Securitas

Risk Intelligence

Ventaja en la toma de decisiones en la zona gris

Protección del sector aeroespacial y de la defensa mediante la inteligencia de riesgos

intelligence@securitas.com

Índice

Nuestro Toolkit de inteligencia 4
Metodología 6
Resumen 8
Situación 10
- Manifestaciones y disturbios 12
- Delincuencia y seguridad 16
- Seguridad corporativa 20
- Terrorismo y extremismo 24

Como lo expresa Sophie Cairney, consultora líder en Inteligencia de Riesgos del Centro de Inteligencia de Riesgos de Securitas: “La industria aeroespacial y de defensa está atrapada en el fuego cruzado de la ‘convergencia’ más que nunca. Esto incluye cómo las amenazas geopolíticas y relacionadas con los conflictos pueden impactar directa e indirectamente a las organizaciones del sector privado, así como los requerimientos de seguridad necesarios para protegerse frente a estas. Pero no todas las amenazas comienzan con una ‘explosión’; y las organizaciones que utilizan estrategias de seguridad basadas en inteligencia para identificar, evaluar y actuar en defensa de sus intereses serán las que definirán el futuro de la seguridad.”

Introducción

Sophie Cairney
Lead Risk Intelligence Consultant

El sector aeroespacial y de defensa (A&D) en 2026 y en los próximos años enfrenta un panorama de amenazas volátil, incierto, complejo y ambiguo (VUCA), marcado por tensiones geopolíticas, polarización social y el creciente uso de tácticas de zona gris tanto por actores estatales como no estatales. A medida que los conflictos persisten y la competencia estratégica se intensifica, las organizaciones de A&D están cada vez más expuestas a riesgos físicos, digitales y reputacionales convergentes, que desafían los modelos tradicionales de seguridad y exigen una toma de decisiones más ágil y basada en inteligencia.

Esta es la premisa central del informe ‘Decision Advantage in the Gray Zone’. Su objetivo es ofrecer una visión general de alto nivel sobre las amenazas que están moldeando la industria y destacar los principales riesgos para los que las organizaciones aeroespaciales y de defensa deben prepararse en el próximo año. Estas amenazas pueden originarse dentro del negocio y sus operaciones, o surgir de un entorno externo cada vez más impredecible.

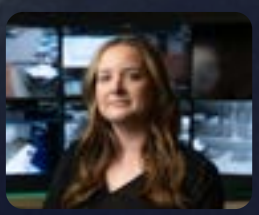
Este informe condensado resume los hallazgos clave del análisis completo ‘Aerospace & Defense Industry – Top Threats 2026’, brindando a los líderes una visión enfocada y accionable de los desafíos más urgentes que definirán el año.

Para acceder al informe completo, comuníquese con Securitas Risk Intelligence o utilice el código QR ubicado en la contraportada de este informe.

Miembros del equipo

Anastasia Jobard
Junior Protective Intelligence Analista *(Sector aeroespacial y de defensa)*

Freddie Venables
Junior Protective Intelligence Analista *(Sector aeroespacial y de defensa)*



Sophie Cairney
Consultor Líder en Inteligencia de Riesgos.

Nuestro Toolkit de inteligencia

Awareness

Reportes programados regularmente y ad hoc sobre el panorama global de seguridad y amenazas, incluyendo reportes de inteligencia (INTREPs) y reportes de situación (SITREPs).

- Reportes diarios de inteligencia global
- Perspectivas semanales de inteligencia global
- Pronósticos mensuales de amenazas
- Resúmenes mensuales de inteligencia (INTSUMs)
- Reportes de situación (SITREPs) y reportes de inteligencia (INTREPs) sobre desarrollos significativos

Alerting

Alertas geo-localizadas vía correo electrónico sobre eventos de seguridad y amenazas cercanas. Totalmente personalizables según nivel de gravedad, proximidad y frecuencia, con tipos de incidentes como:

- Criminalidad
- Disturbios civiles
- Terrorismo
- Clima
- Viajes y transporte

Advisory

Una solución integral de Inteligencia Protectiva, de Amenazas y Riesgos para su organización, operaciones y marca. Incluye:

- Monitoreo adaptado a sus requerimientos específicos
- Resúmenes diarios de inteligencia de monitoreo
- Informes inmediatos para alertas e inteligencia preventiva
- Solución de Inteligencia de Amenazas, Protección y Riesgos
- Acceso al servicio de reportes ad hoc bajo demanda

Proteja su organización con inteligencia líder en la industria. Securitas Risk Intelligence va más allá de identificar lo que está ocurriendo: también explica por qué es importante, qué podría suceder después y, lo más importante, qué acciones pueden tomarse.

Con cuatro niveles de servicios premium, ofrecemos herramientas digitales, servicios gestionados y experiencia especializada integrada, combinados para crear una solución personalizada que responda a sus necesidades específicas.

Adicionalmente, ofrecemos servicios de inteligencia y consultoría ad hoc para atender los requerimientos particulares de nuestros clientes.

Analista

Recursos de inteligencia dedicados, respaldados por la experiencia de la Comunidad Global de Inteligencia de Securitas.

Equipados con todas las herramientas y la formación necesarias para apoyar sus requerimientos de inteligencia y proteger su organización.

