GUÍA PRÁCTICA DE LA OACI SOBRE AMENAZAS INTERNAS

GENERALIDADES

Esta guía práctica, creada por la OACI en colaboración con el Grupo de Trabajo sobre Instrucción del Grupo Experto en Seguridad de la Aviación, está diseñada para ayudar a las organizaciones que actúan en el ámbito de la aviación a reaccionar mejor ante la amenaza interna, que está en constante evolución. Como se señala en la *Declaración del contexto mundial de riesgo para la seguridad de la aviación* de la OACI (Doc 10108 - Distribución limitada), el terrorismo busca sistemáticamente explotar las vulnerabilidades de los controles de seguridad y cometer actos de interferencia ilícita (AUI) contra la aviación, lo cual se facilitaría si se aprovecharan los conocimientos de personas con acceso a información privilegiada, es decir los elementos internos.

¿Quiénes son los elementos internos?

Los elementos internos son el personal a tiempo completo o parcial (que incluye a contratistas, personal temporal y personal autónomo) que trabaja en el sector de la aviación o para ese sector, y cuya función les proporciona acceso privilegiado a lugares u objetos protegidos, o a información sensible en materia de seguridad, o bien a conocimientos acerca de ellos.

¿Qué es la amenaza interna?

La amenaza interna se refiere al riesgo que plantea la posibilidad de que el personal de aviación cometa o facilite un acto de interferencia ilícita mediante el uso de su acceso autorizado, lo que le daría una ventaja táctica.

¿Qué motiva a los elementos internos?

Los elementos internos pueden cometer o facilitar un acto de interferencia ilícita por falta de conocimiento, por complacencia o por malicia. La falta de conocimiento de políticas y procedimientos y la complacencia (entendida como una actitud laxa respecto de las políticas y procedimientos) pueden hacer que estas personas con información privilegiada faciliten involuntariamente un acto de interferencia ilícita por su negligencia, inacción o incumplimiento de las políticas y procedimientos de seguridad.

Por otro lado, los elementos internos maliciosos -aquellos que toman la decisión consciente de llevar a cabo un acto de interferencia ilícita- pueden estar impulsados por una mezcla de vulnerabilidades personales, acontecimientos vitales y factores

situacionales, como el beneficio económico, la ideología, la venganza, el deseo de reconocimiento o la coerción.

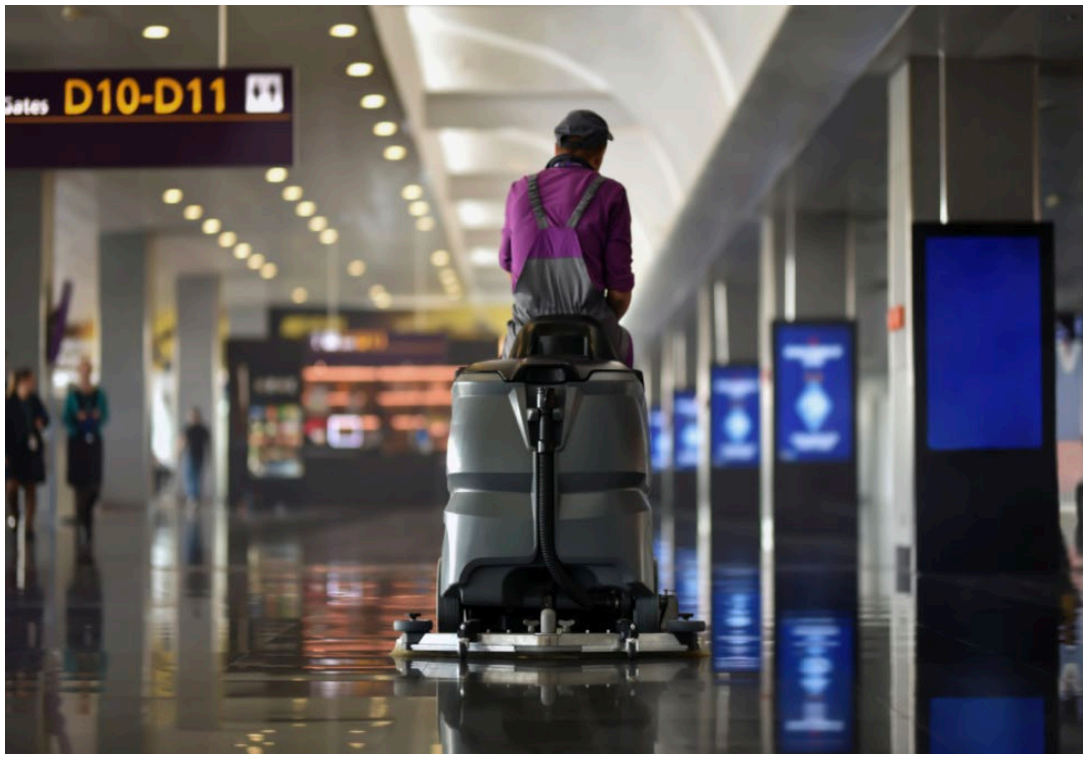
Una persona malintencionada podría infiltrarse en una organización para cometer un AUI o bien la intención de cometerlo podría surgir durante su empleo (por ejemplo, que un tercero la reclute para aprovecharse de su condición de personal de confianza).

