MOLINS

Defensa Penal **Compliance**

Compliance Newsletter Year Review

2025

Índice

Introducción

El ***Compliance*** se ha posicionado como una pieza clave para garantizar la solidez y ética de las organizaciones en el complejo y dinámico marco regulatorio actual. En este contexto, **la actualización continua no es solo un deber**, sino una **necesidad estratégica indispensable** para abordar los desafíos presentes y futuros.

Durante el pasado 2025 han tenido lugar **desarrollos regulatorios y jurisprudenciales importantes en materia de *Compliance***, tanto a nivel nacional como internacional. En concreto, se han observado algunas novedades tales como:

- El **Proyecto de Ley Orgánica que modificará la Ley Orgánica del Código Penal** para la transposición de la Directiva (UE) 2024/1226, relativa a los delitos y las sanciones por la vulneración de medidas restrictivas de la Unión.
- El nuevo **criterio del Tribunal Supremo** en la **carga de probar** tanto la **comisión del delito cometido por la persona física** como la **existencia del incumplimiento organizativo** por parte de **la empresa** (STS 768/2025 de 25 de septiembre).

En este contexto, el Departamento de *Compliance* de **Molins Defensa Penal** ha preparado el presente *Newsletter* a modo de revisión de los principales hitos en materia de *Compliance* del año 2025. Su contenido se estructura de la siguiente manera:

- Se llevará a cabo un análisis de las **novedades legislativas más relevantes** que impactan en la configuración y mejora de los Sistemas de *Compliance*.
- A continuación, se expondrán **resoluciones judiciales de interés en materia de *Compliance*** dictadas durante el año 2025.
- Seguidamente, se presentarán otros **acuerdos y resoluciones sancionadoras** significativas en el ámbito de *Compliance*.
- También se incluirá una breve presentación de **guías, resoluciones institucionales e informes** recientes de particular interés.
- Por último, esta *Newsletter* concluirá con un resumen de las **publicaciones del Departamento de *Compliance*** correspondientes al año 2025.

Novedades legislativas

MOLINS Compliance

- Anteproyecto de Ley Orgánica para la transposición de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).
- Novedades sobre el Reglamento (UE) 2024/1689, de Inteligencia Artificial.
- Proyecto de Ley 121/46 de 4 de febrero de 2025 de transparencia e integridad de las actividades de los grupos de interés.
- Suspensión temporal de la Ley de Prácticas Corruptas en el Extranjero (*Foreign Corrupt Practices Act*) de Estados Unidos
- Nuevas Directrices por parte del Departamento de Justicia estadounidense (DOJ) en materia de investigaciones y aplicación de la FCPA.
- Real Decreto 102/2025, de 18 de febrero, por el que se modifica el Estatuto de la Autoridad Independiente de Protección del Informante, A.A.I., aprobado por el Real Decreto 1101/2024, de 29 de octubre.
- Real Decreto 328/2025, de 15 de abril, por el que se nombra Presidente de la Autoridad Independiente de Protección del Informante, A.A.I., a don Manuel Villoria Mendieta.
- Directiva (UE) 2025/794 del Parlamento Europeo y del Consejo, de 14 de abril de 2025, por la que se modifican las Directivas (UE) 2022/2464 y (UE) 2024/1760 en lo que respecta a las fechas a partir de las cuales los Estados miembros deben aplicar determinados requisitos de presentación de información sobre sostenibilidad y de diligencia debida por parte de las empresas.
- Resolución legislativa del Parlamento Europeo en lo que respecta a determinados requisitos de presentación de información corporativa y de diligencia debida de las empresas en materia de sostenibilidad.
- Anteproyecto de Ley para el buen uso y la gobernanza de la Inteligencia Artificial, de adaptación al Reglamento (UE) 2024/1689 de Inteligencia Artificial.
- Orden PJC/908/2025, de 8 de agosto, por la que se determina la fecha de puesta en funcionamiento de la Autoridad Independiente de Protección del Informante, A.A.I.
- Reglamento Delegado (UE) 2025/2003 de la Comisión, de 8 de septiembre de 2025, por el que se modifica el Reglamento (UE) 2021/821 del Parlamento Europeo y del Consejo en lo que concierne a la lista de productos de doble uso
- Real Decreto-ley 10/2025, de 23 de septiembre, por el que se adoptan medidas urgentes contra el genocidio en Gaza y de apoyo a la población palestina.
- Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, para la transposición de la Directiva (UE) 2024/1226 del Parlamento Europeo y del Consejo, de 24 de abril de 2024, relativa a la definición de los delitos y las sanciones por la vulneración de las medidas restrictivas de la Unión, y por la que se modifica la Directiva (UE) 2018/1673.

Anteproyecto de Ley Orgánica para la transposición de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2)

El 14 de enero de 2025, el Consejo de Ministros aprobó el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, con el objetivo de **transponer la Directiva (UE) 2022/2555 (NIS-2)**, en vigor desde enero de 2023. Dicha Directiva engloba un conjunto de **medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la UE**.

El **Anteproyecto amplía el alcance de la Directiva NIS-2** incluye, además de los sectores ya contemplados (energía, transporte, banca, sanidad, agua, administración pública, infraestructuras digitales y servicios tecnológicos), a la industria nuclear como sector de alta gravedad. También incorpora al sector de la seguridad privada en el grupo de sectores de criticidad media, junto con la gestión de residuos, la producción y distribución de alimentos, los servicios postales y la investigación científica.