Inteligencia Ad Hoc

Experiencia especializada y consultoría para responder a requerimientos de inteligencia dinámicos y específicos.
Los tipos de reportes más comunes incluyen, entre otros:

- Reportes de seguridad para viajes y viajeros: análisis detallado de amenazas de seguridad y riesgos durante desplazamientos.
- Protección ejecutiva y screening defensivo: evaluación de vulnerabilidades de información de un principal objetivo (por ejemplo, un ejecutivo).
- Evaluaciones y monitoreo de seguridad para eventos: procesos de debida diligencia y monitoreo en tiempo real.

Este informe ha sido desarrollado por el Risk Intelligence Center (RIC) de Securitas, nuestra unidad especializada en análisis global de riesgos y visión estratégica. El RIC monitorea continuamente desarrollos geopolíticos, amenazas emergentes y patrones de riesgo específicos de la industria, transformando información compleja en inteligencia clara y basada en evidencia. Su trabajo proporciona la base analítica para las evaluaciones y servicios de inteligencia de Securitas.

Metodología

Enfoque

El RIC utiliza inteligencia de múltiples fuentes, combinando inteligencia de fuentes abiertas (OSINT) y fuentes cerradas, como inteligencia humana (HUMINT), para proporcionar inteligencia procesada y lista para la toma de decisiones.

La inteligencia de múltiples fuentes utiliza todas las fuentes de inteligencia disponibles y apropiadas, basadas en los Requerimientos Críticos de Inteligencia del Cliente (CCIRs).

Amenazas

Las amenazas potenciales consideradas en el contexto de este informe de inteligencia incluyen aquellas que podrían anticiparse razonablemente con base en la inteligencia existente, tales como (aunque no limitadas a):

- Delitos menores y oportunistas, así como actividades del crimen organizado.
- Ataques violentos dirigidos y no dirigidos, tanto de naturaleza criminal como terrorista.
- Actividades de protesta, dirigidas y no dirigidas.
- Seguridad corporativa, incluyendo amenazas internas, espionaje corporativo y operaciones empresariales sensibles.

La inclusión de estas amenazas en este informe no implica que necesariamente vayan a ocurrir, sino que existe el potencial de que se materialicen y que deben ser consideradas al realizar revisiones de seguridad, protección y evaluaciones de riesgo.

De igual forma, aunque se realizan todos los esfuerzos razonables para evaluar cada posible vector de amenaza para las organizaciones, el panorama de seguridad y amenazas es dinámico y está en constante cambio, con nuevas amenazas emergiendo continuamente.

Es importante que este informe sea utilizado como una herramienta dentro de una estrategia de seguridad más amplia, y no como un documento independiente destinado a capturar o describir todas las amenazas potenciales para la industria.

Lenguaje de la probabilidad

Este informe utiliza el lenguaje de probabilidad del RIC para proporcionar una evaluación sobre la probabilidad de que una amenaza se materialice, utilizando como referencia porcentajes, fracciones o proporciones. Esto permite aportar mayor contexto y claridad, además de promover una comprensión estandarizada de las evaluaciones y los términos utilizados.

Término	Probabilidad
Remota	0-5%
Muy improbable	10-20%
Improbable	25-35%
Posibilidad realista	40-50%
Probable	55-75%
Muy probable	80-90%
Casi segura	95-99%

Niveles de amenaza

Este informe utiliza el sistema de niveles de amenaza del RIC para calificar las amenazas en una escala del 1 al 5 en función de la probabilidad y gravedad evaluadas, y/o la intención y capacidad.

5 - EXTREMO	*Amenaza muy alta/extrema.* *Revisar y responder si es necesario.*
4 - ALTO	*Amenaza alta/grave.* *Considere tomar las medidas oportunas.*
3 - MODERADO	*Amenaza moderada.* *Manténgase alerta y tome precauciones.*
2 - BAJO	*Amenaza baja/limitada.* *Tenga cuidado.*
1 - MUY BAJO	*Amenaza muy baja/insignificante.* Para concienciar.

Fecha límite de inteligencia (ICOD)

17:00 UTC, 5 de diciembre de 2025

Aeroespacial y Defensa
Principales Amenazas 2026

Resumen

Escalada del activismo contra la guerra y focalización en organizaciones de A&D (Aeroespacial y Defensa)

El activismo contra la guerra seguirá siendo una preocupación creciente para la industria de A&D, particularmente mientras persista el conflicto entre Gaza e Israel, lo que impulsa motivaciones superpuestas entre los grupos activistas hacia acciones directas más disruptivas y, en algunos casos, violentas. Las organizaciones con vínculos identificables o percibidos con Israel y con empresas de defensa israelíes continúan siendo objetivos importantes.
Se espera que estos grupos intensifiquen campañas coordinadas que incluyan interrupciones físicas, acoso digital y acciones dirigidas contra altos ejecutivos e instalaciones clave.

Factores geopolíticos que impulsan protestas, disturbios y actividad delictiva

Las tensiones geopolíticas seguirán impulsando protestas, disturbios y activismo contra las organizaciones de A&D, alimentadas por conflictos en curso, preocupaciones ambientales y competencia económica.
Se prevé un aumento de las amenazas criminales, especialmente por parte de grupos de crimen organizado respaldados o tolerados por Estados, que buscan robar propiedad intelectual, materiales y componentes, así como llevar a cabo sabotajes.
De manera simultánea, se espera que aumenten las amenazas a la seguridad corporativa, incluyendo espionaje y sabotaje, lo que requerirá una vigilancia reforzada en todo el sector.