¿Cómo pueden actuar los elementos internos?

Estas personas pueden cometer cualquier acto de interferencia ilícita (por ejemplo, la destrucción de una aeronave en servicio, la introducción de un arma o un dispositivo o material peligroso con fines delictivos a bordo de una aeronave o en un aeropuerto). Los elementos internos pueden compartir información confidencial; facilitar el acceso a zonas restringidas; desempeñar sus funciones de forma inadecuada, permitiendo la introducción de artículos prohibidos en zonas restringidas; ayudar a personas externas a obtener acceso a sistemas informáticos u otras infraestructuras digitales[1], etc.

MEDIDAS DE MITIGACIÓN

Las organizaciones pueden mitigar la amenaza interna mediante una serie de medidas y políticas de seguridad relativas al personal. En general, estas medidas apuntan a reducir el riesgo de contratar personal cuyas acciones puedan plantear un problema de seguridad; minimizar la probabilidad de que el personal existente se convierta en un problema de seguridad; reducir el riesgo de actividad de elementos internos; y proteger los bienes de la organización.



[1] Por infraestructura digital se entienden los equipos relacionados principalmente con las comunicaciones móviles y por internet.

Las medidas y herramientas para mitigar la amenaza interna pueden agruparse en las siguientes áreas:

VERIFICACIÓN E INVESTIGACIÓN DE ANTECEDENTES

Políticas y procedimientos: Cualquier marco destinado a mitigar la amenaza interna se basa fundamentalmente en políticas y procedimientos sólidos de verificación de antecedentes, que incluyan la comprobación de la identidad de la persona empleada, su experiencia laboral previa, sus antecedentes penales y su formación académica. Dichas políticas y procedimientos deben ser claros y concisos y deberían revisarse periódicamente.

Verificación inicial de antecedentes: Todo el personal que necesite acceder sin escolta a la parte aeronáutica y a las zonas de seguridad restringidas, así como las personas con acceso a información delicada de seguridad, deberán someterse a una verificación de antecedentes[2] según lo especifique la autoridad competente.

Las verificaciones iniciales de antecedentes deberían cubrir:

- identidad (por ejemplo, entrega de un pasaporte, documento de identidad, partida de nacimiento, etc.);
- antecedentes penales (en la medida en que lo permitan las normativas y leyes locales);
- comprobación de referencias (para verificar la ética profesional y la idoneidad general de la persona); e
- historial laboral (por ejemplo, empleadores anteriores, historial educativo, etc.)

Verificación periódica de antecedentes: Las verificaciones de antecedentes deben ser recurrentes y actualizarse periódicamente como parte de las verificaciones cíclicas de seguridad del personal. Es una buena práctica actualizar la verificación de antecedentes cada vez que haya que renovar los permisos de identificación del personal del aeropuerto.

A menudo, la intención de cometer un acto ilegal o un acto de interferencia ilícita utilizando el acceso o conocimiento de información privilegiada surge después de la contratación. Además, es posible que muchas personas con información privilegiada ya hayan llamado la atención de la dirección (por ejemplo, por faltas de disciplina y bajo rendimiento), lo que debe tenerse en cuenta durante el proceso de verificación de antecedentes recurrente.

Investigación continua: Debe fomentarse un proceso continuo de investigación, en colaboración con las autoridades competentes (y, si es pertinente, con las autoridades de otros Estados). Se trata de evaluar si la persona sigue cumpliendo con los requisitos aplicables a su puesto de trabajo.

[2] Norma 3.5.2 del Anexo 17- *Seguridad de la aviación* (12a edición, Enmienda 18)

Verificación de antecedentes reforzada: Podría ser útil recurrir a verificaciones de antecedentes que cubran aspectos de inteligencia (y cualquier otra información pertinente disponible sobre la idoneidad de una persona para trabajar en una función determinada). De hecho, los Estados pueden colaborar con las autoridades nacionales competentes para incorporar datos enriquecidos en el proceso de verificación e investigación de antecedentes por niveles.

