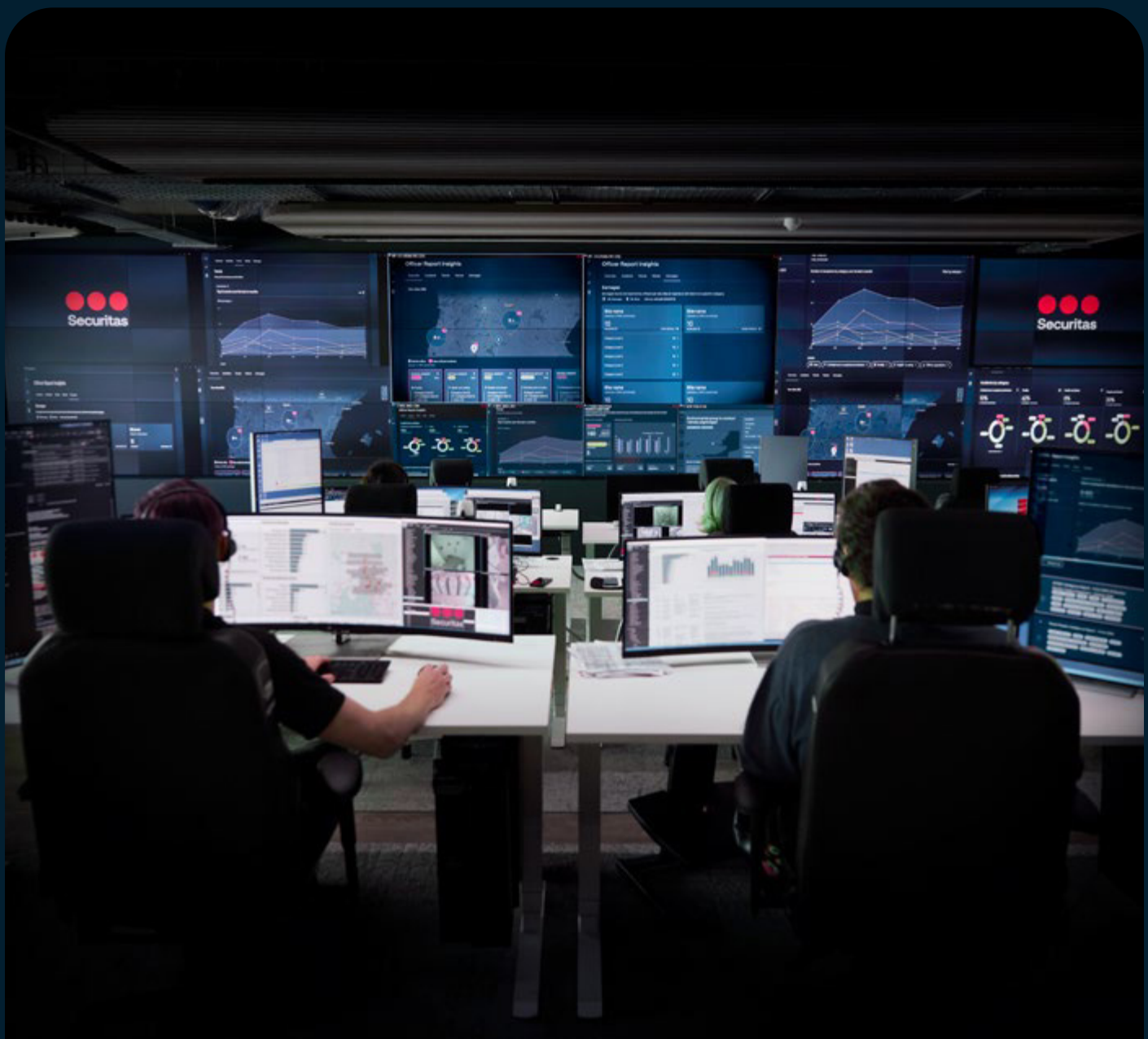
Securitas

Risk Intelligence

Toma de decisiones en entornos complejos

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

Inteligencia@securitas.es



Índice

«El sector aeroespacial y de defensa se encuentra atrapado en el fuego cruzado de la “convergencia” como nunca antes. Esto incluye cómo las amenazas geopolíticas y derivadas de los conflictos pueden afectar, directa e indirectamente, a las organizaciones del sector privado, así como los requisitos de seguridad necesarios para protegerse frente a ellas. Pero no todas las amenazas empiezan con una “explosión”: serán las organizaciones que apliquen estrategias de seguridad guiadas por la inteligencia para identificar, evaluar y actuar en defensa de sus intereses las que definan el futuro de la seguridad».

Introducción

Sophie Cairney

Consultora jefe de inteligencia de riesgos

El sector aeroespacial y de defensa (A&D) afronta, en 2026 y los años venideros, un panorama de amenazas volátil, incierto, complejo y ambiguo (VUCA), determinado por las tensiones geopolíticas, la polarización social y el uso creciente de tácticas en entornos complejos por parte de actores tanto estatales como no estatales. A medida que los conflictos persisten y se intensifica la competencia estratégica, las organizaciones de A&D quedan cada vez más expuestas a riesgos físicos, digitales y reputacionales que convergen entre sí, ponen a prueba los modelos de seguridad tradicionales y exigen una toma de decisiones más ágil y guiada por la inteligencia.

Esta es la premisa central del informe Ventaja en la toma de decisiones en entornos complejos.

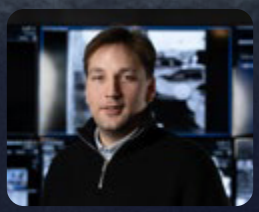
Su objetivo es ofrecer una visión de alto nivel de las amenazas que están moldeando el sector y destacar los principales riesgos para los que las organizaciones aeroespaciales y de defensa deberían prepararse de cara al próximo año. Estas amenazas pueden originarse dentro de la propia empresa y sus operaciones, o surgir de un entorno externo cada vez más impredecible.

Este informe condensado resume las principales conclusiones del análisis completo «Aerospace & Defense Industry – Top Threats 2026», y ofrece a los responsables una visión focalizada y accionable de las cuestiones más apremiantes que definirán el año.