Aumento de la guerra en la zona gris y riesgos de sabotaje

La guerra en la zona gris (GZW, por sus siglas en inglés) y el sabotaje tienen cada vez más probabilidades de causar interrupciones significativas en 2026, incluyendo posibles eventos con múltiples víctimas, interrupciones en la cadena de suministro y fallas en los sistemas de TI o comunicaciones que afecten infraestructuras nacionales críticas y activos aeroespaciales privados.
Es probable que actores estatales y no estatales continúen empleando estas tácticas para socavar, influir y perturbar los intereses occidentales en A&D, lo que hace necesarias sólidas medidas de resiliencia y gestión de crisis.

Aumento de la focalización en ejecutivos y personas VIP

Los ejecutivos y VIP dentro del sector A&D siguen siendo objetivos de alto riesgo tanto para criminales como para activistas, impulsados por el extremismo ideológico, el oportunismo criminal y las tensiones geopolíticas.
El mayor uso de doxxing (exposición de datos personales), medios sintéticos y campañas coordinadas de acoso ha reducido las barreras para el ataque personal. Las organizaciones deben priorizar medidas para proteger la información personal de los ejecutivos, monitorear posibles suplantaciones de identidad e integrar protecciones tanto físicas como cibernéticas.

Persistencia y evolución de los riesgos internos (insider threats)

Las amenazas internas continúan representando un riesgo significativo, con individuos motivados por una amplia variedad de factores que explotan vulnerabilidades para causar interrupciones, pérdida de datos y daño reputacional.
Los actores de estas amenazas pueden incluir empleados, contratistas, activistas, delincuentes y estados hostiles, actuando de manera maliciosa o negligente. Esto subraya la necesidad crítica de contar con programas efectivos de gestión de amenazas internas, controles de acceso y monitoreo continuo de seguridad en 2026.

El panorama general de amenazas para la industria aeroespacial y de defensa en 2026 es moderado, impulsado por una combinación de riesgos de protestas y disturbios de alto nivel y mayores amenazas a la seguridad corporativa, mientras que la exposición al crimen y al terrorismo sigue siendo moderada pero persistente. Los actores de amenazas y los incidentes de seguridad globales probablemente afectarán las operaciones, la seguridad del personal y la reputación de la marca, con efectos que varían según la exposición geográfica y del sector.

De cara al futuro, la próxima crisis a nivel sectorial dentro de la industria aeroespacial y de defensa probablemente se derive de focos de tensión geopolítica o nuevos conflictos, en medio de presiones constantes como el cambio climático y la polarización política, que generan vulnerabilidades adicionales. Las organizaciones que invierten en alerta temprana, resiliencia y seguridad integrada multidominio están mejor posicionadas para mantener una ventaja en la toma de decisiones en este entorno cada vez más conflictivo.