Del mismo modo, si el personal detecta un comportamiento sospechoso o inusual en una persona, se debería contactar a las autoridades de seguridad y locales competentes, ya que podría ser necesaria una verificación de antecedentes reforzada.

INSTRUCCIÓN Y SENSIBILIZACIÓN

Instrucción de sensibilización: Debería fomentarse que todo el personal reciba instrucción de sensibilización acerca de la seguridad y la cultura de la seguridad. Esto contribuiría a que todo el personal conozca las políticas, normas, directrices y procedimientos de seguridad y comprenda por qué es importante cumplirlas para mantener un alto nivel de seguridad. Esta instrucción también permitiría que el personal nuevo adquiera la capacidad de identificar y denunciar sin temor cualquier comportamiento sospechoso a la autoridad competente o a las fuerzas de seguridad, incluso de forma anónima.

Integración de la instrucción: La sensibilización en materia de seguridad podría integrarse en la instrucción inicial y recurrente existente o mediante el uso de material de campañas, talleres, sesiones libres (sin necesidad de inscripción previa), etc. para promover una cultura de la seguridad sólida y efectiva en la aviación.

Instrucción específica para cada función: En el caso de determinadas categorías de personal, como supervisoras y supervisores, personal de la administración y personal con responsabilidades relativas a la seguridad del personal, convendrá impartir una instrucción más exhaustiva y específica para cada función, adaptada a los resultados esperados en cada caso.

Campañas de sensibilización: Deberían diseñarse mensajes visuales que cubran aspectos clave de la seguridad para exhibirlos en las organizaciones y en los aeropuertos de modo que sirvan de recordatorio visual al personal.

MEDIDAS DE CONTROL DEL ACCESO

Inspección: Deberían establecerse medidas de control de acceso para tener la certeza de que las personas que no sean pasajeras o pasajeros y los objetos que lleven consigo sean inspeccionados antes de que se les permita ingresar en las zonas de seguridad restringidas del aeropuerto[3]. La inspección debería incorporar algunos métodos aleatorios e imprevisibles para compensar el hecho de que dichas personas tienen conocimiento de información privilegiada, de modo de reducir así la probabilidad de que se introduzcan artículos prohibidos en la parte aeronáutica, incluso cuando quienes los transporten sean miembros del personal.

Políticas y procedimientos: Las políticas y procedimientos deben ser claros e incluir lo siguiente:

- desactivar las tarjetas de identificación del personal que se haya desvinculado de la organización (por ejemplo, por renuncia, jubilación, etc.);
- limitar los derechos de acceso a las zonas restringidas de personas titulares de pases en función de estrictas necesidades operacionales;
- proteger adecuadamente el perímetro y los puntos de control del acceso para evitar que el personal eluda las inspecciones de seguridad; y
- aplicar protocolos de supervisión y ampliar el uso del circuito cerrado de televisión (CCTV) en las actividades operativas, cuando corresponda.