Miembros del equipo

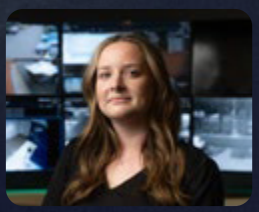
Anastasia Jobard

Analista junior de inteligencia de seguridad (sector aeroespacial y de defensa)



Freddie Venables

Analista junior de inteligencia de seguridad (sector aeroespacial y de defensa)



Sophie Cairney

Consultora jefe de inteligencia de riesgos

Nuestro kit de inteligencia

Conciencia

Informes periódicos y ad hoc sobre el panorama global de seguridad y amenazas, incluidos informes de inteligencia (INTREP) e informes de situación (SITREP).

— Informes diarios de inteligencia global.

— Perspectivas semanales de inteligencia global.

— Pronósticos mensuales de amenazas.

— Resúmenes mensuales de inteligencia

— Informes de situación (SITREP) e informes de inteligencia (INTREP) sobre desarrollos relevantes.

Alertas

Alertas por correo electrónico con geolocalización sobre incidentes de seguridad y amenazas en las inmediaciones. Totalmente personalizables en función de la gravedad, la proximidad y la frecuencia, con los siguientes tipos de incidentes:

— Criminalidad.

— Disturbios civiles.

— Terrorismo.

— Clima.

— Viajes y transporte.

Asesoramiento

Una solución integral de inteligencia de protección, amenazas y riesgos para tu organización, tus operaciones y tu marca. Incluye:

— Monitorización de tus requisitos específicos.

— Resúmenes diarios de inteligencia de monitorización.

— Informes inmediatos de inteligencia de advertencia.

— Solución de inteligencia de amenazas, protección y riesgos.

— Acceso al servicio de informes ad hoc bajo demanda.

Proteje tu organización con inteligencia líder en el sector. Securitas Risk Intelligence va más allá de identificar lo que está sucediendo. También explica por qué es importante, qué podría ocurrir a continuación y, lo más importante, qué medidas se pueden tomar. Con cuatro niveles de servicios premium, ofrecemos herramientas digitales, servicios gestionados y experiencia integrada, todo ello combinado para crear una solución a medida que satisfaga tus necesidades específicas. Además, ofrecemos inteligencia ad hoc y servicios de consultoría para satisfacer las necesidades concretas de nuestros clientes.

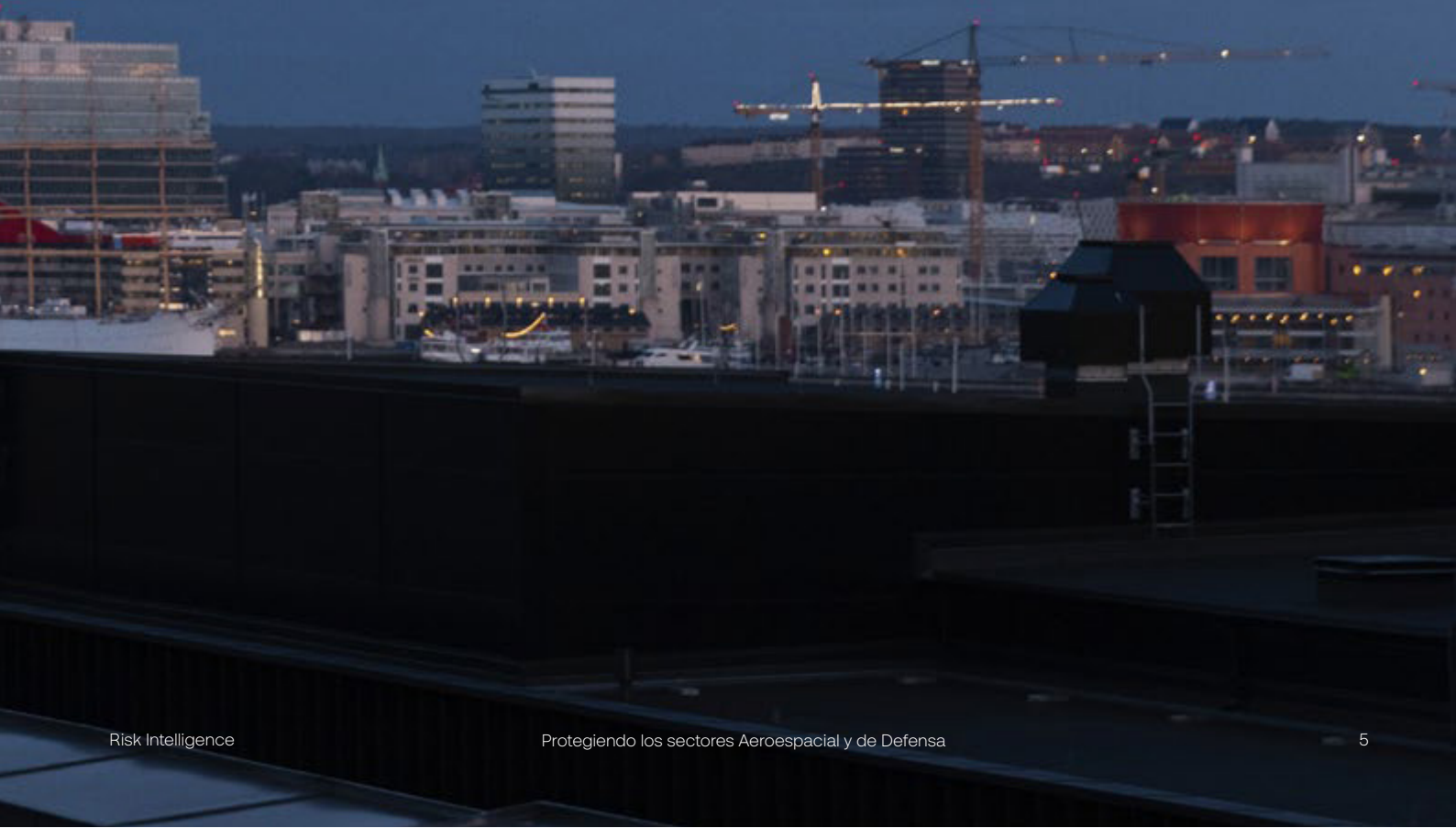
Análisis

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 tus requisitos de inteligencia y proteger tu organización.

Inteligencia Ad-hoc

Conocimiento experto y consultoría para cualquier requisito de inteligencia específico y dinámico. Los tipos de informe más habituales incluyen, entre otros:

- Informe de seguridad de viajes y viajeros: análisis en profundidad de la seguridad en los desplazamientos.
- Protección de ejecutivos y screening defensivo: evaluación de la vulnerabilidad de la información de un principal (p. ej., un directivo).
- Evaluaciones y screening de seguridad de eventos: diligencia debida y monitorización en directo.



