

De la Intuición del Café al desastre en las Entidades Críticas Aeroportuarias

Disclaimer 1

Sobre la naturaleza de la información y la protección de contenidos reservados

El contenido del presente artículo se fundamenta exclusivamente en fuentes abiertas, públicas y legalmente accesibles, tales como normativa publicada en diarios oficiales, documentación técnica y divulgativa de organismos internacionales, información proporcionada por fabricantes de equipos de seguridad, comunicaciones institucionales y referencias disponibles en repositorios oficiales y medios de acceso general.

En ningún caso se reproducen, citan o describen procedimientos operativos internos, protocolos específicos, metodologías detalladas, configuraciones técnicas, niveles de inspección, parámetros de funcionamiento o contenidos pertenecientes a la parte clasificada o restringida del Programa Nacional de Seguridad para la Aviación Civil (PNS/PNSAC) ni de ningún otro documento sometido a reserva, confidencialidad o difusión limitada.

Las descripciones incluidas tienen un carácter general, conceptual y no operativo, y se orientan exclusivamente a contextualizar el marco normativo, la arquitectura funcional de los sistemas de seguridad y los principios organizativos aplicables a infraestructuras críticas y entornos aeroportuarios. No se aporta información sensible que pueda comprometer la seguridad de la aviación civil, la integridad de los sistemas AVSEC, la protección de infraestructuras críticas o la eficacia de los dispositivos de seguridad.

Cualquier referencia a tecnologías, fases de inspección, capacidades de los sistemas SIEB/SATE, equipos de rayos X (RX), sistemas de tomografía computarizada (CT/EDS) u otros medios técnicos se basa únicamente en información divulgada en fuentes abiertas y no implica, en ningún caso, la revelación de configuraciones concretas, criterios de decisión, umbrales de alarma, procedimientos internos ni elementos sujetos a clasificación.

El presente artículo tiene un propósito estrictamente informativo y divulgativo. No interpreta, modifica ni sustituye las obligaciones legales, técnicas u operativas establecidas por la normativa vigente, por el PNS/PNSAC ni por cualesquiera otros documentos oficiales, públicos o reservados, que prevalecen en todo caso sobre cualquier consideración aquí expuesta.

Disclaimer 2

Sobre los límites de actuación del personal y el marco competencial

Este artículo no pretende cuestionar la labor de los responsables de equipo ni de los inspectores que, dentro de su marco legal y funcional, desempeñan correctamente sus tareas de supervisión y apoyo. Su contribución resulta esencial siempre que no adopten decisiones técnico-operativas ni asuman funciones reservadas a personal debidamente habilitado conforme a la normativa de seguridad privada y de protección de infraestructuras críticas.

Cuando un profesional ocupa un punto estratégico dentro del dispositivo de seguridad, resulta imprescindible delimitar con precisión el alcance de sus actuaciones. Toda decisión con impacto técnico, legal u operativo debe estar recogida en las órdenes de puesto, en las Instrucciones Técnicas Operativas (ITOs) o ser emitida por personal habilitado por el Ministerio del Interior o, en su caso, contar con una delegación formal de funciones otorgada por el jefe o director de seguridad de la organización, en los términos previstos por la legislación aplicable.

Esta delimitación garantiza que:

- ✓ La actuación del personal se ajusta al marco normativo, evitando responsabilidades administrativas, civiles o penales derivadas de decisiones no autorizadas o adoptadas fuera de competencia.
- ✓ Las infraestructuras y las personas quedan protegidas frente a riesgos operativos que requieren criterios técnicos específicos y habilitación profesional adecuada.
- ✓ La cadena de mando se mantiene clara, coherente y trazable, asegurando que cada decisión técnica-operativa pueda ser auditada, documentada y, en su caso, depurada conforme a la normativa vigente.

El objetivo es diferenciar nítidamente la supervisión operativa de la toma de decisiones técnico-legales, de modo que cada intervención cuente con respaldo normativo, habilitación exigible o delegación expresa, evitando cualquier forma de improvisación competencial que pueda comprometer la seguridad, la resiliencia del sistema o la responsabilidad jurídica del personal y de las entidades implicadas.

Introducción

La seguridad en infraestructuras críticas no es un juego de mesas redondas ni un laboratorio de buenas intenciones. Es un entramado jurídico y técnico operativo que exige precisión, competencias definidas y respeto estricto a la ley. La Ley 5/2014 de Seguridad Privada (España, 2014) no es un adorno. Establece quién puede hacer qué, y con qué responsabilidades, porque la improvisación jerárquica no es creatividad, es un riesgo añadido.

Pero en el ámbito de infraestructuras críticas, el marco no se agota en la seguridad privada. La protección de servicios esenciales está estructurada además por la Ley 8/2011, de 28 de abril, de protección de infraestructuras críticas, desarrollada por el Real Decreto 704/2011, y hoy reforzada por la Directiva (UE) 2022/2557 (Directiva CER), que impone obligaciones de resiliencia, análisis de riesgos y coordinación permanente con las autoridades competentes. La habilitación individual no es solo un requisito profesional, es una pieza clave dentro de un sistema nacional y europeo de resiliencia.

En este marco, el personal habilitado no es un extra decorativo. Cada nivel (vigilantes, jefes y directores de seguridad) tienen sus distintas funciones legales y competencias claras, y el sistema depende de que se cumplan. La seguridad pública retiene la autoridad coercitiva, mientras que la privada opera dentro de su perímetro competencial, un equilibrio delicado que cualquier intromisión sin habilitación puede romper.

La verdadera ironía de la seguridad es que cumplir la ley y seguir protocolos no se ve como virtud, sino como obstáculo por quienes no entienden que la competencia no es opcional, es la única garantía de que el sistema funcione y de que no haya víctimas por decisiones improvisadas. La seguridad no se improvisa, la ley se cumple, y quienes ignoran los límites establecidos arriesgan mucho más que su reputación, ponen en juego la integridad de todo el sistema que se supone, han de proteger.