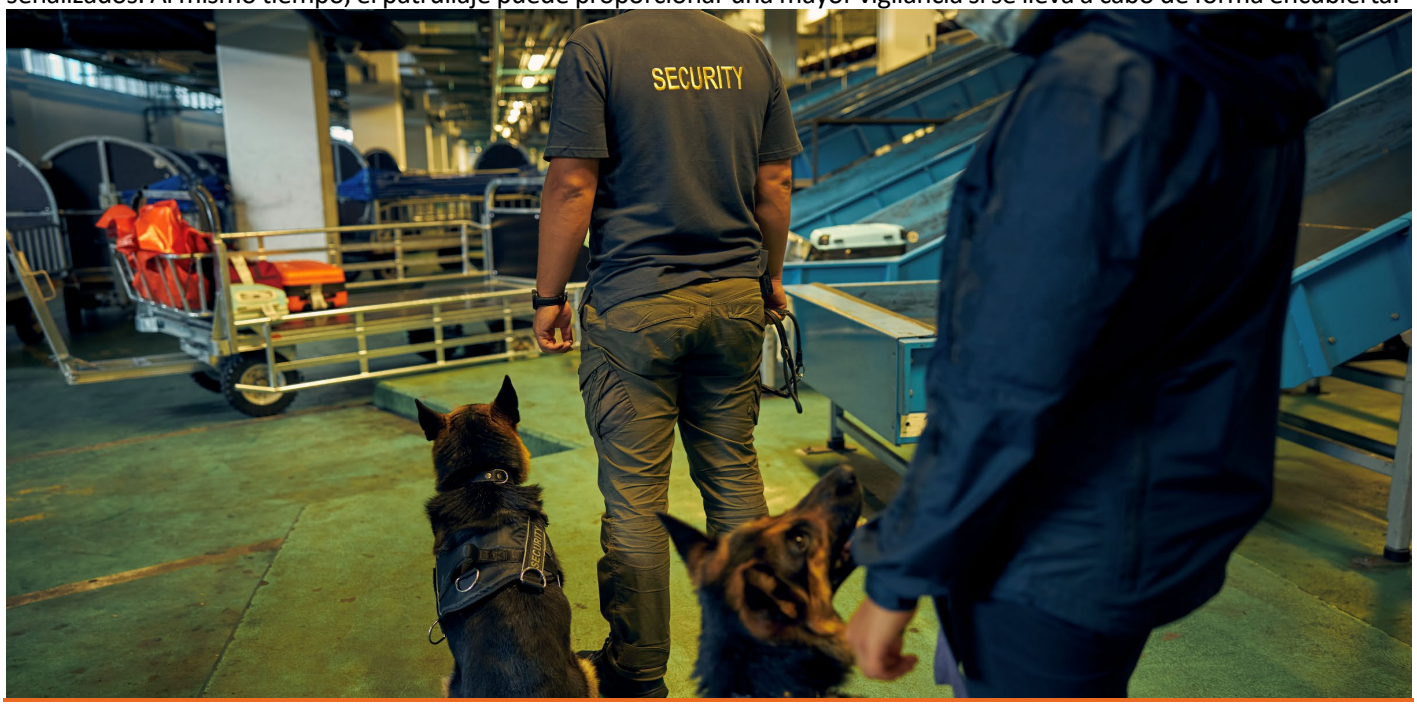
[3] Norma 4.2.5 del Anexo 17- *Seguridad de la aviación* (12a edición, Enmienda 18)

Revisar las listas de acceso: Se recomienda revisar los procedimientos de expedición de permisos de identificación del personal del aeropuerto para cerciorarse de que quien solicite el acceso a una zona determinada tenga necesidad de ingresar en ella por motivos estrictamente operacionales.

PATRULLAJE

Aleatorio e imprevisible: El patrullaje debería realizarse de forma aleatoria e imprevisible (por ejemplo, mediante controles puntuales), de modo que las patrullas no puedan evitarse ni eludirse como resultado del reconocimiento que puedan haber llevado a cabo grupos hostiles o de información proporcionada por elementos internos. Además, el patrullaje no debería centrarse únicamente en la vigilancia del personal del aeropuerto, sino que debería incluir también a pasajeros y pasajeras, otros sectores de interés del aeropuerto y la infraestructura y bienes aeroportuarios para detectar signos de actividad inusual o de seguridad deficiente.