Este informe ha sido elaborado por el Centro de Inteligencia de Riesgos (RIC) de Securitas, nuestra unidad especializada en el análisis global de riesgos y el conocimiento estratégico. El RIC monitoriza de forma continua los desarrollos geopolíticos, las amenazas emergentes y los patrones de riesgo específicos de cada sector, transformando información compleja en inteligencia clara y basada en evidencias. Su trabajo constituye el fundamento analítico de las evaluaciones y los servicios de inteligencia de Securitas.

Metodología

El RIC emplea inteligencia de todas las fuentes (all-source), combinando inteligencia de fuentes abiertas (OSINT) y fuentes cerradas como la inteligencia de fuentes humanas (HUMINT) para ofrecer inteligencia procesada. La inteligencia all-source utiliza todas las fuentes disponibles y apropiadas en función de los Requisitos Críticos de Inteligencia del Cliente (CCIR).

Amenazas

Las amenazas potenciales consideradas en el contexto de este informe de inteligencia incluyen aquellas que podrían anticiparse razonablemente a partir de la inteligencia existente, tales como (sin limitarse a estas):

- Delincuencia menor y oportunista, así como actividad delictiva organizada.
- Ataques violentos dirigidos y no dirigidos, tanto de naturaleza criminal como terrorista.
- Actividad de protesta, dirigida y no dirigida.
- Seguridad corporativa, incluidas amenazas internas, espionaje corporativo y operaciones empresariales sensibles.

La inclusión en este informe no implica que ninguna de estas amenazas vaya a producirse, sino que existe la posibilidad de que se materialicen y que deben tenerse en cuenta a la hora de realizar revisiones de seguridad y evaluaciones de riesgos.
Del mismo modo, es importante que este informe se utilice como una herramienta más dentro de una estrategia de seguridad más amplia, en lugar de como un documento independiente del que se espere que recoja y describa todas las amenazas

Lenguaje de probabilidad

Este informe emplea el lenguaje de probabilidad del RIC para evaluar la verosimilitud de que una amenaza se materialice, tomando como referencia un porcentaje, una fracción o un ratio. Esto aporta contexto y claridad y favorece una comprensión estandarizada de las evaluaciones y los términos empleados.

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

Niveles de amenaza

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

5 - EXTREMO	Amenaza muy alta / extrema. Revísar y responder si es necesario.
4 - ALTO	Amenaza grave. Considerar la posibilidad de tomar las medidas oportunas.
3 - MODERADO	Amenaza moderada. Mantenter alerta y tomar las precauciones necesarias.
2 - BAJO	Amenaza baja o limitada. Para tomar en cuenta
1 - MUY BAJO	Amenaza muy baja o insignificante. A título informativo.

Fecha límite de recepción de datos (ICOD)

17:00 UTC, 5 de diciembre de 2025

Principales amenazas para el sector aeroespacial y de defensa en 2026

Resumen

El activismo contra la guerra y los ataques contra las organizaciones de A&D

El activismo contra la guerra seguirá siendo una preocupación creciente para el sector de la defensa y la aeronáutica, sobre todo mientras persista el conflicto entre Gaza e Israel, lo que impulsa a los grupos activistas, con motivaciones que se solapan, a recurrir a acciones directas más disruptivas y, en ocasiones, violentas. Las organizaciones con vínculos identificables o percibidos con Israel y las empresas de defensa israelíes siguen siendo objetivos importantes. Se prevé que estos grupos intensifiquen sus campañas coordinadas, que incluyen actos de perturbación física, acoso digital y acciones dirigidas contra altos ejecutivos e instalaciones clave.

Factores geopolíticos que impulsan las protestas, los disturbios y la actividad delictiva

Las tensiones geopolíticas seguirán alimentando las protestas, los disturbios y el activismo contra las organizaciones del sector aeroespacial y de defensa, impulsados por los conflictos actuales, las preocupaciones medioambientales y la competencia económica. Se prevé un aumento de las amenazas delictivas, en particular por parte de grupos de delincuencia organizada respaldados o tolerados por el Estado que pretenden sustraer propiedad intelectual, materiales y componentes, así como llevar a cabo actos de sabotaje. Al mismo tiempo, se espera que aumenten las amenazas a la seguridad corporativa, incluyendo el espionaje y el sabotaje, lo que exigirá una mayor vigilancia en todo el sector.

El aumento de la guerra en entornos complejos y los riesgos de sabotaje

Es cada vez más probable que la guerra en entornos complejos (GZW) y el sabotaje provoquen perturbaciones significativas en 2026, incluyendo posibles incidentes con un gran número de víctimas, interrupciones en la cadena de suministro y cortes en los sistemas informáticos o de comunicaciones que afecten a infraestructuras nacionales críticas y a activos aeroespaciales privados. Es probable que los actores estatales y no estatales sigan empleando estas tácticas para socavar, influir y perturbar los intereses occidentales en el sector aeroespacial y de la defensa, lo que exigirá medidas sólidas de resiliencia y gestión de crisis.

Aumento de los ataques dirigidos contra ejecutivos y personalidades importantes

Los ejecutivos y personalidades destacadas del sector aeroespacial y de la defensa siguen siendo objetivos prioritarios tanto para delincuentes como para activistas, impulsados por el extremismo ideológico, el oportunismo criminal y las tensiones geopolíticas. El uso cada vez mayor del doxxing, los medios sintéticos y las campañas coordinadas de acoso ha reducido las barreras para los ataques personales. Las organizaciones deben dar prioridad a las medidas destinadas a proteger la información personal de los ejecutivos, vigilar los casos de suplantación de identidad e integrar medidas de protección tanto físicas como cibernéticas.

Riesgos persistentes y en constante evolución derivados de amenazas internas

Las amenazas internas siguen representando un riesgo significativo, ya que hay personas motivadas por una amplia variedad de factores que aprovechan las vulnerabilidades para provocar interrupciones, pérdidas de datos y daños a la reputación. Entre los autores de estas amenazas pueden figurar empleados, contratistas, activistas, delincuentes y Estados hostiles que actúan de forma maliciosa o por negligencia. Esto pone de relieve la necesidad fundamental de contar con programas eficaces contra las amenazas internas, controles de acceso y una supervisión continua de la seguridad en 2026.