Áreas de amenaza clave

Protestas y disturbios

Nivel de amenaza evaluado: 4

Delincuencia y seguridad

Nivel de amenaza evaluado: 3

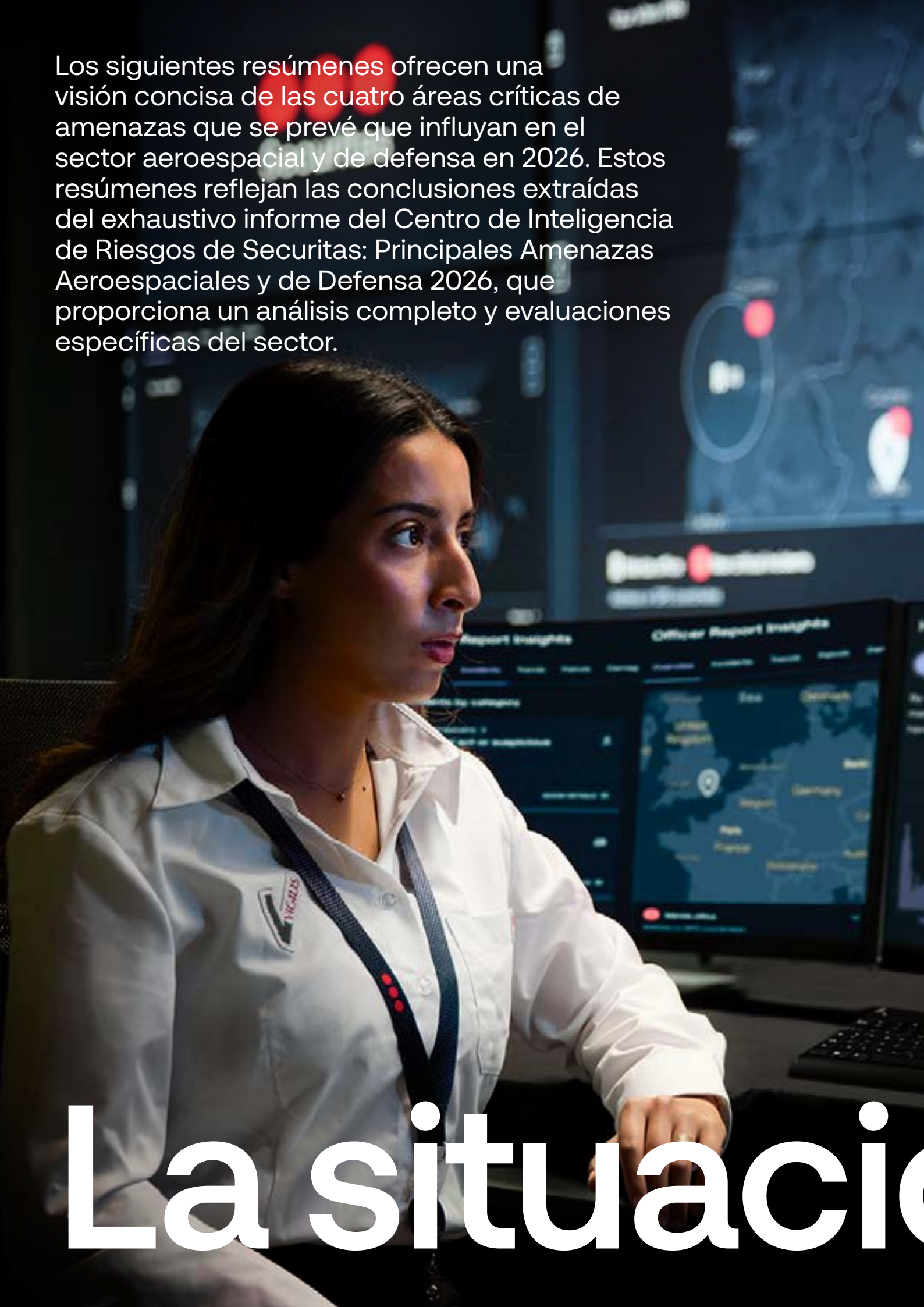
Seguridad corporativa

Nivel de amenaza evaluado: 4

Terrorismo y extremismo

Nivel de amenaza evaluado: 3

Los siguientes resúmenes ofrecen una visión concisa de las cuatro áreas críticas de amenazas que se prevé que influyan en el sector aeroespacial y de defensa en 2026. Estos resúmenes reflejan las conclusiones extraídas del exhaustivo informe del Centro de Inteligencia de Riesgos de Securitas: Principales Amenazas Aeroespaciales y de Defensa 2026, que proporciona un análisis completo y evaluaciones específicas del sector.



La situaci


Spain
historical event pattern
Burglary
Trespassing
intelligence briefs

ón

El panorama de protestas y disturbios en 2026 seguirá siendo muy activo, diverso y cada vez más coordinado. Las redes propalestinas y pacifistas, los grupos ecologistas e incluso los teóricos de la conspiración con intereses afines continuarán utilizando a las organizaciones aeroespaciales y de defensa como objetivos simbólicos y operativos. Los activistas están adoptando tácticas digitales y presenciales más sofisticadas, ampliando sus campañas desde las instalaciones y las cadenas de suministro hasta la presión dirigida a ejecutivos, personalidades importantes y empleados. Esto crea un entorno de amenazas más impredecible y personalizado para el sector.

Protestas y disturbios
Panorama general

Panorama general de las protestas y los disturbios

Evaluación de amenazas

Escenario más probable (MLCOA) vs. escenario más peligroso (MDCOA)

MLCOA: Los activistas mantienen protestas frecuentes, movilización en línea y acciones disruptivas dirigidas contra organizaciones de A&D, ampliando la presión para incluir a ejecutivos, miembros de juntas directivas y empleados.

Aumenta la visibilidad en torno a viviendas, eventos y sedes corporativas, aunque la mayoría de las interacciones siguen siendo no violentas, pero sí disruptivas.

MDCOA: Campañas coordinadas de acción directa en múltiples ubicaciones generan una gran disrupción operativa, con el acoso dirigido que escala a confrontaciones agresivas en residencias privadas o lugares de trabajo.

No se pueden descartar riesgos aislados de violencia, coerción criminal o sabotaje de alto impacto.

Dinámicas clave

1 Movilización antibelicista/propalestina

- Gaza-Israel sigue siendo el principal motor del activismo disruptivo contra las organizaciones de defensa y armamento.
- Las redes activistas atacan a empresas y proveedores percibidos como vinculados a programas de defensa, a menudo coordinando acciones transfronterizas.
- Las tácticas incluyen bloqueos de instalaciones, interrupciones en la cadena de suministro, interferencia en eventos importantes y campañas coordinadas depresión digital.
- Los nuevos grupos activistas adoptan tácticas, técnicas y procedimientos (TTP) cada vez más disruptivos, a pesar de las restricciones impuestas por las autoridades a estos grupos.

2 Ataques dirigidos a ejecutivos, personalidades importantes y empleados

Los ejecutivos y altos directivos son cada vez más objeto de ataques mediante la divulgación de información personal, comunicaciones hostiles, medios de comunicación sintéticos, cartas abiertas y campañas en redes sociales.

- Aumentan los ataques dirigidos a domicilios particulares, ya que los activistas utilizan información pública para identificar direcciones y rutinas personales.
- Los empleados que se encuentran en las entradas de las instalaciones son grabados, identificados y avergonzados públicamente en línea, lo que genera problemas de reputación y seguridad personal.
- Los activistas también utilizan el «ataque relacional», aprovechando los cargos directivos, las afiliaciones universitarias o las alianzas de los ejecutivos para ejercer presión.

3 Activismo estudiantil y presión universitaria

- Grupos estudiantiles continúan protestando contra los vínculos de las universidades con empresas de defensa y aeroespacial, interrumpiendo eventos de reclutamiento y colaboraciones de investigación.
- Persisten los campamentos, las pancartas y las acciones coordinadas en los campus, presionando a las universidades para que reconsideren su colaboración con organizaciones de defensa.