1. Marco normativo:

Existe un principio de reserva funcional tan elemental que debería ser tan evidente como el aire, solo quien está habilitado puede ejercer las funciones que la ley le atribuye.

La Ley 8/2011 introduce un principio complementario. La seguridad de infraestructuras críticas es una responsabilidad compartida entre operadores críticos y Estado, bajo un sistema de planificación estructurado (Planes de Seguridad del Operador, Planes de Protección Específicos y Planes de Apoyo Operativo). Esto implica que cualquier desviación competencial no afecta solo a una empresa, conculca un engranaje coordinado a nivel nacional.

Nada de “responsables de equipo con criterio propio” ni de “inspectores intuitivos”, salvo con delegación de funciones, porque sin habilitación, no hay competencia legal que

valga. Seamos claros, en ocasiones incluso con habilitación la competencia puede brillar por su ausencia. (véase *disclaimer* 2).

Cuando se invade una competencia reservada no solo se incumple la Ley 5/2014, se altera la arquitectura prevista en el Real Decreto 704/2011, que articula la relación entre operadores y Fuerzas y Cuerpos de Seguridad del Estado, Secretaría de Estado de Seguridad y el CNPIC. La improvisación no rompe únicamente la jerarquía interna, compromete la coherencia del sistema de Protección de Infraestructuras Críticas (PIC), en su conjunto.

1.1. La jerarquía

El sistema distingue tres perfiles legales claves para la estructura técnico-operativa, aunque la Ley 5/2014 reconoce otras categorías profesionales: escoltas, guardas rurales, guardas de caza y pesca, y detectives privados. Estas figuras tienen competencias específicas dentro de su ámbito, pero no sustituyen ni desplazan la jerarquía de decisión central.

- ✓ Vigilante de seguridad (art. 32): la primera línea de defensa. Detecta, verifica y ejecuta protocolos. No decide; cumple. Cualquier intento de innovar por iniciativa propia constituye un riesgo certificado, solo en determinadas situaciones, en base a su formación y experiencia y en una situación sobrevenida ha de actuar si la actuación no está planificada o prevista, con lo que la responsabilidad sería exigible al jefe o al director de seguridad.
- ✓ Jefe de seguridad (art. 35): organiza, supervisa y coordina. Garantiza coherencia técnica y operativa; cualquier desviación sin habilitación es un acto de teatro de guiñol peligroso.
- ✓ Director de seguridad (art. 36): la mente estratégica. Si el departamento está legalmente constituido, absorbe la mayoría de las funciones del jefe de seguridad además de las suyas propias. Traducido: si hay director, el jefe no puede inventarse atajos ni interpretaciones creativas.

El resto de los “responsables” o “inspectores” que pululan en muchas empresas son figurantes laborales; cualquier intento de asumir funciones reservadas es ilegal y peligroso. La ley no los reconoce, y los tribunales tampoco lo permiten (Audiencia Provincial de Madrid, 2018).

Incluso dentro de las otras categorías habilitadas, como escoltas o detectives privados, sus competencias están delimitadas por la ley y no incluyen funciones de supervisión ni coordinación general de servicios de seguridad privada. Ignorar esto no solo es una improvisación, es una gentil invitación directa a la responsabilidad administrativa, civil, e incluso penal.

Porque actuar fuera de la habilitación no es un “error creativo”: es jugar con la posibilidad de acabar con penas privativas de libertad y la inhabilitación especial que te impediría volver a ejercer tu profesión.

La Ley 5/2014 no es flexible. Reconocer otras categorías profesionales no es un salvoconducto para saltarse la jerarquía; la habilitación es el único pasaporte válido para tomar decisiones críticas en seguridad privada. Saltarse este principio no demuestra iniciativa ni valentía: demuestra desconocimiento o desprecio del sistema que mantiene viva la integridad operativa.

2. La ironía de la improvisación

Lo más jugoso, y trágicamente previsible, es que, a pesar de la claridad normativa, siempre surgen quienes creen que la habilitación es un simple adorno.

Los llamados “mandos” entre comillas, autodenominados jefes de equipo (en puridad y desde el rigor responsables), o inspectores de servicios vacíos de competencias y delegación formal deciden quién pasa, dónde te colocas, si rechazas una maleta sospechosa, si permites el acceso de alguien sin documentación, quién sube o baja por la cinta, o incluso qué objetos pueden ser trasladados entre zonas críticas, sin que la ley les otorgue autoridad alguna para tomar tales decisiones. Mandos que, en realidad, no tienen potestad para decidir sobre ninguna función reservada; solo se les reconoce la apariencia jerárquica.

Esas conductas pueden constituir intrusismo profesional (art. 403 CP) o, con mayor frecuencia, infracciones muy graves tipificadas en la Ley 5/2014 (art. 58 y ss.) con sanciones administrativas elevadas y posible vía penal accesorio. (España, 1995, art. 403). Pero en infraestructuras críticas el problema no es solo penal individual.

La Directiva CER (UE 2022/2557) obliga a los Estados miembros a garantizar que las entidades críticas puedan prevenir, resistir, absorber y recuperarse de incidentes graves. Cuando un “mando” informal altera protocolos, no solo asume un riesgo jurídico personal: debilita la capacidad de resiliencia exigida por el Derecho de la Unión Europea.

Para quienes todavía necesitan un sutil recordatorio, la famosa sala de fiestas, con su estricta acústica y régimen de ocupación, no es una metáfora abstracta; es la consecuencia tangible de confundir autoridad informal con potestad legal.

Aquí hay un matiz esencial que muchos ignoran, la habilitación no es suficiente por sí sola. En un mundo donde los riesgos cambian de un momento a otro, la seguridad exige formación permanente, actualización constante y dominio práctico de los procedimientos. La resiliencia no se construye con intuiciones ni con jerarquías aparentes, sino con competencias acreditadas, procedimientos auditables y trazabilidad, tal como exige el marco PIC y la normativa europea.