La perspectiva general de amenazas para el sector de la defensa y la aeronáutica en 2026 es moderada, impulsada por una combinación de riesgos elevados de protestas y disturbios y amenazas de seguridad corporativa intensificadas, mientras que la exposición a la delincuencia y el terrorismo sigue siendo moderada, aunque persistente. Es probable que los actores maliciosos y los incidentes de seguridad a nivel mundial afecten a las operaciones, la seguridad del personal y la reputación de la marca, con efectos que variarán en función de la exposición geográfica y sectorial. De cara al futuro, es muy probable que la próxima crisis a nivel sectorial en el sector de la defensa y la aeronáutica tenga su origen en focos de tensión geopolítica o en la reanudación de conflictos, en un contexto de presiones continuas, como el cambio climático y la polarización política, que generan vulnerabilidades adicionales. Las organizaciones que invierten en sistemas de alerta temprana, resiliencia y seguridad integrada entre dominios están mejor posicionadas para mantener la ventaja en la toma de decisiones en este entorno cada vez más competitivo.

Áreas de mayor riesgo

Manifestaciones y disturbios

NIVEL 4

Delincuencia y seguridad

NIVEL 3

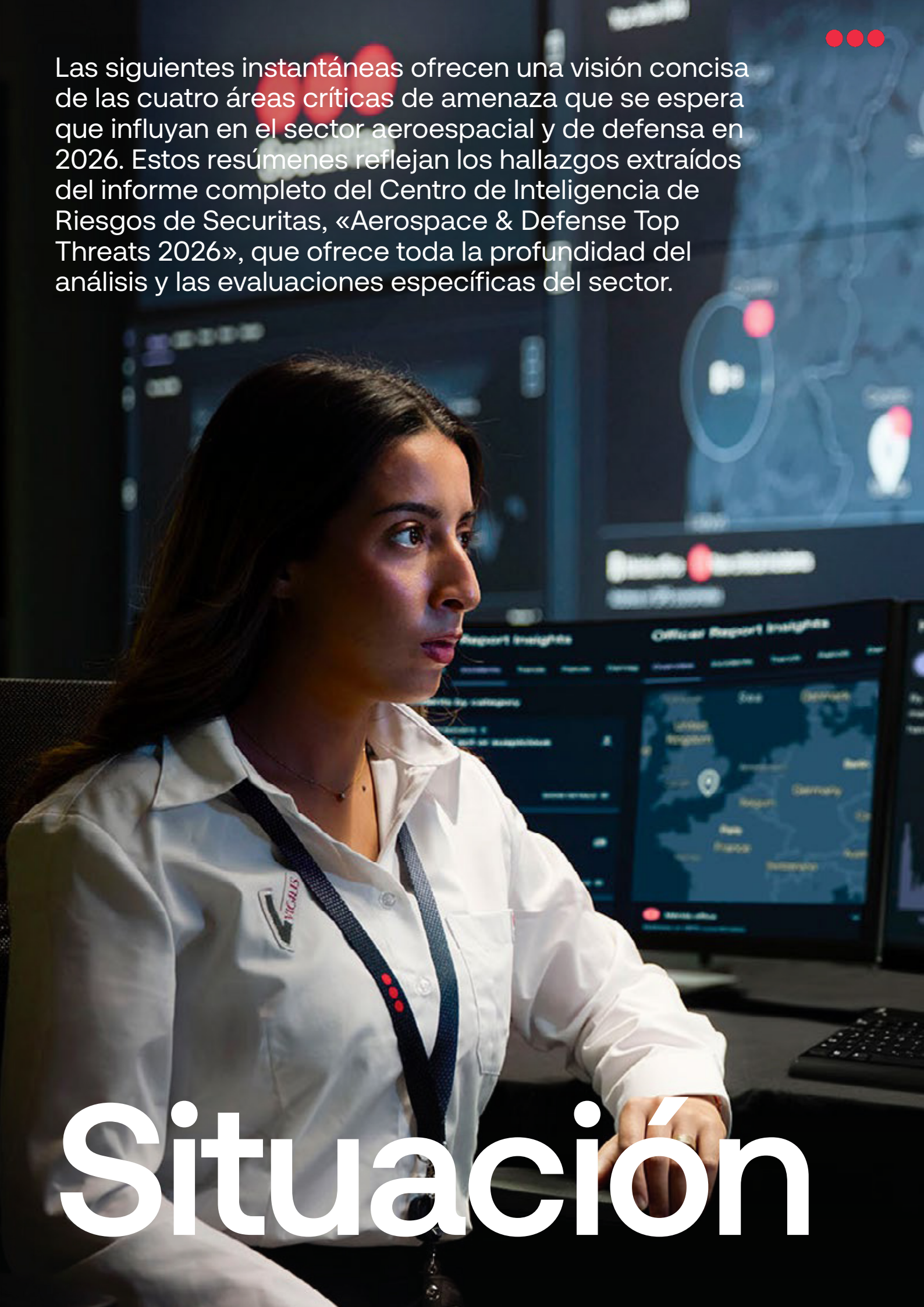
Seguridad corporativa

NIVEL 4

Terrorismo y extremismo

NIVEL 3

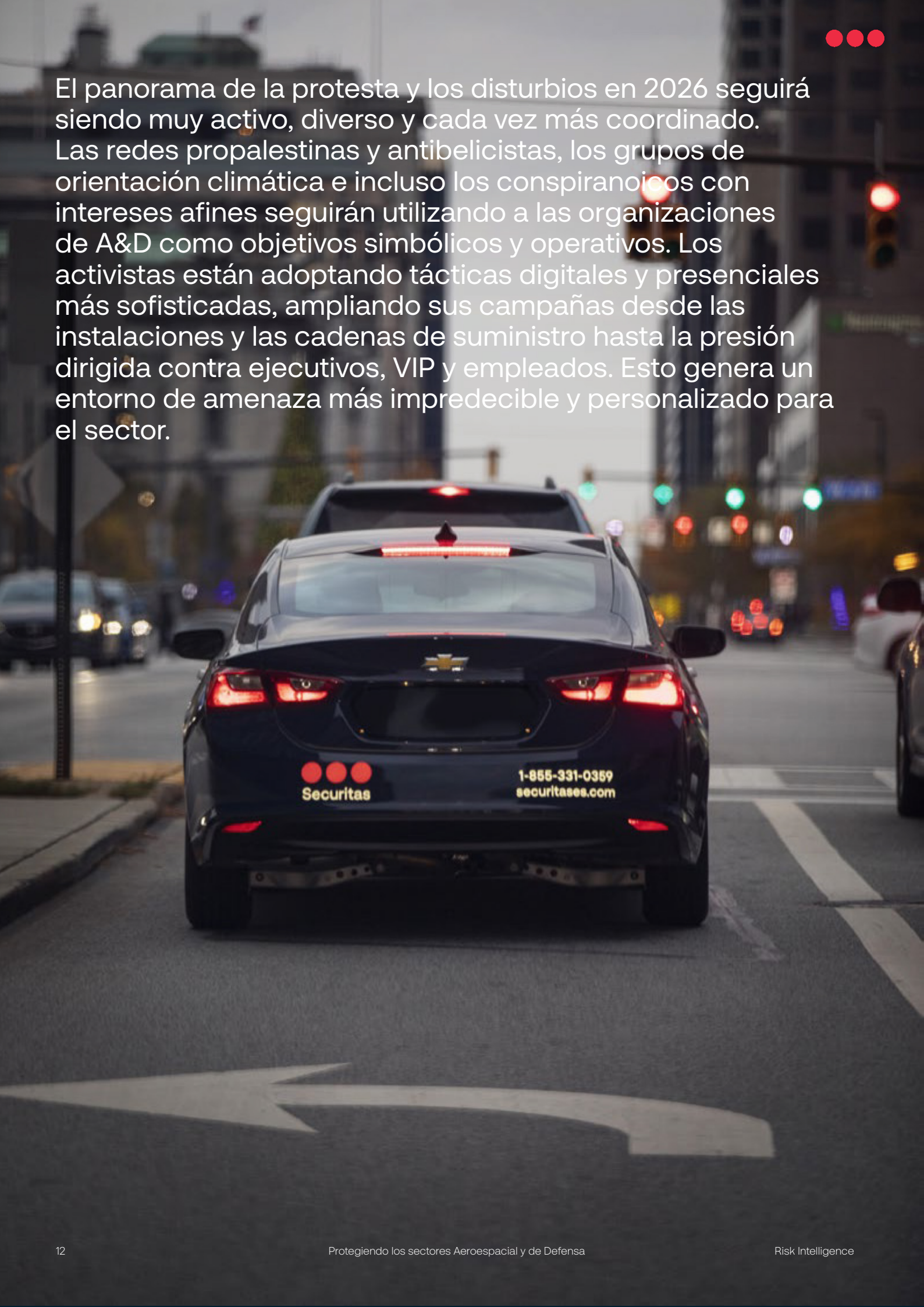
Las siguientes instantáneas ofrecen una visión concisa de las cuatro áreas críticas de amenaza que se espera que influyan en el sector aeroespacial y de defensa en 2026. Estos resúmenes reflejan los hallazgos extraídos del informe completo del Centro de Inteligencia de Riesgos de Securitas, «Aerospace & Defense Top Threats 2026», que ofrece toda la profundidad del análisis y las evaluaciones específicas del sector.



Situación


Historical event pattern
Burglary
Trespassing
Intelligence briefs

El panorama de la protesta y los disturbios en 2026 seguirá siendo muy activo, diverso y cada vez más coordinado. Las redes propalestinas y antibelicistas, los grupos de orientación climática e incluso los conspiranoicos con intereses afines seguirán utilizando a las organizaciones de A&D 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 contra ejecutivos, VIP y empleados. Esto genera un entorno de amenaza más impredecible y personalizado para el sector.



Protestas y disturbios

Protestas y disturbios

Evaluación de la amenaza

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

MLCOA: los activistas mantienen protestas frecuentes, movilización en línea y disrupciones dirigidas contra organizaciones de A&D, ampliando la presión a ejecutivos, miembros del consejo y empleados. Aumenta la visibilidad en torno a domicilios, eventos y campus, y la mayoría de las interacciones siguen siendo no violentas, aunque disruptivas. MDCOA: campañas coordinadas de acción directa en múltiples emplazamientos provocan una disrupción operativa importante, con un acoso dirigido que escala hasta confrontaciones agresivas en domicilios o lugares de trabajo. No pueden descartarse riesgos aislados de violencia, coacción 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 A&D.