4 El activismo ambiental converge con los discursos antibélicos

- Las organizaciones aeroespaciales y de defensa siguen siendo objetivos prioritarios del activismo climático.
- Grupos como Extinction Rebellion (XR) y sus afiliados a A22 se centran en exhibiciones aéreas, eventos de gran visibilidad y activos relacionados con emisiones o impacto ambiental.
- La creciente convergencia entre el activismo climático, los discursos antibélicos y las narrativas anticapitalistas aumenta el nivel de amenaza y amplía los posibles objetivos.

Acciones Prioritarias

- Reducir la visibilidad de la información de ejecutivos y empleados en fuentes abiertas, garantizando un monitoreo proactivo frente a doxing, suplantación de identidad y actividades de reconocimiento hostil.
- Prepararse para movilizaciones intersectoriales en torno a eventos clave de la industria, puntos críticos geopolíticos y ciclos de contratación que puedan actuar como catalizadores de protestas o campañas dirigidas.
- Fortalecer los planes de respuesta basados en escenarios para protestas pacíficas, acoso dirigido, interrupciones en la cadena de suministro y acciones coordinadas en múltiples sitios, integrando equipos de seguridad física, recursos humanos, comunicaciones y asuntos legales.

La criminalidad seguirá representando una amenaza persistente para las organizaciones del sector A&D durante 2026, impulsada por tensiones geopolíticas, presiones económicas y la continua presión sobre las cadenas de suministro globales. El alto valor de los productos de la industria, los materiales sensibles y la información propietaria incrementa la exposición a robos, sabotajes, adquisiciones ilícitas y facilitación criminal.

Los grupos de crimen organizado (OCGs) y actores alineados con Estados continuarán explotando brechas en la verificación de proveedores y en las redes logísticas, traficando componentes críticos a través de mercados grises y negros. A medida que aumenten las presiones de producción, las organizaciones enfrentarán mayores riesgos de que piezas falsificadas o robadas ingresen a las cadenas de suministro legítimas.

Las amenazas cibernéticas también se intensificarán, con actores respaldados por Estados y motivados financieramente perfeccionando operaciones de espionaje, exfiltración de datos y suplantación de identidad habilitada por inteligencia artificial. La exposición de ejecutivos, la manipulación mediante medios sintéticos y las amenazas híbridas digitales/físicas continuarán ampliando la superficie de ataque, resaltando la necesidad de una integración entre la seguridad cibernética y la seguridad física.

Panorama de Crimen y Seguridad

Evaluación de Amenazas

Curso de acción más probable (MLCOA) vs. curso de acción más peligroso (MDCOA)

MLCOA: Actores criminales continúan atacando las cadenas de suministro del sector A&D mediante robos recurrentes de materiales menores, piezas y componentes. Los artículos robados o reutilizados aparecen en mercados ilícitos, aumentando el riesgo de contaminación de las cadenas de suministro. Los ciberdelincuentes mantienen una presión constante con fines de lucro financiero y robo de datos.

MDCOA: Una campaña criminal de gran escala —potencialmente respaldada por Estados adversarios— ataca la cadena de suministro del sector A&D mediante robo, sabotaje y adquisiciones ilícitas. La disrupción obliga a depender de proveedores no autorizados, introduciendo componentes peligrosos en los procesos de producción y afectando la seguridad y la capacidad operativa.

Dinámicas Clave

1 Adquisición Ilícita y Vulnerabilidades en la Cadena de Suministro

- Los grupos de crimen organizado (OCGs) siguen siendo los principales facilitadores del robo, desvío y adquisición encubierta de componentes para Estados sancionados como Rusia, Irán y China.
- Aviónica, sensores, tarjetas de circuitos y componentes de precisión robados son traficados a través de mercados grises y negros a precios inflados.
- Las escaseces de suministro y los cuellos de botella en la producción aumentan los incentivos para adquirir componentes no verificados, lo que eleva los riesgos de contaminación de la cadena de suministro.
- • Los puntos débiles en la gestión de carga, la verificación de proveedores y el cumplimiento transfronterizo continúan siendo explotados.

2 Colaboración en Profundización entre OCG y Estados

- Las sanciones y los controles de exportación están acelerando la colaboración entre Estados adversarios y grupos de crimen organizado (OCGs) que buscan obtener piezas restringidas.
- Los grupos criminales aprovechan corredores de contrabando ya establecidos, empresas fachada e intermediarios logísticos perfeccionados durante recientes disrupciones geopolíticas.
- Dado que los ensamblajes de gran tamaño siguen siendo difíciles de sustraer, el enfoque se desplaza hacia componentes más pequeños y de alto valor, así como otros objetivos más lucrativos y accesibles.

3 Escalada del Ciberespionaje e Intrusiones Habilitadas por IA

- Actores cibernéticos respaldados por Estados y grupos criminales están perfeccionando operaciones de espionaje, robo de credenciales y exfiltración de datos contra redes del sector A&D.
- La suplantación de identidad habilitada por inteligencia artificial, los audios y videos sintéticos, y los documentos deepfake incrementan las capacidades de engaño y reducen las barreras de detección.
- Durante 2025 se registraron múltiples campañas sostenidas, incluidos ciberataques contra importantes empresas israelíes del sector A&D y continuas operaciones de espionaje por actores respaldados por Rusia.
- El phishing y el compromiso a través de proveedores pequeños o prestadores de servicios continúan siendo vías clave de acceso a programas de alto valor.