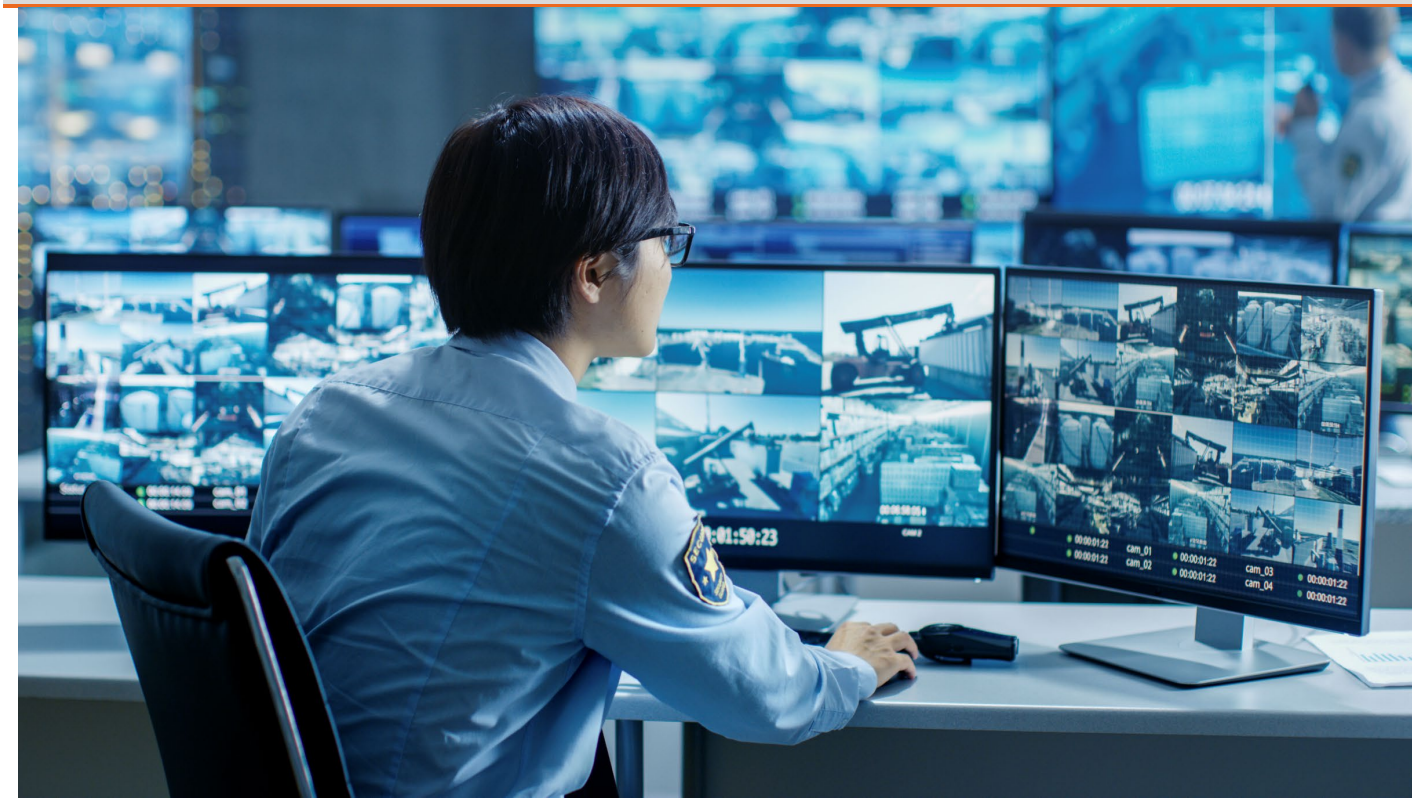
El patrullaje puede resultar eficaz como elemento disuasorio visual si el personal va uniformado y utiliza vehículos señalizados. Al mismo tiempo, el patrullaje puede proporcionar una mayor vigilancia si se lleva a cabo de forma encubierta.



VIGILANCIA Y CONTROL

Métodos: El control de calidad y la supervisión de los procesos y del personal que pueda convertirse en una amenaza interna pueden desempeñar un papel importante a la hora de evitar o afrontar rápidamente incidentes de seguridad y actos de interferencia ilícita. Entre los métodos de vigilancia, se incluyen las cámaras de CCTV, la revisión de los registros de los sistemas (por ejemplo, solicitudes de acceso) y la vigilancia por parte del personal.

El personal supervisor también desempeña un papel fundamental a la hora de reconocer y seguir de cerca cualquier actividad y comportamiento inusual del personal al que supervisa.



Datos: En algunas organizaciones, los datos del personal pueden encontrarse en varios registros de aplicaciones informáticas que registran las acciones del personal. Estos datos digitales pueden revelar los patrones de conducta en el trabajo y utilizarse como herramienta para determinar si existe alguna intención maliciosa entre el personal del aeropuerto (por ejemplo, si se revela que accede a zonas en las que no tiene necesidad de ingresar por motivos operacionales).

Entre las aplicaciones, podrían incluirse las siguientes:

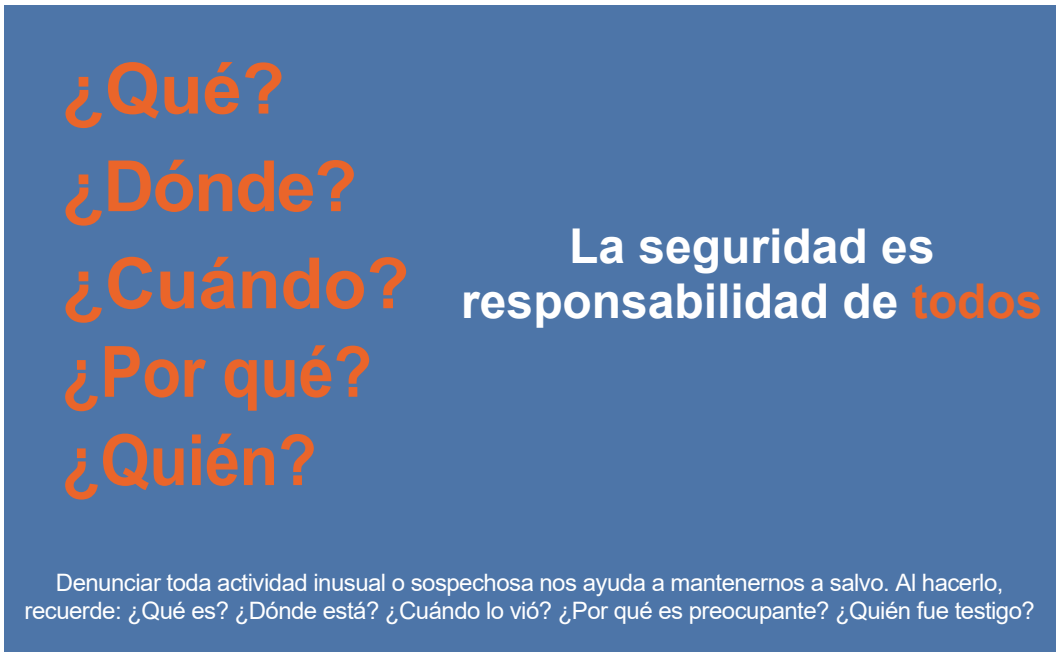
- registros físicos de entrada y salida, con especial atención al horario y acceso a los espacios físicos;
- registros digitales de entradas y salidas, con especial atención al cruzamiento entre credenciales, horarios y usuarios;
- registros de aplicaciones de correo electrónico; y
- registros de aplicaciones de bases de datos.