La autoridad del mando no se ejerce únicamente por la habilitación, sino que se consolida mediante experiencia, formación continua y liderazgo efectivo que guía, respalda y protege al operador diligente. Ignorar esta cuestión convierte cualquier título en un adorno, y cualquier decisión improvisada en un acto de riesgo.

Pero aquí radica la ironía más cruda y operativa. No es la multa ni la amenaza penal lo que destruye el sistema, sino la fractura profesional en el desempeño de las funciones operativas y cultural que generan estos “mandos”. La cadena de mando se resquebraja, los vigilantes legítimos reciben mensajes contradictorios y la desviación se normaliza como rutina diaria cronificándose.

Hoy se deja pasar un objeto dudoso “porque nunca pasa nada”; mañana, alguien confía su vida y la de terceros a la improvisación de quien carece de habilitación, formación o experiencia suficiente. La ironía no es literatura para recrearnos, sin duda es operativa, corrosiva y potencialmente letal.

La jerarquía técnica, la habilitación y la formación continua no son ornamentos de oficina ni títulos de conveniencia. Son garantías de profesionalidad, seguridad y legalidad. Ignorarlas no es “mostrar iniciativa”; es desobedecer la arquitectura que mantiene viva la integridad del sistema.

En infraestructuras críticas, donde cada decisión repercute directamente sobre la seguridad de personas, instalaciones y servicios esenciales, la improvisación jerárquica no es valentía ni liderazgo visible, simplemente son riesgos añadidos, cuantificables y prevenibles.

Quien quiera liderar, que se habilite formalmente y mantenga actualización constante. Quien quiera innovar, que proponga protocolos dentro del marco legal y operativo existente. Todo lo demás es un lujo que ni el sistema ni la sociedad pueden permitirse, y cuya consecuencia puede ir más allá de una multa, inhabilitación profesional y eventuales responsabilidades jurídicas de mayor calado.

3. El paradigma aeroportuario: precisión normativa y ausencia de concesión ante la duda

La seguridad en la aviación civil no es un juego de buena voluntad ni de criterios subjetivos, es un sistema tan preciso como un reloj suizo y tan implacable como la lógica de un teorema, donde cualquier concesión ante la duda puede traducirse en consecuencias irreversibles.

La imagen de un objeto sospechoso no admite “premonición”. Confiar en la percepción subjetiva equivale a permitir que un aprendiz de astrónomo dicte las órbitas de satélites críticos. Más aún cuando quienes toman esas decisiones hace tiempo que no operan escáneres, han perdido la categoría C2 de AESA, o simplemente se encuentran

desentrenados en funciones que exceden lo que la Ley 5/2014 de Seguridad Privada y su normativa derivada les permite.

Bien sea por olvido, desentrenamiento o mera inercia profesional, con frecuencia la línea se cruza por desconocimiento, no por mala intención (a lo mejor en alguna ocasión); y en un entorno regulado, la ignorancia técnica no es un pecado inocuo, sino un riesgo con consecuencias potencialmente irreversibles.

El Reglamento (CE) n.º 300/2008 establece normas comunes de seguridad de la aviación civil, mientras que el Reglamento de Ejecución (UE) 2015/1998 desarrolla procedimientos detallados para su aplicación. Ambos textos incluyen, sin ambigüedad, armas de fuego, imitaciones y objetos susceptibles de convertirse en armas como artículos prohibidos en zonas restringidas y en cabina, salvo verificación física en condiciones controladas (UE, 2008; UE, 2015). Permitir interpretaciones discrecionales es tan absurdo como afinar un Stradivarius a oído en lugar de con un diapasón, un fallo puede resonar en cadena, afectando a toda la partitura que se instaura para dar protección.

En España, el Programa Nacional de Seguridad para la Aviación Civil (PNSAC) consolida este principio de “no concesión ante la duda”, aplicable a cualquier imagen obtenida mediante sistemas de RX o EDS que sugiera morfología compatible con un arma.

Esta directriz no es opcional, es un mandato legal, y su incumplimiento equivale a sustituir la precisión científica por la improvisación barroca. Se alinea con el Anexo 17 del Convenio de Chicago, que exige medidas preventivas basadas en la detección temprana y eliminación de riesgos antes del embarque (OACI, 2016).

En otras palabras, en el aeropuerto no hay espacio para las artes adivinatorias heroicas, ni para la estética de la improvisación, cada decisión debe ser replicable, trazable, técnica y jurídicamente irreprochable.

4. Arquitectura jurídica y funcional del aeropuerto: delimitación espacial, competencias y régimen de control

La seguridad aeroportuaria no opera en un espacio uniforme, sino en un entorno jurídicamente estratificado.

La delimitación de zonas en un aeropuerto no responde a criterios meramente arquitectónicos, sino a una clasificación funcional y normativa establecida en el Reglamento (CE) n.º 300/2008 del Parlamento Europeo y del Consejo y desarrollada por el Reglamento de Ejecución (UE) 2015/1998 de la Comisión, así como por el Programa Nacional de Seguridad para la Aviación Civil (PNSAC) en el ámbito español.

Esta zonificación determina el régimen de acceso, el tipo de control exigible y la competencia del personal actuante.

4.1. Zona pública o zona tierra (*landside*)

Es el espacio accesible al público general sin necesidad de someterse a controles de seguridad aeroportuaria en sentido estricto. Incluye vestíbulos, áreas de facturación, zonas comerciales abiertas y accesos exteriores.

En esta área pueden desarrollarse funciones de:

- ✓ Vigilancia general.
- ✓ Control de accesos administrativos.
- ✓ Prevención y respuesta ante incidentes ordinarios.

Sin embargo, no constituye zona restringida de seguridad conforme a la normativa europea. Por tanto, el régimen jurídico aplicable es distinto del que rige en zonas sometidas a inspección de seguridad.

4. 2. Zona aire (*airside*)

Comprende las áreas operativas del aeropuerto a las que solo se puede acceder tras superar los controles establecidos o mediante acreditación válida conforme a la normativa aplicable.