- Las redes activistas atacan a empresas y proveedores percibidos como vinculados a programas de defensa, coordinando a menudo acciones transfronterizas.
- Las tácticas incluyen bloqueos de instalaciones, disrupciones en la cadena de suministro, interferencia en grandes eventos y campañas coordinadas de presión digital.
- Los nuevos grupos activistas adoptan tácticas, técnicas y procedimientos (TTP) cada vez más disruptivos, pese a las restricciones impuestas por las autoridades.

2 Focalización en ejecutivos, VIP y empleados

- Los ejecutivos y altos cargos son objeto creciente de doxing, comunicaciones hostiles, medios sintéticos, cartas abiertas y campañas en redes sociales.
- Aumenta la focalización en domicilios: los activistas emplean información de acceso público para mapear direcciones particulares y rutinas personales.
- Se filma, identifica y señala públicamente en línea a empleados en los accesos de las instalaciones, lo que genera problemas reputacionales y de seguridad personal.
- Los activistas también recurren a la «focalización relacional», aprovechando los cargos en consejos, las afiliaciones universitarias o las alianzas de un directivo para ejercer presión.

3 Activismo estudiantil y presión universitaria

- Los grupos estudiantiles continúan con protestas dirigidas contra los vínculos universitarios con empresas de A&D, perturbando eventos de captación y alianzas de investigación.
- Las acampadas, el despliegue de pancartas y las acciones coordinadas en los campus persisten, presionando a las universidades para que reconsideren su colaboración con organizaciones de defensa.

4 Convergencia del activismo medioambiental con las narrativas antibelicistas

- Las organizaciones aeroespaciales y de defensa siguen siendo objetivos destacados del activismo climático.
- Grupos como Extinction Rebellion (XR) y los afiliados a A22 se centran en ferias aéreas, eventos de gran visibilidad y activos asociados a emisiones o impacto medioambiental.
- La creciente convergencia entre el activismo climático, el antibelicismo y las narrativas anticorporativas amplifica los niveles de amenaza y amplía el abanico de posibles objetivos.

Acciones

- **Reducir la visibilidad de la información** de ejecutivos y empleados en fuentes abiertas, garantizando una monitorización proactiva frente al doxing, la suplantación de identidad y el reconocimiento hostil.
- **Prepararse para la movilización** entre acciones en torno a eventos sectoriales clave, focos geopolíticos y ciclos de contratación que puedan actuar como catalizadores de protestas o campañas dirigidas.
- **Reforzar los planes de respuesta** basados en escenarios ante protestas pacíficas, acoso dirigido, disrupciones en la cadena de suministro y acciones coordinadas en múltiples emplazamientos, integrando los equipos de seguridad física, RR. HH., comunicación y jurídico.