4 Incremento de Ataques contra Ejecutivos y Personas Sensibles

- La exposición de información personal impulsa el doxing, la intimidación y las presiones híbridas digitales y físicas.
- Las bases de datos públicas y las filtraciones de información personal identificable (PII) reducen las barreras para que actores adversarios identifiquen y rastreen a ejecutivos.
- Durante 2025 se evidenció una escalada en la gravedad de las acciones dirigidas contra ejecutivos, pasando de amenazas en línea a intentos de secuestro, sabotaje de propiedades y complots de asesinato vinculados a Estados.
- • Los medios sintéticos, las narrativas manipuladas y la suplantación de identidad cibernética personalizada intensifican los riesgos reputacionales y de seguridad.

Acciones Prioritarias

- **Fortalecer la verificación y validación de proveedores** en todos los niveles de la cadena, priorizando controles que eviten el ingreso de componentes falsificados, robados o ilícitos a la cadena de suministro.
- **Implementar estrategias integradas de seguridad cibernética y física** para abordar espionaje, sabotaje, suplantación mediante contenido sintético, exposición de ejecutivos y amenazas híbridas.
- **Realizar evaluaciones específicas sobre actores de amenaza probables** (OCGs, redes alineadas con Estados y personal interno descontento) para identificar vulnerabilidades en logística, personal y sistemas digitales.
- **Desarrollar, probar y actualizar periódicamente planes de respuesta a incidentes** —incluyendo intrusiones cibernéticas, compromisos en la cadena de suministro y ataques dirigidos a ejecutivos— respaldados por ejercicios interfuncional.

Los riesgos de seguridad corporativa para las organizaciones del sector A&D se intensificarán en 2026 a medida que las amenazas internas, el espionaje corporativo, las acciones encubiertas hostiles, las actividades de reconocimiento y la transferencia de activos sensibles converjan con el aumento de las tensiones geopolíticas y un entorno sociopolítico profundamente polarizado.

Actores de amenaza, incluidos empleados, contratistas, activistas, criminales, auditores y grupos alineados con Estados, continúan explotando vulnerabilidades en los ámbitos físico, digital y humano, desafiando las capacidades de detección y respuesta, y aumentando el riesgo de disrupciones operacionales, reputacionales y estratégicas.

Panorama de Seguridad Corporativa

Panorama de Seguridad Corporativa

Evaluación de Amenazas

Curso de acción más probable (MLCOA) vs. curso de acción más peligroso (MDCOA)

MLCOA: Las organizaciones enfrentan la continua divulgación accidental o maliciosa de información sensible, uso indebido interno de bajo nivel, actividades oportunistas de reconocimiento y sostenidos intentos de espionaje mediante ingeniería social, robo de credenciales, uso de drones e infiltración presencial. El aumento de la polarización ideológica contribuye a mayores riesgos internos impulsados por agravios, mientras que actividades hostiles rutinarias ponen a prueba la postura de seguridad en instalaciones corporativas y cadenas de suministro.

MDCOA: Actores patrocinados por Estados y actores híbridos intensifican campañas coordinadas que incluyen reclutamiento interno, sabotaje, espionaje complejo, reconocimiento habilitado por drones y explotación de relaciones con terceros para acceder o desviar activos sensibles. Empleados maliciosos extraen datos valiosos o facilitan ataques posteriores, mientras adversarios sofisticados aprovechan actividades de reconocimiento y acciones encubiertas para interrumpir operaciones, comprometer cadenas de suministro o generar daños reputacionales y legales.

Dinámicas Clave

1 Incremento de Amenazas Internas

- Las amenazas internas abarcan empleados, contratistas, visitantes y terceros aliados, actuando de forma maliciosa o negligente en entornos físicos y digitales.
- Las motivaciones incluyen presión financiera, agravios ideológicos, circunstancias personales, coerción, búsqueda de notoriedad o explotación por parte de actores hostiles.
- Las filtraciones de información sensible —incluyendo documentos internos, correos electrónicos o información personal identificable (PII)— a través de herramientas de IA o redes sociales generan exposición operativa, legal y reputacional.
- Casos relevantes en 2025 evidenciaron el reclutamiento, respaldado por Estados, de personas con acceso privilegiado, incluyendo robo de secretos comerciales y exfiltración para programas de inteligencia extranjera.
- Indicadores de actividad maliciosa incluyen violaciones reiteradas de seguridad, intentos de acceso inexplicables, actividades en horarios inusuales, transferencia de archivos a dispositivos personales y patrones de renuncia anticipada.

2 Expansión de la Exposición al Espionaje Corporativo

- El aumento de la competencia geopolítica incrementa el espionaje dirigido contra diseños propietarios, datos de I+D, propiedad intelectual y tecnologías de doble uso.
- Actores respaldados por Estados explotan intrusiones cibernéticas, ingeniería social, visitas de dignatarios extranjeros y accesos internos para obtener información confidencial.
- Las organizaciones involucradas en programas de adquisición, investigaciones sensibles o contratos gubernamentales enfrentan un mayor nivel de exposición y focalización.
- Eventos registrados en 2025 —desde arrestos por espionaje en Letonia, Turquía y Ucrania, hasta filtraciones de imágenes de aeronaves prototipo— evidencian la amplitud de las tácticas utilizadas por los adversarios.
- Las campañas de espionaje respaldan operaciones posteriores, incluyendo manipulación de información, ransomware o actividades coordinadas en zonas grises.