Dentro de la zona aire se distinguen categorías de especial relevancia:

a) Zonas restringidas de seguridad (ZRS)

Definidas por el Reglamento (CE) n.º 300/2008 como aquellas áreas en las que se aplican medidas específicas para proteger la aviación civil contra actos de interferencia ilícita.

El acceso exige:

- ✓ Control de seguridad previo (pasajeros, equipaje de mano, equipaje facturado, personal, mercancías o suministros).
- ✓ O acreditación específica sometida igualmente a verificación y control.

Las ZRS no son un concepto simbólico: activan un régimen reforzado de inspección, trazabilidad y supervisión.

b) Zonas críticas de las ZRS

Son subespacios dentro de las zonas restringidas donde la protección se intensifica debido a su proximidad a aeronaves, áreas de estacionamiento o infraestructuras esenciales.

En estas zonas, las medidas de control son más estrictas y el margen de discrecionalidad operativa es inexistente. La normativa europea exige que cualquier persona u objeto que acceda haya sido sometido a controles de seguridad adecuados y documentados.

4.3. Diferenciación técnica esencial

Una de las confusiones operativas más frecuentes (y jurídicamente más peligrosas) consiste en equiparar el control de accesos con el control de seguridad. Son figuras distintas, con naturaleza y finalidad diferentes.

a) Control de accesos

Tiene carácter administrativo y verificativo. Su finalidad es comprobar que la persona dispone de autorización válida para acceder a una determinada zona.

Incluye:

- ✓ Verificación de acreditación aeroportuaria.
- ✓ Comprobación de identidad.
- ✓ Validación de vigencia y nivel de autorización.

No implica evaluación técnica de amenazas ni análisis de objetos transportados. El hecho de disponer de acreditación válida no excluye la posibilidad (ni la obligación) de someterse a controles de seguridad adicionales cuando proceda conforme a la normativa.

b) Control de seguridad

Tiene carácter técnico-operativo y preventivo. Su finalidad es detectar objetos, sustancias o dispositivos prohibidos antes de su introducción en zonas restringidas o en aeronaves.

Incluye:

- ✓ Inspección mediante equipos de rayos X (RX), EDS, detectores de trazas de explosivos (ETD) u otros sistemas homologados.
- ✓ Registros o inspecciones manuales.
- ✓ Aplicación del principio de “no concesión ante la duda”.
- ✓ Procedimientos de verificación física controlada.

Este control se rige directamente por el Reglamento (CE) n.º 300/2008, el Reglamento de Ejecución (UE) 2015/1998 y el PNSAC, y solo puede ser ejecutado por personal habilitado y específicamente formado conforme a los estándares establecidos por la autoridad competente.

Tabla 1

Comparativa de zonas aeroportuarias y régimen de seguridad

Zona pública <i>Landside</i> Zona tierra	Zona del aeropuerto accesible al público general. No forma parte de la zona de operaciones.	Acceso libre o administrativo básico (sin control de seguridad estricto).	Vigilancia general; control de accesos administrativos (identidad/autorización básica); prevención de incidentes ordinarios. No aplica control técnico de seguridad.	Vigilantes (art. 32): detección, verificación y ejecución de protocolos básicos. Prohibida cualquier decisión técnica sin habilitación superior.	Bajo a medio. Margen limitado; no afecta a la introducción de artículos prohibidos en zonas críticas.	Reglamento (CE) 300/2008 (Anexo 1.1); PNSAC 2025 (parte pública); Ley 5/2014 (art. 32).
Zona aire <i>Airside</i> Zona de operaciones	Zona de circulación y operaciones: plataforma, pistas, hangares, etc. Acceso restringido por seguridad aeroportuaria. Incluye accesos controlados, ZRS y zonas críticas.	Acreditación válida + control previo (motivo legítimo).	Control de accesos (administrativo) + control de seguridad según subzona (técnico: RX, EDS, ETD, inspección manual).	Vigilantes (art. 32), jefes (art. 35), directores (art. 36): supervisión, coordinación y ejecución según habilitación. Formación continua (C2 AESA si aplica). Prohibido asumir funciones reservadas sin delegación formal.	Medio a alto. Depende de subzona; en ZRS y zonas críticas → discrecionalidad cero.	Reglamento (CE) 300/2008 (Anexos 1.1-1.2); Reglamento (UE) 2015/1998 (Anexo 1); PNSAC 2025.
Zonas Restringidas de Seguridad (ZRS)	Parte del lado aire donde se aplican normas reforzadas contra interferencia ilícita. Incluye: zona post-control de pasajeros, equipaje facturado pendiente (no seguro), zonas de carga/embarque de aeronaves.	Control de seguridad previo (inspección personas/objetos) + acreditación específica verificada.	Control técnico-preventivo obligatorio (RX, EDS, ETD, inspección manual). Principio “no concesión ante la duda”. Control de accesos estricto.	Solo personal habilitado (vigilantes/jefes/directores). Ejecución de controles exclusivamente por habilitados. Mandos sin delegación formal carecen de potestad.	Alto a muy alto. Discrecionalidad operativa: cero. Todas las decisiones deben ser trazables y replicables.	Reglamento (CE) 300/2008 (Anexo 1.1.2); Reglamento (UE) 2015/1998 (Anexos 1.2-1.3); PNSAC 2025 (1.1.2); Anexo 17 OACI.
Zonas críticas de las ZRS	Subespacios de máxima protección dentro de ZRS, próximos a aeronaves o infraestructuras esenciales. Se establecen en aeropuertos con >60 acreditados ZRS. Incluyen: post-control de pasajeros, equipaje facturado pendiente, zonas de operaciones de aeronaves.	Controles intensificados y 100% documentados (personas/vehículos).	Control de seguridad reforzado: inspección 100%, observación constante si hay exención temporal, perímetro inmediato ante duda. Cero discrecionalidades; decisiones totalmente protocolizadas.	Solo personal habilitado con formación continua y C2 AESA (si aplica). Vigilantes/jefes/directores con delegación formal. Cualquier “mando informal” incurre en intrusismo.	Muy alto a crítico. Discrecionalidad inexistente. Respuesta inmediata a TEDAX/EOD ante sospecha de IED. Responsabilidad penal/civil directa por desviaciones.	Reglamento (CE) 300/2008 (Anexo 1.1.3); Reglamento (UE) 2015/1998 (Anexo 1.4); PNSAC 2025 (1.1.3, umbral >60); Directiva (UE) 2022/2557 (resiliencia).