La delincuencia seguirá siendo una amenaza persistente para las organizaciones de A&D a lo largo de 2026, impulsada por las tensiones geopolíticas, las presiones económicas y la presión continuada sobre las cadenas de suministro globales. El elevado valor de los productos del sector, los materiales sensibles y la información propietaria incrementa la exposición al robo, el sabotaje, la adquisición ilícita y la facilitación delictiva. Los grupos de delincuencia organizada (OCG y los actores alineados con Estados seguirán explotando las brechas en la verificación de proveedores y las redes logísticas, traficando con componentes críticos a través de mercados grises y negros. A medida que se intensifican las presiones de producción, las organizaciones afrontan un riesgo creciente de que piezas falsificadas o robadas se infiltren en cadenas de suministro legítimas.

Las ciberamenazas también se intensificarán: actores respaldados por Estados y con motivación económica perfeccionarán el espionaje, la exfiltración de datos y las operaciones de suplantación habilitadas por IA. La exposición de los ejecutivos, la manipulación mediante medios sintéticos y la focalización híbrida digital/física seguirán ampliando la superficie de ataque, lo que subraya la necesidad de una seguridad ciber-física integrada.

Delicuencia y seguridad

Evaluación de la amenaza

Most likely (MLCOA) vs Most dangerous course of action (MDCOA)Curso de acción más probable (MLCOA) frente a curso de acción más peligroso (MDCOA).

NIVEL 3

MLCOA: los actores delictivos siguen atacando las cadenas de suministro de A&D con robos recurrentes de materiales, piezas y componentes menores. Los artículos robados o reutilizados afloran en mercados ilícitos, aumentando el riesgo de contaminación de las cadenas de suministro. Los ciberdelincuentes mantienen una presión constante con fines económicos y de robo de datos.
MDCOA: una campaña delictiva a gran escala —potencialmente respaldada por Estados adversarios— ataca la cadena de suministro de A&D mediante robo, sabotaje y adquisición ilícita. La disrupción obliga a recurrir a proveedores no autorizados, introduciendo componentes peligrosos en los procesos de producción y afectando a la seguridad y a la producción.

Dinámicas clave

1 Adquisición ilícita y vulnerabilidades de la cadena de

- Los OCG siguen siendo los principales facilitadores del robo, la desviación y la adquisición encubierta de componentes para Estados sancionados, incluidos Rusia, Irán y China.
- Aviónica, sensores, placas de circuitos y componentes de precisión robados se trafican a través de mercados grises y negros a precios inflados.
- La escasez de suministros y los cuellos de botella en la producción aumentan los incentivos para obtener componentes no verificados, elevando los riesgos de contaminación.
- Se siguen explotando los puntos débiles en el transporte de mercancías, la verificación de proveedores y el cumplimiento transfronterizo.

2 OCGProfundización de la colaboración entre OCG y EstadosState Collaboration Deepening

- Las sanciones y los controles de exportación aceleran la colaboración entre Estados adversarios y OCG que buscan piezas restringidas.
- Los grupos delictivos aprovechan corredores de contrabando consolidados, sociedades pantalla e intermediarios logísticos perfeccionados durante las recientes disrupciones geopolíticas.
- Dado que los grandes conjuntos siguen siendo difíciles de robar, la atención se desplaza hacia componentes más pequeños y de alto valor, así como hacia objetivos más lucrativos y accesibles.

3 Escalada del ciberespionaje y la intrusión habilitada por IA

- Actores cibernéticos respaldados por Estados y criminales perfeccionan las operaciones de espionaje, robo de credenciales y exfiltración de datos contra las redes de A&D.
- La suplantación habilitada por IA, el audio/vídeo sintético y los documentos deepfake aumentan el engaño y reducen las barreras de detección.
- En 2025 se registraron múltiples campañas sostenidas, incluidos ciberataques a importantes empresas israelíes de A&D y espionaje continuado por parte de actores respaldados por Rusia.
- El phishing y el compromiso a través de proveedores o prestadores de servicios más pequeños siguen siendo vías clave de acceso a programas de alto valor.

4 Creciente focalización en ejecutivos y personas sensibles

- La exposición de información personal alimenta el doxing, la intimidación y la presión híbrida digital-física.
- Las bases de datos públicas y las filtraciones de datos personales (PII) reducen las barreras para que los adversarios identifiquen y rastreen a los ejecutivos.
- En 2025 se observó una escalada en la severidad de las acciones dirigidas contra ejecutivos, desde amenazas en línea hasta intentos de secuestro, sabotaje de propiedades y complots de asesinato vinculados a Estados.
- Los medios sintéticos, las narrativas manipuladas y la suplantación cibernética personalizada intensifican los riesgos reputacionales y de seguridad.

Acciones

- **Reforzar la verificación y el escrutinio de proveedores en todos los niveles,** priorizando los controles que impidan la entrada de componentes falsificados, robados o ilícitos en la cadena de suministro.Implantar estrategias de seguridad ciber-física integradas que aborden el espionaje, el sabotaje, la suplantación sintética, la exposición de ejecutivos y las vías de amenaza híbridas.
- **Realizar evaluaciones específicas** de los actores de amenaza probables (OCG, redes alineadas con Estados, personal interno descontento) para identificar vulnerabilidades en logística, personal y sistemas digitales.
- **Desarrollar, probar y actualizar periódicamente los planes de respuesta a incidentes** —incluidas intrusiones cibernéticas, compromisos de la cadena de suministro y la focalización en ejecutivos—, respaldados por ejercicios interfuncionales.

Los riesgos de seguridad corporativa para las organizaciones de A&D se intensificarán en 2026 a medida que las amenazas internas, el espionaje corporativo, la acción encubierta hostil, la actividad de reconocimiento y la transferencia de activos sensibles se entrecruzan con unas tensiones geopolíticas elevadas y un entorno sociopolítico profundamente polarizado. Los actores de amenaza —entre ellos empleados, contratistas, activistas, delincuentes, auditores y grupos alineados con Estados— continúan explotando vulnerabilidades en los dominios físico, digital y humano, dificultando las capacidades de detección y respuesta y aumentando el riesgo de disrupción operativa, reputacional y estratégica.