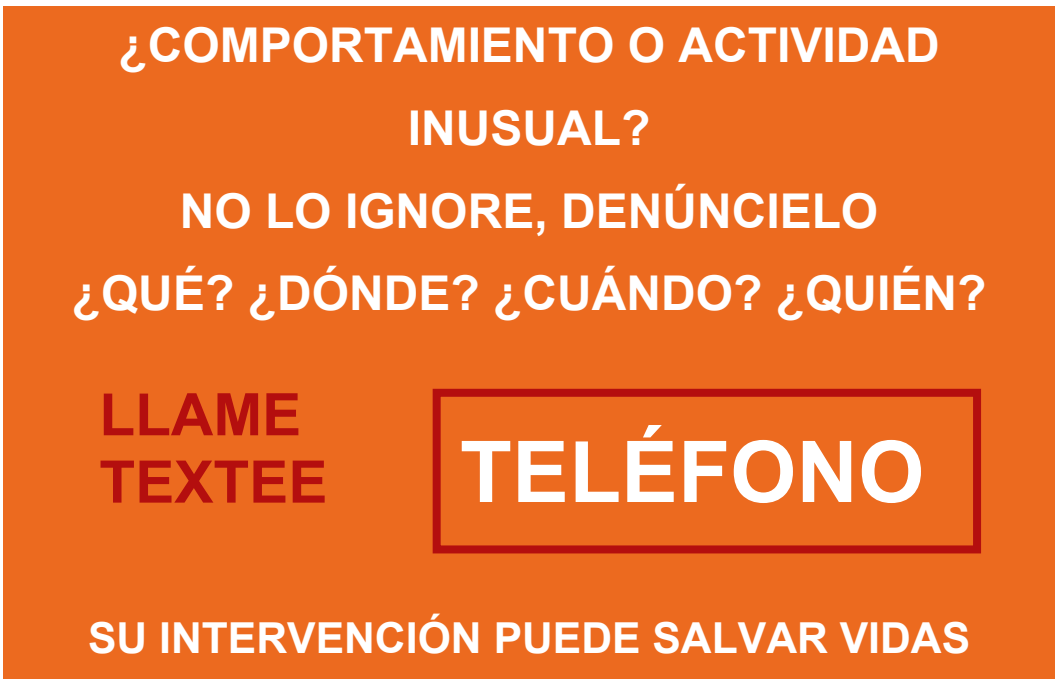
MECANISMOS DE DENUNCIA

Denuncia de comportamientos sospechosos: Los mecanismos de denuncia deberían ser accesibles a todas las personas que integran la organización, y no sólo a las que participan directamente en la seguridad. Estos mecanismos son importantes porque quienes integran el personal son los "ojos", los "oídos" y la "voz" de la organización.

Pueden establecerse mecanismos de denuncia mediante los cuales el personal pueda señalar sin temor cualquier comportamiento o incidente sospechoso por mensaje de texto, correo electrónico, llamadas telefónicas, canales internos de comunicación o en persona. Cualquier denuncia debe recibir una respuesta clara, efectiva y rápida.

Las denuncias anónimas o confidenciales pueden ser muy eficaces para mitigar posibles amenazas internas y establecer una cultura de seguridad efectiva en la organización.

