disponibilidad de la organización, sus datos, el personal, las instalaciones y los recursos asociados.

ELABORACIÓN DE UN PROGRAMA DE MITIGACIÓN DE AMENAZAS DE AGENTES INTERNOS

La Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA, por sus siglas en inglés) ayuda a las partes interesadas en infraestructura crítica a elaborar o ampliar sus programas de mitigación de amenazas de agentes internos. En los programas exitosos de mitigación de amenazas de agentes internos, se emplean prácticas y sistemas que limitan o monitorean el acceso a todas las funciones de la organización. Los programas de mitigación de amenazas de agentes internos deben poder detectar e identificar acciones inadecuadas o ilegales, evaluar las amenazas para determinar los niveles de riesgo e implementar soluciones para gestionar y mitigar las posibles consecuencias de un incidente de agentes internos.

Las organizaciones deben formar un equipo de gestión de amenazas multidisciplinario para crear un plan de respuesta a incidentes, de modo que se garantice que su respuesta a un incidente de agentes internos o amenaza potencial esté estandarizada, y se puede aplicar y repetir de manera consistente.

Para establecer eficazmente un programa de gestión de amenazas de agentes internos, las organizaciones deben hacer lo siguiente:

Obtener el apoyo de la dirección de la organización

Empezar con poco: aproveche las capacidades y los recursos existentes.

Definir el propósito del programa y destacar el retorno de la inversión al revelar lo que se podría perder en un incidente de amenaza de agentes internos exitoso.

Identificar lo que valora la organización y sus activos físicos e intelectuales críticos para protegerse contra amenazas de agentes internos.

Mantener las vías para denunciar

Desarrollar una cultura de responsabilidad compartida diseñada para ayudar al individuo y al posible agente interno.

Desarrollar vías de denuncia confidenciales que sean fáciles de encontrar, comprender y utilizar.

Proporcionar capacitación y concientización

Capacitar a los empleados para reconocer los indicadores de amenazas de agentes internos y los comportamientos preocupantes que podrían conducir a un incidente en la organización.

DATOS BÁSICOS SOBRE LAS AMENAZAS DE AGENTES INTERNOS

El coste medio total de un riesgo de amenaza de agentes internos aumentó en 2023 a

$16.2 millones por organización.

(tardando una media de 86 días en identificarse y contenerse)

Fuente: Ponemon 2023 Insider Threat Report, *2023 Cost of Insider Risks Global Report*

90%

de los profesionales de la ciberseguridad consideran que sus organizaciones son vulnerables a ser víctimas de amenazas de agentes internos

Fuente: Crowd Research Partners, *Insider Threat 2018 Report.*

$121 mil millones

fue el costo anual estimado a nivel nacional de la violencia en el lugar de trabajo en 2021

Fuente: National Safety Council, Workplace Violence, *A Universal Threat, 2022*

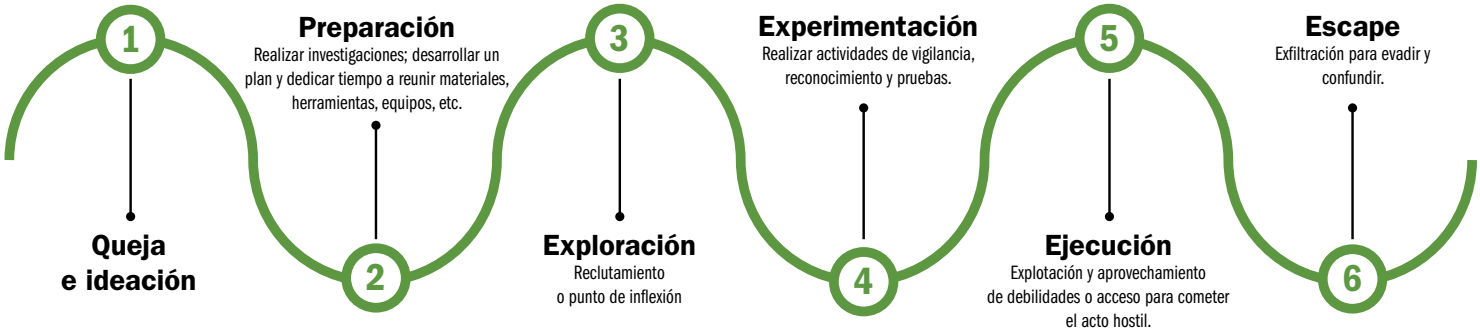
25%

de la violencia en el lugar de trabajo no se denuncia

Fuente: AlertFind, *Workplace Violence Statistics 2018*

PROGRESIÓN DE UNA AMENAZA DE AGENTES INTERNOS HACIA UN INCIDENTE MALICIOSO

La actividad maliciosa de un agente interno rara vez es espontánea; generalmente es el resultado de una decisión deliberada de actuar. Una posible amenaza de agentes internos progresa a lo largo de una vía identificable hasta convertirse en un incidente malicioso.[1] Un agravio o una humillación profundamente arraigados, ya sean reales o percibidos, suelen ser el primer paso en el proceso hacia la violencia intencional.[2]



> Todos forman parte del equipo de amenaza de agentes internos, no solo la policía o el personal de seguridad. "Es responsabilidad de todos mantener segura la agencia y la misión".
>
> – EXPERTO EN ASUNTOS GUBERNAMENTALES
> (DE UN "STRATEGIC PLAN TO LEVERAGE THE SOCIAL & BEHAVIORAL SCIENCES TO COUNTER THE INSIDER THREAT," PERSEREC OPA-2018-082)

RECURSOS ADICIONALES

Obtenga más información sobre las amenazas de agentes internos con algunos de nuestros otros recursos a continuación.

GUÍA DE MITIGACIÓN DE AMENAZAS DE AGENTES INTERNOS

EVALUACIÓN DEL PROGRAMA DE MITIGACIÓN DE RIESGOS DE AGENTES INTERNOS

LA FUNCIÓN DEL DEPARTAMENTO DE RECURSOS HUMANOS EN LA PREVENCIÓN DE AMENAZAS DE AGENTES INTERNOS

TALLER SOBRE MITIGACIÓN DE AMENAZAS DE AGENTES INTERNOS

Para obtener asistencia regional directa, visite cisa.gov/about/regions.

Para obtener recursos adicionales sobre amenazas de agentes internos y otros productos e información sobre seguridad de infraestructura, visite cisa.gov/insider-threat-mitigation.

1. Federal Bureau of Investigation Behavioral Analysis Unit. (2015). Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks. (p. 24). U.S. Department of Justice, Federal Bureau of Investigation. Washington, DC. Consultado en fbi.gov/file-repository/making-prevention-a-reality.pdf/view.
2. El término "queja" tal como se utiliza aquí se debe distinguir de la presentación formal de una queja por parte de un empleado basada en casos de discriminación u otra conducta inapropiada en el lugar de trabajo dirigida contra él. La presentación de una queja formal no se debe interpretar como indicativa de una amenaza de agentes internos.