Seguridad corporativa

Seguridad corporativa

Evalucación de la amenaza

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

MLCOA: las organizaciones afrontan la divulgación accidental o malintencionada continua de información sensible, el uso indebido de bajo nivel por parte de personal interno, el reconocimiento oportunista y los intentos sostenidos de espionaje mediante ingeniería social, robo de credenciales, actividad con drones e infiltración presencial. La mayor polarización ideológica contribuye a más riesgos internos motivados por agravios, y la actividad hostil rutinaria pone a prueba la postura de seguridad en instalaciones corporativas y cadenas de suministro. MDCOA: actores estatales e híbridos intensifican campañas coordinadas que implican reclutamiento de personal interno, sabotaje, espionaje complejo, reconocimiento mediante drones y explotación de relaciones con terceros para acceder a activos sensibles o desviarlos. Personal interno malicioso exfiltra datos valiosos o facilita ataques posteriores, mientras adversarios sofisticados emplean el reconocimiento y la acción encubierta para perturbar operaciones, comprometer cadenas de suministro o infligir daños reputacionales y legales.

Dinámicas clave

1 Aumento de las amenazas internas

- Las amenazas internas abarcan a empleados, contratistas, visitantes y socios externos, que actúan de forma maliciosa en entornos físicos y digitales.
- Las motivaciones incluyen presión económica, agravios ideológicos, circunstancias personales, coacción, búsqueda de notoriedad o explotación por parte de actores hostiles.
- Las filtraciones de información sensible a través de herramientas de IA o redes sociales generan exposición operativa, legal y reputacional.
- Casos destacados de 2025 evidencian el robo de secretos comerciales y su exfiltración para programas de inteligencia extranjeros.
- Entre los indicadores de actividad maliciosa figuran las infracciones de seguridad repetidas, los intentos de acceso inexplicables y patrones de dimisión temprana.

2 Ampliación de la exposición al espionaje corporativo

- La creciente competencia geopolítica incrementa el espionaje dirigido a datos de I+D, propiedad intelectual y tecnologías de doble uso.
- Los actores respaldados por Estados explotan intrusiones cibernéticas, ingeniería social, visitas de dignatarios extranjeros y el acceso de personal interno para obtener información confidencial.
- Las organizaciones implicadas en programas de contratación, investigación sensible o contratos gubernamentales son objeto de una focalización más intensa.
- Los acontecimientos de 2025 ponen de manifiesto la amplitud de las tácticas de los adversarios.
- Las campañas de espionaje respaldan operaciones posteriores, incluida la manipulación de información, el ransomware o la actividad coordinada en entornos complejos.

3 Aumento de la frecuencia del sabotaje y la acción encubierta hostil

- Actores estatales y no estatales realizan actividad encubierta, poniendo a prueba las capacidades de detección y respuesta.
- Las amenazas incluyen incendios provocados, reconocimiento con drones, paquetes bomba, manipulación de cables submarinos, guerra electrónica y amenazas de bomba falsas.
- Las tácticas híbridas se dirigen a instalaciones militares, nodos de transporte, infraestructuras logísticas, plantas de ensamblaje y emplazamientos de doble uso.
- Numerosos incidentes de 2024-2025 en toda Europa evidencian drones sobrevolando instalaciones nucleares, trenes de munición, instalaciones navales e infraestructuras de doble uso.
- La externalización de la acción encubierta aumenta la negación plausible, pero también eleva la imprevisibilidad y el riesgo de escalada.

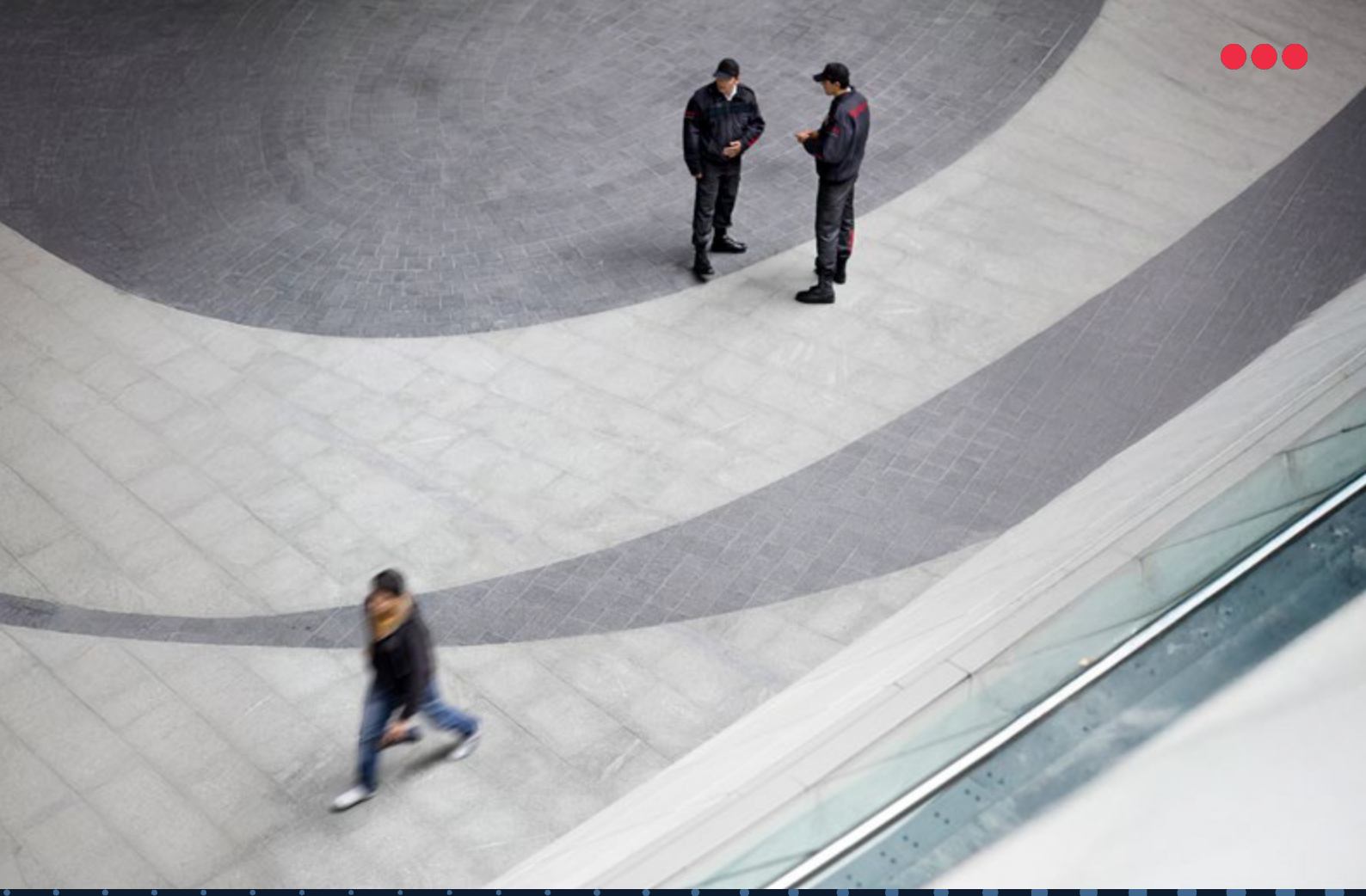
4 Reconocimiento hostil y desafíos de la auditoría de seguridad