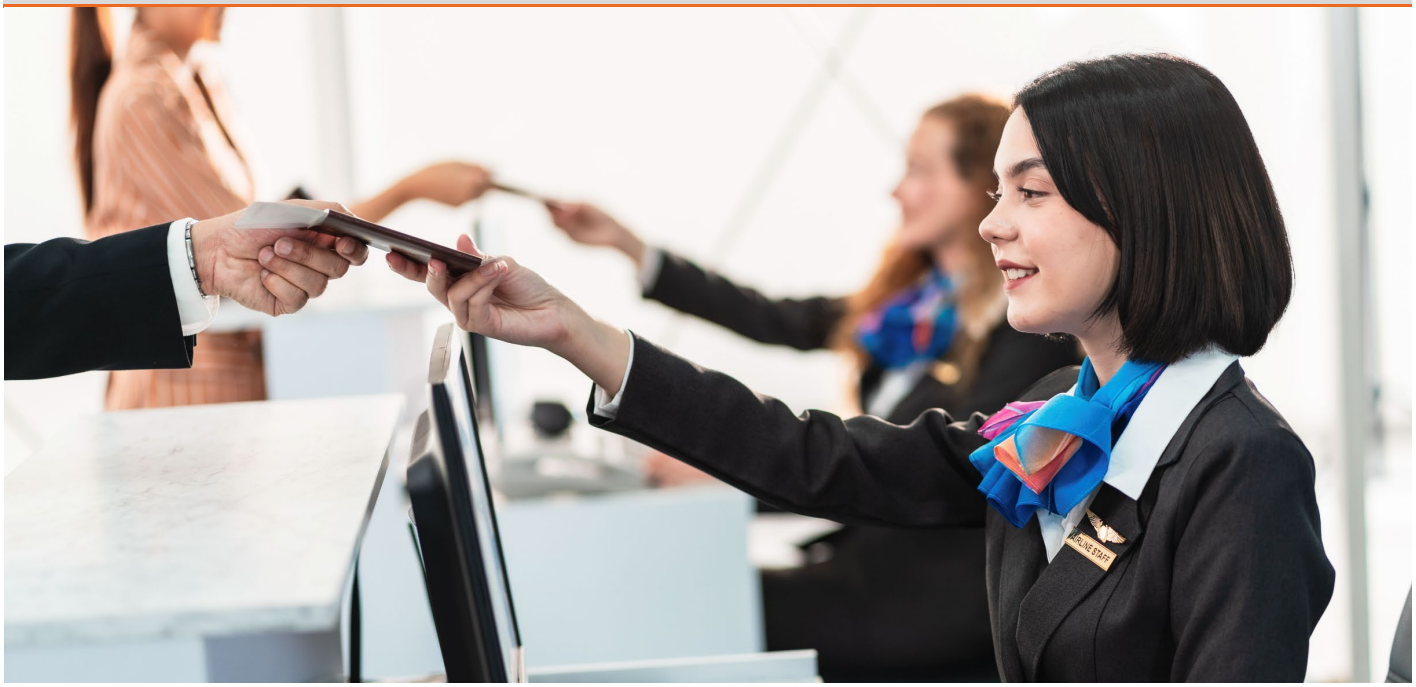




DETECCIÓN DE COMPORTAMIENTOS[4]

Detección de comportamientos: Una herramienta útil para ayudar a mitigar la amenaza interna puede ser la detección de comportamientos. Se basa en la premisa de que las personas pueden mostrar signos de comportamiento sospechoso o inusual, y que estos signos pueden ser captados por personas que hayan recibido la instrucción adecuada.

Instrucción: Capacitar al personal para que sepa reconocer una actividad sospechosa y un comportamiento inusual y cómo denunciarlo puede ser muy útil.
La instrucción en detección de comportamientos debe impartirse a una amplia variedad de personal que incluya, entre otras, a las personas encargadas de expedir pases y de realizar verificaciones de antecedentes e inspecciones. A su vez, todo el personal podría beneficiarse de este tipo de instrucción como parte de la instrucción de sensibilización sobre seguridad.



CULTURA DE LA SEGURIDAD[5]

Una cultura de seguridad sólida y efectiva: Establecer una cultura de seguridad positiva en todo el sector de la aviación es esencial para mitigar la amenaza interna y obtener resultados de seguridad efectivos y sólidos. Posibles acciones:

- se puede motivar e informar al personal acerca de los riesgos internos mediante sesiones informativas periódicas sobre amenazas y cuestiones de seguridad más generales;
- se puede instruir al personal para que sepa detectar y denunciar cualquier comportamiento anómalo o sospechoso; y
- el personal puede ser una valiosa fuente de información sobre vulnerabilidades y cómo abordarlas.