Fuente: elaboración propia.

- ✓ **Control de accesos vs. control de seguridad:** el Reglamento (UE) 2015/1998 distingue funciones: el control de accesos es una verificación administrativa (identidad, acreditación, vigencia), mientras que el control de seguridad es una evaluación técnica orientada a detectar artículos prohibidos mediante equipos homologados y el principio de *no concesión ante la duda*. Confundir ambos o delegar el control de seguridad en personal no habilitado altera la arquitectura de protección y puede constituir infracción grave, e incluso, un delito.
- ✓ **Umbral actualizado de zonas críticas:** el PNSAC 2025 eleva el umbral para declarar zonas críticas a más de 60 personas acreditadas para ZRS (antes >40), reforzando la protección en aeropuertos con mayor densidad operativa.
- ✓ **Cero discrecionalidades operativas:** en ZRS y zonas críticas, la normativa vigente (Reglamento 2015/1998 y PNSAC 2025) establece que toda actuación debe ser

replicable, auditada y documentada, eliminando la discrecionalidad individual. La trazabilidad es obligatoria y cualquier desviación constituye incumplimiento.

4.4. Consecuencia jurídica y operativa de la delimitación zonal

La zonificación no es un formalismo. Determina:

- ✓ El nivel de riesgo asumido.
- ✓ El tipo de control exigible.
- ✓ La competencia funcional del personal.
- ✓ La trazabilidad documental obligatoria.
- ✓ El régimen de responsabilidad en caso de fallo.

Autorizar el acceso administrativo a una persona no equivale a validar la seguridad de los objetos que transporta. Del mismo modo, desplazar objetos entre zonas con distinto régimen jurídico sin aplicar el control correspondiente no constituye una decisión organizativa menor, implica alterar el perímetro de seguridad definido por la normativa europea.

En un aeropuerto, cada metro cuadrado tiene un régimen jurídico diferenciado. Ignorar esa delimitación no es una cuestión de estilo pragmático, sino una infracción del sistema de protección diseñado para prevenir actos de interferencia ilícita.

Es por ello por lo que, en un entorno normativamente estratificado, la improvisación jerárquica no solo invade competencias personales, altera el equilibrio técnico-jurídico que sostiene la seguridad de la aviación civil.

5. Formación, simulacros y la ironía de la seguridad cumplida

De la misma manera, para mayor tranquilidad colectiva, no podemos olvidar que el sistema no descansa únicamente sobre la buena voluntad operativa, sino sobre obligaciones formativas expresamente impuestas por el ordenamiento jurídico.

La Norma Básica de Autoprotección, aprobada por el Real Decreto 393/2007, no exige la mera existencia formal de un plan, sino su implantación efectiva, su revisión periódica, la formación obligatoria de todo el personal sin excepción y la realización de simulacros al menos con la periodicidad mínima anual prevista normativamente.

Su Capítulo VI no admite interpretaciones creativas, la formación debe ser real, la implantación verificable y el entrenamiento funcional en lo que respecta a la implementación de las medidas de emergencia.

Algunas comunidades autónomas refuerzan estas exigencias, como ocurre en Canarias con el Decreto 67/2015, que establece pautas de desarrollo normativo alineadas con la Norma Básica. La coordinación con otros planes, la integración con planes de ámbito

superior y la articulación operativa con distintos actores intervinientes no son “sugerencias” ni innovaciones de mandos creativos, forman parte de la estructura obligatoria del plan, definida en su Capítulo VII, que impone que toda actuación ante un incidente no rutinario o una emergencia sobrevenida sea coherente, replicable y trazable en coordinación con otros planes de ámbito superior.

Conviene recordar (con la serenidad que exige el Derecho penal) que la omisión de estas obligaciones no es una cuestión meramente administrativa. La falta de implantación real, la ausencia de formación efectiva, la no realización de simulacros o la no actualización de los planes cuando procede pueden encajar en los tipos penales relativos a los delitos contra la seguridad y salud de los trabajadores (arts. 316 y ss. del Código Penal), configurados como delitos de exposición al riesgo.

Es decir, no exigen que el daño se materialice, basta con la creación de una situación de riesgo grave para la vida, la salud o la integridad física de los trabajadores mediante la infracción de normas de prevención, u otras análogas, legalmente exigibles. El Derecho no espera a que haya víctimas para reaccionar, sanciona la exposición intolerable al riesgo.

Resulta, por ello, profundamente tranquilizador comprobar cómo, en la práctica generalizada, la formación se imparte con el rigor debido, los simulacros se realizan con escenarios realistas, la actualización de los planes es constante y la integración con otros planes y actores se cumple como dispone la estructura normativa.

Afortunadamente, nadie confunde la implantación con la mera aprobación documental ni el simulacro con una representación coreografiada de evacuación previamente anunciada. Porque si así fuera (si la formación fuese nominal, el simulacro simbólico y la actualización inexistente) no estaríamos ante una simple disfunción organizativa, sino ante la generación consciente de un riesgo jurídicamente relevante. El riesgo, cuando es evitable y normativamente prevenible, deja de ser accidente para convertirse en una responsabilidad un poquito más seria.