- Los auditores de seguridad siguen filmando instalaciones de forma abierta para generar interacción en línea, revelando información e indicadores críticos (puntos de acceso, cobertura de CCTV, códigos, datos de empleados).
- El reconocimiento encubierto mediante drones, dispositivos camuflados o visitas repetidas proporciona inteligencia de segunda mano a activistas, delincuentes y actores respaldados por Estados.
- Los auditores seguirán aprovechando los derechos de acceso a terrenos públicos, generando riesgos reputacionales para las organizaciones objetivo derivados de una mala gestión de las interacciones con el personal de seguridad.
- El reconocimiento mediante drones en emplazamientos sensibles sigue aumentando, frecuentemente vinculado a intereses de inteligencia extranjera.

Acciones

- Reforzar los programas frente a amenazas internas mediante indicadores conductuales, monitorización de fuentes abiertas e integración entre RR. HH., ciberseguridad y seguridad física.
- Mejorar los controles sobre el manejo de información sensible, los procesos de desvinculación y el acceso privilegiado de empleados, contratistas y socios.
- Ampliar la formación en contraespionaje y OPSEC, especialmente para los equipos implicados en I+D, contratación, proyectos sensibles y delegaciones extranjeras.
- Actualizar los planes de gestión de crisis y respuesta a incidentes para incluir el sabotaje, la acción encubierta, las incursiones de drones, las brechas facilitadas por personal interno y los eventos de reconocimiento.
- Mejorar la transparencia de la cadena de suministro, el cumplimiento de sanciones y la monitorización de socios externos, incluidas la diligencia debida y el rastreo de activos.
- Formar al personal de primera línea y a los equipos de seguridad para gestionar adecuadamente a auditores y al reconocimiento hostil, evitando la escalada y protegiendo la información sensible.

El terrorismo y el extremismo seguirán siendo consideraciones persistentes para las organizaciones aeroespaciales y de defensa en 2026, impulsados por los focos de conflicto globales, los agravios ideológicos en evolución y las dinámicas de radicalización en curso. Aunque por el momento no hay indicios de un aumento de la focalización directa sobre el sector, los riesgos indirectos derivados de la inestabilidad regional, la exposición de la cadena de suministro, las amenazas falsas y el desorden informativo siguen siendo significativos. Los extremistas violentos domésticos (DVE), los terroristas autoiniciados (S-IT) y los grupos activos a escala internacional continúan adaptándose, con cambios legales y narrativas en línea que influyen en su comportamiento en múltiples jurisdicciones.



Terrorismo y extremismo

Evaluación de la amenaza

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

MLCOA: no hay indicios claros de un aumento de la focalización directa sobre las organizaciones de A&D. No obstante, los incidentes terroristas que afectan a las cadenas de suministro, en particular en regiones de alto riesgo con conflictos activos o tensión geopolítica, siguen siendo una posibilidad realista. MDCOA: las percepciones de implicación del sector A&D en conflictos globales generan ataques dirigidos contra empresas, instalaciones o cadenas de suministro. El desorden informativo, las críticas al sector y los focos geopolíticos convergen con agravios personales, alimentando la radicalización entre extremistas violentos domésticos (DVE), terroristas autoiniciados (S-IT) y grupos terroristas consolidados.

Dinámicas clave

1 Evolución de las motivaciones asociadas al DVE/S-IT

- Las motivaciones extremistas incluyen ideologías de extrema derecha, extrema izquierda, de carácter racial o étnico, antiautoridad y antitecnología.
- Los agravios o resentimientos personales se entrelazan cada vez más con narrativas geopolíticas amplificadas a través de las redes sociales.
- Los procesos de radicalización se aceleran mediante las plataformas en línea, a pesar del aumento de la prohibición y restricción de las redes extremistas.

2 Nuevas designaciones legales que configuran el panorama de amenazas

- La designación de nuevos grupos que anteriormente se consideraban redes de activistas o de delincuencia común actúa como elemento disuasorio para parte de su actividad.
- Las restricciones impuestas y las acciones dirigidas contra estos grupos pueden llevar a sus miembros más comprometidos a operar de forma clandestina, reforzando sus medidas de seguridad operativa (OPSEC) y/o cambiando de identidad o reubicándose para evitar ser detectados o perseguidos.
- La percepción pública de que las medidas adoptadas contra grupos activistas son excesivamente severas puede generar una reacción negativa, con el consiguiente riesgo de aumentar involuntariamente el apoyo social al grupo y a sus reivindicaciones.

3 Ataques mediante engaños (hoaxes) y acciones disruptivas

- Las empresas del sector A&D (Aeroespacial y Defensa) siguen siendo vulnerables a comunicaciones maliciosas, falsas amenazas de bomba y falsas alarmas destinadas a interrumpir sus operaciones.
- Estas acciones suelen tener como objetivo provocar una respuesta, poner a prueba las medidas de seguridad u obtener información sobre los
- Las actividades de engaño (hoaxes) se utilizan cada vez más para evaluar la capacidad de respuesta de las organizaciones y facilitar labores de reconocimiento e inteligencia previa sobre los

4 Amenazas indirectas derivadas de las zonas de conflicto global

- Los incidentes terroristas en regiones con una elevada tensión geopolítica plantean riesgos indirectos para las cadenas de suministro, la logística y el personal.
- Los gobiernos occidentales continúan advirtiendo de que es probable que se produzcan atentados terroristas a corto plazo, aunque no estén dirigidos específicamente contra el sector de la Aeroespacial y Defensa (A&D).

Acciones

- Realizar evaluaciones de amenazas, vulnerabilidades y riesgos (TVRA) específicas de cada emplazamiento y evaluaciones de amenazas por proximidad, centradas en las instalaciones situadas cerca de focos geopolíticos o nodos logísticos clave.
- Reforzar los planes de continuidad de negocio y gestión de crisis, garantizando su alineación con las directrices nacionales de contraterrorismo y los programas de concienciación de los empleados.

Contacto

Inteligencia@securitas.es