3 Incremento de Sabotajes y Acciones Encubiertas Hostiles

- Actores estatales y no estatales llevan a cabo actividades encubiertas por debajo de los umbrales de escalamiento, poniendo a prueba las capacidades de detección y respuesta.
- Las amenazas incluyen incendios provocados, reconocimiento mediante drones, bombas enviadas en paquetes, manipulación de cables submarinos, guerra electrónica y falsas amenazas de bomba.
- Las tácticas híbridas tienen como objetivo instalaciones militares, centros de transporte, infraestructura logística, plantas de ensamblaje y ubicaciones de doble uso.
- Numerosos incidentes entre 2024 y 2025 en Europa evidenciaron drones sobrevolando instalaciones nucleares, trenes de municiones, bases navales e infraestructura de doble uso.
- La subcontratación de acciones encubiertas a intermediarios criminales o extremistas incrementa la negación plausible, pero también eleva la imprevisibilidad y los riesgos de escalamiento.

4 Reconocimiento Hostil y Desafíos en Auditorías de Seguridad

- Los auditores de seguridad continúan grabando instalaciones de manera abierta para generar interacción en línea, exponiendo información crítica e indicadores sensibles (puntos de acceso, cobertura de CCTV, códigos y datos de empleados).
- El reconocimiento encubierto mediante drones, dispositivos disfrazados o visitas repetitivas a instalaciones proporciona inteligencia indirecta para activistas, criminales y actores respaldados por Estados.
- Los auditores seguirán aprovechando derechos de acceso a terrenos públicos, generando riesgos reputacionales para las organizaciones objetivo ante un manejo inadecuado de las interacciones con el personal de seguridad.
- El reconocimiento habilitado por drones en sitios sensibles —incluyendo centros de investigación e instalaciones de defensa— continúa en aumento y frecuentemente está vinculado a intereses de inteligencia extranjera.