6. Contenido esencial del procedimiento

Cuando un objeto presenta morfología sospechosa en imagen radiológica, el procedimiento no admite concesiones, ocurrencias ni “percepciones de sobremesa de los que yo llamo expertos en café”. Es inamovible y secuencial, porque cada paso protege vidas, instalaciones y la credibilidad del sistema:

1. Retención inmediata: inmovilización del objeto en el punto de inspección. Nada de “lo dejamos pasar, que parece inofensivo”, “ya volverá alguien a recogerlo” o “mejor paso yo por alto porque hay cola de embarque”. Cada segundo de duda es una invitación al riesgo.
2. Comunicación al “supervisor” habilitado: solo personal con habilitación oficial y formación continua según la Ley 5/2014 (España, 2014) puede asumir la

evaluación. La autoridad no se hereda por jerarquía aparente ni por el autodenominado “jefe de equipo” que decide dónde te colocas, quién pasa, si rechazas una maleta o dejas entrar a alguien sin documentación. La experiencia y la formación permanente son el verdadero bastón del mando.

3. Verificación física controlada: realizada por personal habilitado siguiendo los protocolos del PNSAC y la normativa europea. No es un trámite simbólico; es la única manera de transformar la sospecha radiológica en certeza.
4. Registro documental trazable: cada actuación debe quedar documentada para garantizar responsabilidad y permitir reconstrucción ex post. Sin registro, la actuación se disuelve en la niebla de la arbitrariedad.

Cualquier intento de interpretación o “innovación técnico-operativa” por responsables de equipo o coordinadores vacíos de competencia y sin delegación formal es ilegal y compromete todo el sistema. La ley no reconoce la creatividad improvisada ni las corazonadas.

Solo la habilitación legal, la formación permanente y los procedimientos estandarizados y su conocimiento legitiman la decisión, protegen a los profesionales diligentes y blindan la organización frente a consecuencias que podrían ser, literalmente, irreversibles.

7. Dimensión técnico-radiológica

Los sistemas de rayos X 2D, predominantes en la inspección aeroportuaria, generan imágenes bidimensionales basadas en densidad y algoritmos de pseudocolor, pero no permiten reconstrucción tridimensional ni verificación funcional de los objetos (ICAO, 2015; Schroeder et al., 2023). Lo que no quiere decir que no existan los escáneres tridimensionales 3D en el nivel correspondiente (véase *disclaimer 1*).

Su interpretación debe ser realizada exclusivamente por personal habilitado y en formación continua, conforme a estándares europeos y estatales (Reglamento (UE) 2015/1998; AESA, 2023). Los “pálpitos de sobremesa” del personal no autorizado corroe la integridad del sistema y no sustituye evidencia técnica.

Las limitaciones de los Rayos X 2D son claras:

- ✓ No distinguen con certeza entre armas reales y réplicas.
- ✓ No revelan mecanismos internos ni modificaciones funcionales ocultas, esenciales para separar lo benigno de lo letal.
- ✓ No permiten evaluar la disposición tridimensional de los componentes, impidiendo descartar elementos detonantes o accesorios de un artefacto.

Cuando la imagen sugiere la posible presencia de un IED (*Improvised Explosive Device*, dispositivo explosivo improvisado), artefacto diseñado para detonar fuera de controles formales y que puede incorporar circuitería, detonadores y carga principal, la

respuesta operativa cambia radicalmente. No se debe tratar como un objeto prohibido convencional ni “abrirlo en zona controlada como si fuera un arma de juguete”. La doctrina y los procedimientos de respuesta a amenazas explosivas exigen:

1. Establecimiento inmediato de un perímetro de seguridad, evacuando toda presencia civil y no autorizada.
2. Activación de unidades especializadas EOD/TEDAX:
 - o **EOD** (*Explosive Ordnance Disposal*): especialistas en desactivación de artefactos explosivos, con procedimientos, robótica y tecnología específica para neutralizar amenazas.
 - o **TEDAX-NRBQ** (Técnicos Especialistas en Desactivación de Artefactos Explosivos – Riesgos Nucleares, Radiológicos, Biológicos y Químicos): unidades españolas con competencias formales y equipamiento certificado por la Guardia Civil y Policía Nacional (Guardia Civil, s.f.; Policía Nacional, s.f.).
3. Coordinación inmediata con las Fuerzas y Cuerpos de Seguridad del Estado, asegurando trazabilidad, cadena de mando y documentación operativa.

Esta respuesta especializada no es opcional ni de segunda línea; está codificada en los procedimientos aeroportuarios y es proporcional al riesgo que representa un IED.

Confiar en los oráculos de tiempos pasados frente a estos dispositivos es pseudociencia aplicada a la seguridad: un lujo que la aviación civil no puede permitirse. Liberar un artefacto por confianza mal fundada puede derivar en daños irreversibles y en responsabilidad civil y penal, incluyendo privación de libertad e inhabilitación profesional según nuestro vigente Código Penal (España, 1995, art. 403).

La habilitación formal, la formación permanente y la adhesión estricta a procedimientos estandarizados no son adornos retóricos, son las únicas herramientas que transforman la sospecha técnica en certeza operativa, blindan al operador diligente y evitan que la improvisación se convierta en desastre previsible.

7.1. Riesgo de reconversión funcional

La literatura europea y los informes de *Europol* y *Small Arms Survey* advierten sobre la creciente transformación de armas legales en letales, lo que eleva la amenaza más allá de lo aparente (Florquin & King, 2018; Jongleux & Florquin, 2020; Schroeder et al., 2023). Incluso una réplica que parece un juguete puede ocultar riesgos significativos, la apariencia externa no concede licencia para la negligencia.

7.2. Consecuencias inmediatas:

- ✓ La retención preventiva deja de ser un gesto formal para convertirse en una fuente activa de inteligencia, que ilumina patrones de riesgo y comportamientos anómalos.

- ✓ Subestimar un objeto es regalar al azar la gestión del riesgo. La brecha entre la amenaza real y la percepción subjetiva se transforma en un hueco práctico donde puede colarse la tragedia.
- ✓ Solo los procedimientos reglados aseguran que la seguridad no dependa del “olfato del café por si ya está listo” del mando de turno ni de la jerarquía informal que decide por simpatía.