[4] La detección de comportamientos es la aplicación de técnicas que implican el reconocimiento de características comportamentales que incluyen, entre otros elementos, signos fisiológicos o gestuales indicativos de un comportamiento anómalo (una combinación de indicios verbales y no verbales) para identificar a personas que puedan tener la intención de cometer un acto de interferencia ilícita.
[5] Encontrará más información sobre este tema (incluidos los recursos pertinentes de la OACI) en el sitio web de la OACI sobre cultura de la seguridad en www.icao.int/Security/Security-Culture

LIDERAZGO Y ESTRATEGIA

Un liderazgo fuerte: Es fundamental que el personal directivo comprenda que es su papel demostrar con el ejemplo las acciones y los comportamientos positivos que espera de su personal. Debería fomentarse una comunicación franca entre el personal y el personal directivo, ya que es importante que la dirección comprenda la presión que soporta el personal en sus operaciones cotidianas, así como los riesgos internos que dichas presiones pueden suscitar.

Si quien ocupa un cargo ejecutivo (por ejemplo, de la administración superior) hace suyos los principios relativos a los riesgos de seguridad, aplica las políticas de seguridad para dar el ejemplo al personal subalterno y sirve de modelo de los comportamientos esperados, seguramente logrará promover el cumplimiento en toda la organización y contribuirá aún más a mitigar la amenaza interna.

Estrategia: Se recomienda una estrategia de mitigación de la amenaza interna (respaldada por la dirección) para ayudar a que el personal entienda cómo reconocer y denunciar cualquier comportamiento sospechoso en el lugar de trabajo.

La estrategia también puede incluir políticas, directrices y procedimientos de control de la amenaza interna relacionada con el personal. Entre esas políticas, se incluyen las medidas que deben adoptarse antes de la contratación y mientras dure el vínculo laboral. La estrategia y las políticas deberían revisarse periódicamente con todas las partes interesadas.

Los documentos marco[6], manuales y guías pueden ser herramientas útiles adicionales.

[6] Por ejemplo, www.cpni.gov.uk/insider-risks/insider-risk-mitigation-framework

FACTORES HUMANOS

Actuación humana y factores humanos: Las organizaciones deben comprender de qué manera la actuación humana puede contribuir a mitigar la amenaza interna. Esto implica también tomar conciencia de cómo los factores humanos pueden afectar a las personas, que pueden utilizar su acceso privilegiado, intencionalmente o no, para cometer un acto de interferencia ilícita. Quienes ocupan cargos ejecutivos y la alta dirección deberían:

- comprender cabalmente las capacidades humanas y cómo éstas pueden contribuir a mitigar el riesgo de la amenaza interna;
- comprender las limitaciones humanas y cómo pueden gestionarse de modo que no afecten la actuación;
- facilitar los mecanismos para que el personal notifique cualquier preocupación con respecto a la seguridad y cualquier comportamiento sospechoso;
- comprender la relación entre los factores humanos, la cultura de la seguridad y la motivación;
- asegurarse de que el personal disponga de los recursos necesarios;
- cerciorarse de que el personal de supervisión sea capaz de identificar los signos de estrés y fatiga para poder tratarlos con prontitud; y
- evitar la complacencia en las actividades cotidianas.

TECNOLOGÍAS AVANZADAS[7]

Detección de trazas de explosivos (ETD): El uso de máquinas de ETD puede añadir una capa adicional de seguridad a los procedimientos regulares de inspección de personas que no son pasajeras, conjuntamente o en reemplazo de otras medidas de seguridad aleatorias e imprevisibles empleadas en toda la zona de seguridad restringida, contribuyendo así a mitigar la amenaza interna.

[7] La aplicación de tecnologías avanzadas puede ayudar a mitigar el riesgo que supone la amenaza interna, ya que permite incrementar los niveles de detección durante el proceso de inspección de seguridad y/o añadir capas de seguridad adicionales cuando se aplican medidas en forma aleatoria e imprevisible en todo el entorno del aeropuerto.

Perros detectores de explosivos (EDD): Los equipos de EDD pueden utilizarse para muchos fines, como: control de seguridad en todas las zonas del aeropuerto (tierra, aire, pasajeros y pasajeras, personas que no son pasajeras, equipaje, carga, etc.), recorrido de seguridad de zonas restringidas y como medio para aplicar medidas de seguridad aleatorias e imprevisibles.

Inteligencia Artificial (IA): El uso de sistemas basados en inteligencia artificial por parte de personal con la instrucción necesaria puede ayudar a identificar tendencias y actividades anómalas. Por ejemplo, las soluciones modernas de gestión de incidentes pueden contribuir a identificar incidentes y diferenciar sucesos triviales de amenazas inminentes, tales como intentos de intrusión en zonas restringidas.

— FIN —