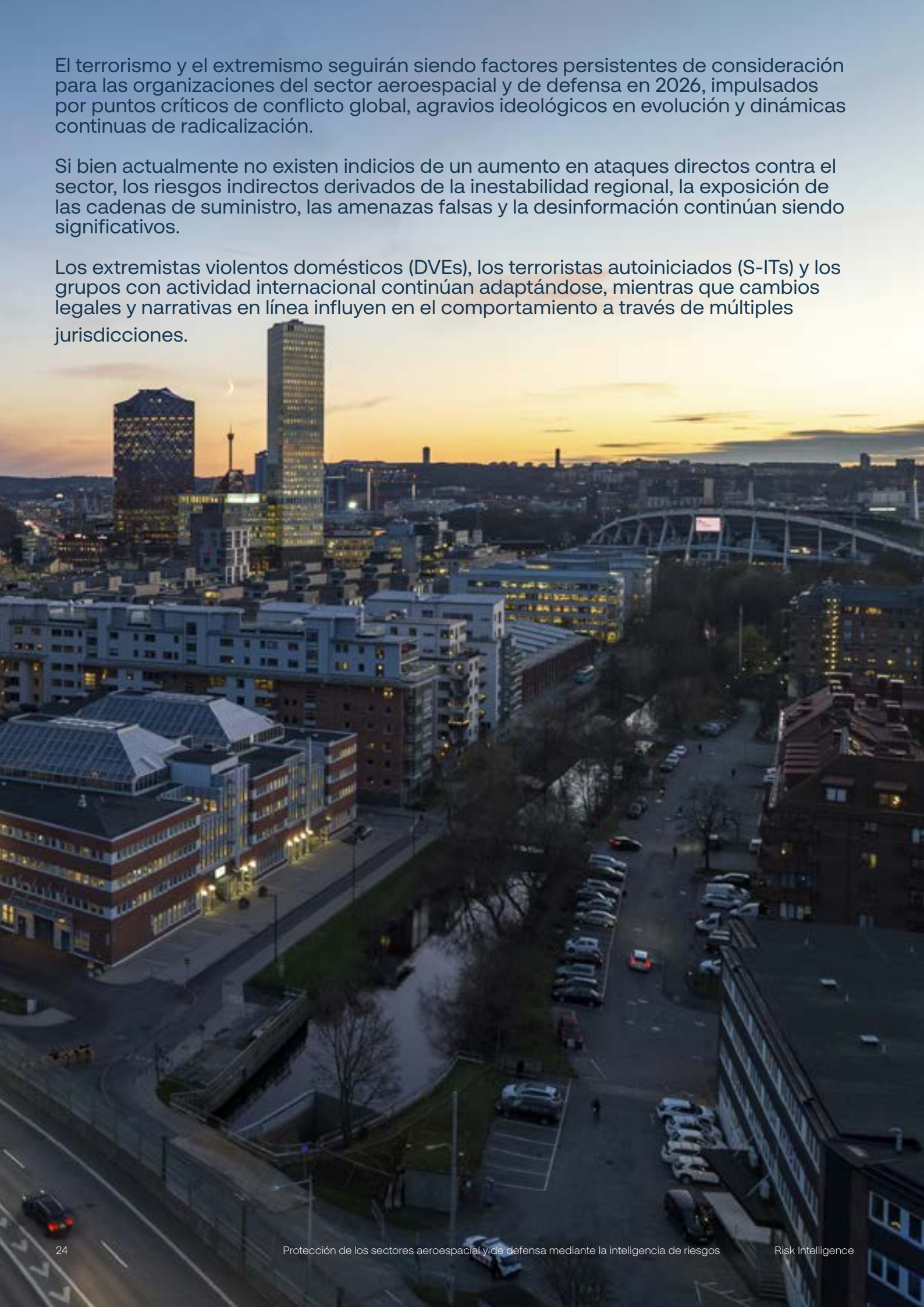
Acciones Prioritarias

- Fortalecer los programas de amenazas internas mediante indicadores conductuales, monitoreo de fuentes abiertas e integración entre recursos humanos, ciberseguridad y seguridad física.
- Reforzar los controles sobre el manejo de información sensible, los procesos de desvinculación laboral y los accesos privilegiados de empleados, contratistas y aliados.
- Ampliar la capacitación en contraespionaje y seguridad operacional (OPSEC), especialmente para equipos involucrados en I+D, adquisiciones, proyectos sensibles y delegaciones extranjeras.
- Actualizar los planes de crisis y respuesta a incidentes para incluir sabotaje, acciones encubiertas, incursiones con drones, brechas facilitadas por amenazas internas y eventos de reconocimiento hostil.
- Mejorar la transparencia de la cadena de suministro, el cumplimiento de sanciones y el monitoreo de terceros aliados, incluyendo debida diligencia y trazabilidad de activos.
- Capacitar al personal de primera línea y a los equipos de seguridad para gestionar adecuadamente a auditores y actividades de reconocimiento hostil, evitando escalamientos mientras se protege la información sensible.
- Desarrollar capacidades de preparación contra drones, fortalecer la coordinación con entidades públicas y poner a prueba los procedimientos de respuesta mediante ejercicios de mesa y ejercicios multiagencia.

El terrorismo y el extremismo seguirán siendo factores persistentes de consideración para las organizaciones del sector aeroespacial y de defensa en 2026, impulsados por puntos críticos de conflicto global, agravios ideológicos en evolución y dinámicas continuas de radicalización.

Si bien actualmente no existen indicios de un aumento en ataques directos contra el sector, los riesgos indirectos derivados de la inestabilidad regional, la exposición de las cadenas de suministro, las amenazas falsas y la desinformación continúan siendo significativos.

Los extremistas violentos domésticos (DVEs), los terroristas autoiniciados (S-ITs) y los grupos con actividad internacional continúan adaptándose, mientras que cambios legales y narrativas en línea influyen en el comportamiento a través de múltiples jurisdicciones.



Panorama de Terrorismo y Extremismo

Evaluación de Amenazas

Curso de acción más probable (MLCOA) vs. curso de acción más peligroso (MDCOA)

MLCOA: No existen señales claras de un aumento en ataques directos contra organizaciones del sector A&D. Sin embargo, los incidentes terroristas que afecten cadenas de suministro, particularmente en regiones de alto riesgo con conflictos activos o tensiones geopolíticas, continúan siendo una posibilidad realista.

MDCOA: Las percepciones sobre la participación del sector A&D en conflictos globales generan ataques dirigidos contra empresas, instalaciones o cadenas de suministro. La desinformación, las críticas al sector y los puntos críticos geopolíticos convergen con agravios personales, alimentando procesos de radicalización entre extremistas violentos domésticos (DVEs), terroristas autoiniciados (S-ITs) y grupos terroristas establecidos.

Dinámicas Clave

1 Evolución de las Motivaciones de DVEs y S-ITs

- Las motivaciones extremistas incluyen ideologías de extrema derecha, extrema izquierda, raciales/étnicas, antiautoridad y antitecnología.
- Los agravios personales se entrelazan cada vez más con narrativas geopolíticas amplificadas en redes sociales.
- Los ciclos de radicalización se aceleran a través de plataformas en línea, a pesar del aumento en la proscripción de redes extremista.

2 Designaciones Legales que Moldean el Comportamiento Extremista

- Las nuevas designaciones de grupos previamente considerados redes activistas o criminales disuaden parte de sus actividades.
- Las restricciones y acciones dirigidas contra estos grupos provocarán que los elementos más comprometidos pasen a operar "en la clandestinidad", fortaleciendo su seguridad operacional (OPSEC) y/o cambiando de identidad o ubicación para evitar ser detectados.
- La respuesta pública negativa frente a medidas percibidas como "excesivamente severas" contra grupos activistas presenta el riesgo de generar incrementos no intencionados en el apoyo público hacia el grupo y sus causas.

3 Ataques mediante Engaños y Disrupción

- Las empresas del sector A&D continúan siendo vulnerables a comunicaciones maliciosas, falsas amenazas de bomba y alarmas disruptivas.
- Estas acciones suelen tener como objetivo provocar respuestas, poner a prueba los protocolos de seguridad u obtener información operativa.
- Las actividades engañosas se utilizan cada vez más para evaluar capacidades de respuesta y facilitar actividades de reconocimiento contra sitios objetivo.

4 IAmenazas Indirectas derivadas de Zonas de Conflicto Global

- Los incidentes terroristas en regiones con elevadas tensiones geopolíticas representan riesgos indirectos para las cadenas de suministro, la logística y el personal.
- Los gobiernos occidentales continúan advirtiendo que los ataques terroristas seguirán siendo probables en el corto plazo, aunque no estén específicamente rigidos contra el sector A&D.

Acciones Prioritarias

- Realizar evaluaciones de vulnerabilidad y riesgo de amenazas (TVRAs) específicas para cada sitio, enfocándose en instalaciones ubicadas cerca de puntos críticos geopolíticos o centros logísticos clave.
- Fortalecer los planes de continuidad del negocio y gestión de crisis, garantizando su alineación con las directrices nacionales de contraterrorismo y los programas de concientización para empleados.

Lea el Informe Completo
de la Industria

Contacto

intelligence@securitas.com