7.3. Replicabilidad y trazabilidad

En aviación civil, la legitimidad de una actuación no surge del instinto ni de la confianza personal, sino de la capacidad de replicar, auditar y justificar cada paso (OACI, 2016). La cadena mínima de actuación frente a una imagen sospechosa debe ser estrictamente:

1. Detección: identificación radiológica (RX) del objeto conforme a procedimientos estandarizados.
2. Retención: inmovilización inmediata para evitar desplazamiento o manipulación indebida.
3. Comunicación: notificación inmediata a personal habilitado y formado específicamente para estas contingencias.
4. Verificación: examen físico en zona controlada, cumpliendo protocolos europeos y nacionales.
5. Registro: documentación completa y trazable para auditoría interna, supervisión externa y eventual revisión judicial.

La replicabilidad no es un lujo académico, sencillamente es la garantía de que la actuación puede resistir escrutinio legal, técnico y funcional en cualquier área.

En el entorno de las entidades críticas aeroportuarias, el éxito no se mide por si algo salió bien, sino por si cada paso puede demostrarse y justificarse. El operador diligente no se protege con heroísmo improvisado, se protege siguiendo el guion que convierte la sospecha en certeza, y la clarividencia en un peligro prevenido.

8. Cuando la prevención funciona, pero la cultura la desgasta

Aquí se revela la siguiente paradoja: el operador cumple estrictamente la norma, pero los micro incentivos mal calibrados del entorno organizativo logran que la prevención se perciba como un estorbo. James Reason y Sidney Dekker demostraron que los sistemas complejos no colapsan por un error aislado, sino por la acumulación de desviaciones normalizadas (Reason, 1997; Dekker, 2011).

Cuando un “mando” (autodenominado, sin habilitación formal) reprende a un operador por retener una maleta sospechosa “para no retrasar el flujo”, se transmite un mensaje demoledor: cumplir la norma puede acarrear sanción informal. Este mensaje no

es inocuo, erosiona la cultura de seguridad, reemplaza la autoridad legal con la autoridad fáctica del que “*manda sin poder mandar*”, y allana el terreno para fallos sistémicos.

Ejemplos cotidianos ilustran la gravedad:

- ✓ Se indica a un vigilante que deje pasar un objeto dudoso “porque la cola es larga”.
- ✓ Se ordena al personal que abra accesos o deje entrar a pasajeros sin documentación “para no retrasar operaciones”.
- ✓ Se premia la rapidez sobre la prudencia, generando la percepción de que la obediencia informal sustituye a la norma escrita.

Un ejemplo particularmente ilustrativo (según versiones de las testigos difundidas por medios y actualmente pendiente de esclarecimiento judicial, por lo que permanece *sub iudice*) de las consecuencias derivadas de no aplicar de forma estricta el procedimiento secuencial se produjo en las inmediaciones del Aeropuerto de Gran Canaria en mayo de 2025.

Minutos antes de un incidente exterior que culminó en una intervención policial por amenazas con arma blanca, el individuo era un inmigrante (término empleado aquí en su sentido estrictamente técnico para describir el flujo migratorio como aquella persona que entra en un país distinto al de origen y sin connotación valorativa o peyorativa) implicado habría intentado acceder a una zona restringida pasando por un filtro de control de seguridad. Al cruzar el arco detector de metales, este activó la alarma por presencia metálica en su mochila.

Sin embargo, en lugar de someter inmediatamente el bulto al escáner RX obligatorio y proceder a la verificación física controlada (paso esencial para transformar una sospecha en una certeza operativa), se optó por expulsarlo o dirigirlo hacia el exterior de la instalación, aparentemente en coordinación con personal presente en el punto.

Lo que pudo interpretarse como una medida “práctica” para evitar congestiones o retrasos derivó en que un artículo prohibido (un cuchillo de grandes dimensiones) permaneciera en posesión del individuo, facilitando su uso posterior en una zona pública con elevado tránsito de personas. El resultado fue un riesgo evitable que escaló hasta generar amenazas directas contra terceros y agentes, obligando a una intervención policial de alto riesgo y a un desenlace irreversible.

Esta secuencia (basada en testimonios públicos y en una investigación judicial en curso) evidencia cómo cualquier desviación del protocolo, ya sea por presión, criterio informal o aparente coordinación improcedente, no solo incumple el Reglamento (UE) 2015/1998 (Anexos 1.2 y 1.3), el PNSAC (principio de no concesión ante la duda) y la Ley 5/2014 (competencias reservadas a personal habilitado), sino que además fractura la cadena de resiliencia exigida por la Directiva CER. La habilitación formal, la formación continua y la adhesión estricta al procedimiento no son

formalidades accesorias, constituyen la barrera esencial que evita que una alarma ignorada se convierta en un riesgo real para personas e infraestructuras críticas.

El resultado es un ecosistema en el que la improvisación jerárquica se normaliza, las decisiones técnicas se diluyen en caprichos y la resiliencia del sistema se debilita. La ironía no es literaria, es operativa, jurídica y potencialmente letal.

9. Liderazgo habilitado y cultura de seguridad

El liderazgo en seguridad aeroportuaria no se improvisa con autoproclamaciones ni con presencia de uniforme; es un ejercicio consciente de responsabilidad técnica, legal y operativa, y tiene tres obligaciones ineludibles:

1. Proteger al operador diligente: garantizar que toda actuación conforme al procedimiento sea reconocida como correcta y respaldada institucionalmente. No se trata de premiar la obediencia superficial; se trata de blindar al profesional que aplica la norma cuando realmente importa.
2. Reforzar la autoridad habilitada: asegurar que las decisiones solo recaigan en personal legalmente competente y formado continuamente. La habilitación formal combinada con experiencia práctica es el único bastón de mando que evita errores irreversibles.
3. Neutralizar la autoridad fáctica: impedir que mandos autodenominados o “inspectores de café” modifiquen procedimientos por conveniencia, pálpito o necesidad de aparentar eficiencia. La jerarquía informal puede ser letal para la integridad del sistema, un despacho con despacho vacío no es liderazgo, es un escenario peligroso.

En un entorno de alta criticidad, la prevención solo funciona cuando la organización protege a quienes aplican la ley y sanciona a quienes la ignoran o la puentean. Ignorar estos principios no es audacia ni innovación, es sabotaje institucional disfrazado de eficiencia, con consecuencias que van desde la fractura cultural hasta la responsabilidad penal de quienes confunden protagonismo con competencia.

Ejemplo gráfico de riesgo de autoridad fáctica: un “jefe de equipo” sin habilitación decide desplazar a un operador, autorizar el paso de un pasajero sin documentos o liberar una maleta dudosa “para no entorpecer la cola”.

Cada una de estas decisiones aparenta eficiencia, pero erosiona la seguridad real y construye seguridad aparente, un espejismo que solo el desastre podrá desmentir porque el verdadero liderazgo en seguridad no se proclama, se ejerce, protege, respalda y disciplina. Todo lo demás es ruido administrativo (que no hilo musical) que el sistema no puede permitirse.

CONCLUSIONES

PERORITACIONES

1. La seguridad no se improvisa. En infraestructuras críticas aeroportuarias, cada función exige una habilitación legal específica, formación continua y respeto estricto a las competencias reservadas. Invadir esos ámbitos genera consecuencias que pueden incluir sanciones económicas graves, inhabilitación y, en determinados casos, penas de prisión.
2. Seguridad real frente a seguridad aparente. La prevención efectiva se sustenta en procedimientos replicables, trazabilidad documental y verificación física obligatoria ante cualquier duda radiológica. Sustituir estos pilares por intuiciones, atajos o jerarquías informales genera vulnerabilidades sistémicas y debilita la resiliencia exigida por la Directiva (UE) 2022/2557.
3. El liderazgo técnico es la única autoridad legítima. La dirección operativa se fundamenta en experiencia acreditada y adhesión normativa (como recogen los arts. 32-36 de la Ley 5/2014), no en mandos autoproclamados ni en la apariencia de eficiencia. Quien antepone la improvisación a la norma dinamita la cultura de seguridad y expone a quienes sí actúan con diligencia.
4. Cultura de la seguridad y los procedimientos forman un todo indivisible. Retener, comunicar, verificar y documentar (incluyendo la activación de EOD/TEDAX ante indicios de IED) no es una elección, sino un mandato del PNSAC y del Reglamento (UE) 2015/1998. Penalizar la diligencia o premiar la improvisación convierte la prevención en una vulnerabilidad colectiva.
5. La complacencia normalizada es un riesgo transversal. Cada decisión delegada a “expertos en café” y cada maleta liberada “porque nunca pasa nada” debilita el sistema de protección de infraestructuras críticas. El descuido individual amplifica la exposición de todos, como demuestran desviaciones reales detectadas en controles aeroportuarios.

La verdadera profesionalidad no consiste en saltarse normas para parecer eficiente, sino en liderar desde la competencia legal y la protección real de vidas.

REFERENCIAS

Agencia Estatal de Seguridad Aérea (AESA). (s. f.). *Programa Nacional de Seguridad para la Aviación Civil (PNSAC) – Parte pública*. Ministerio de Transportes y Movilidad Sostenible.

<https://www.transportes.gob.es/aviacion-civil/legislacion-del-sector-aereo/normativa-basica-del-sector-aereo-estructura/security/actualizacion-pns>

Boletín Oficial del Estado. (2007, 24 de marzo). *Real Decreto 393/2007, de 23 de marzo, por el que se aprueba la Norma Básica de Autoprotección de centros, establecimientos y dependencias dedicados a actividades que puedan dar origen a situaciones de emergencia* (BOE n.º 72).

<https://www.boe.es/buscar/act.php?id=BOE-A-2007-6237>

España. (1995). *Código Penal, Real Decreto Legislativo 10/1995, de 23 de noviembre*. Boletín Oficial del Estado, 282.

<https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444>

España. (1995). *Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales*. Boletín Oficial del Estado.

<https://www.boe.es/buscar/act.php?id=BOE-A-1995-24292>

España. (2011, 29 de abril). *Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas*. Boletín Oficial del Estado.

<https://www.boe.es/eli/es/l/2011/04/28/8/con>

España. (2011). *Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas*. Boletín Oficial del Estado, 121. <https://www.boe.es/buscar/act.php?id=BOE-A-2011-8849>

España. (2014). *Ley 5/2014, de 4 de abril, de Seguridad Privada* (versión consolidada). Boletín Oficial del Estado, 83.

<https://www.boe.es/buscar/act.php?id=BOE-A-2014-3649>

European Commission. (1998). *Reglamento de Ejecución (UE) 2015/1998 de la Comisión, de 5 de noviembre de 2015, por el que se establecen medidas detalladas para la aplicación de las normas básicas comunes de seguridad aérea* (DOUE L 299). <https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:32015R1998>

European Parliament & Council. (2008). *Reglamento (CE) n.º 300/2008 del Parlamento Europeo y del Consejo, de 11 de marzo de 2008, por el que se establecen normas comunes para la seguridad de la aviación civil* (DOUE L 97). <https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:32008R0300>

International Civil Aviation Organization (OACI). (2022). *Anexo 17 al Convenio sobre Aviación Civil Internacional: Seguridad – Protección de la aviación civil internacional contra los actos de interferencia ilícita* (12.^a ed.). https://www.icao.int/publications/catalogue/cat_2025_en.pdf

Secretaría de Estado de Seguridad. (2015). *Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos* (BOE n.º 224). <https://www.boe.es/boe/dias/2015/09/18/pdfs/BOE-A-2015-10060.pdf>

Unión Europea. (2022). *Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE (DO L 333)*. <https://eur-lex.europa.eu/ELI/dir/2022/2557/oj>