Asimismo, especifica el **ámbito de aplicación** en las entidades públicas o privadas que tengan la residencia fiscal en España, o que, teniendo su residencia en otro Estado de la UE, ofrezcan sus servicios o desarrollen su actividad en España. Dichas entidades deberán realizar una evaluación individualizada de su riesgo y establecer actuaciones para garantizar y elevar los niveles de seguridad de sus redes y sistemas de información, además de prevenir el riesgo de incidentes.

El texto prevé la creación del **Centro Nacional de Ciberseguridad**, que actuará como organismo coordinador a nivel nacional y punto de contacto con la UE, y será responsable de elaborar el listado de entidades consideradas esenciales o importantes.

Además, el Anteproyecto establece la obligación de **designar a un responsable de la seguridad de la información**, quien tendrá la responsabilidad de elaborar estrategias y políticas de ciberseguridad, supervisar su implementación, gestionar incidentes, garantizar el cumplimiento de los criterios de seguridad establecidos por proveedores externos y actuar como punto de contacto con las autoridades de control. Además, en las entidades esenciales, este responsable deberá estar acreditado por el Ministerio del Interior.

Novedades sobre el Reglamento (UE) 2024/1689, de Inteligencia Artificial

Pese a que el Reglamento no se aprobó en 2025, cabe resaltar que **durante el presente año han entrado en vigor algunas de sus disposiciones**, teniendo en cuenta la aplicación progresiva que prevé el propio Reglamento hasta agosto de 2026. En concreto, son aplicables desde el **2 de febrero de 2025**:

- Capítulo I sobre **disposiciones generales**, entre las que destaca la **definición de sistema** de Inteligencia Artificial (en adelante, IA) y **alfabetización en materia de IA**. Comporta que los proveedores y quienes se encargan de implantar sistemas de IA deberán adoptar medidas para asegurar que, en la medida de lo posible, las personas que operen o utilicen dichos sistemas posean una formación adecuada en la materia.
- Capítulo II sobre **prácticas prohibidas**. Algunas de las más destacadas son las siguientes:
    - El uso de sistemas de IA que empleen técnicas subliminales o manipuladoras que alteren sustancialmente el comportamiento y la capacidad de decisión informada de las personas.
    - El uso de sistemas de IA que exploten vulnerabilidades (edad, discapacidad o situación socioeconómica) con el fin de alterar sustancialmente su comportamiento.
    - Clasificar personas según su comportamiento o características si ello conlleva un trato injustificado, desproporcionado o fuera de contexto.
    - Clasificar personas mediante datos biométricos con el fin de inferir aspectos sensibles como raza, ideología o vida sexual, salvo en contextos legales o de tratamiento lícito de datos.

Para concretar algunas de las disposiciones anteriores, la **Comisión Europea ha publicado Directrices** en la materia para enfocar algunos conceptos jurídicos indeterminados.

Por otra parte, siguiendo el esquema de aplicación progresiva del Reglamento, desde el **2 de agosto de 2025** también tienen efecto las disposiciones relativas a obligaciones para los proveedores de modelos de IA y a ciertos aspectos sobre las sanciones que deberán haber previsto los Estados miembros.

Novedades legislativas

MOLINS Compliance

Proyecto de Ley de transparencia e integridad de las actividades de los grupos de interés

A fecha de 4 de febrero, el Gobierno impulsó el Proyecto de Ley de transparencia e integridad de las actividades de los grupos de interés, con el **objetivo de regular, en el ámbito de la Administración General del Estado y el sector público institucional, las relaciones entre los grupos de interés** (también denominados *lobbies*) y las personas responsables públicas, conforme a **criterios de transparencia, integridad e igualdad**.

Destacan las siguientes novedades:

- Creación del **Registro de Grupos de Interés**, de inscripción obligatoria, pública, gratuita y electrónica, gestionado por la Oficina de Conflictos de Intereses.
- **Prohibición general** de contactos con responsables públicos **sin inscripción previa** en el Registro.
- Se introduce la figura del "**informe de huella normativa**", que deberá integrarse en los expedientes normativos para reflejar qué *lobbies* han participado en la elaboración en cada norma.
- **Código de conducta vinculante** para grupos de interés.

Cabe destacar que, en septiembre de 2025, se publicaron **las enmiendas al articulado presentado por el Gobierno** por parte de los distintos grupos parlamentarios durante la tramitación del Proyecto de Ley en el Congreso.

Suspensión temporal de la Ley de Prácticas Corruptas en el Extranjero (FCPA) de Estados Unidos (EEUU) y nuevas directrices de aplicación

El 10 de febrero de 2025, el presidente de Estados Unidos (en adelante, EEUU) Donald J. Trump firmó la Orden Ejecutiva (en adelante, OE) titulada "**Pausar la aplicación de la FCPA para promover la seguridad económica y nacional de Estados Unidos**", por la cual se instruyó al Departamento de Justicia (en adelante, DOJ) a **suspender la iniciación de nuevas investigaciones** o **procesos** en virtud de la FCPA durante un período inicial de **180 días**, con posibilidad de extenderse otros 180 días si la *Attorney General* lo consideraba apropiado.

Durante este paréntesis, la OE exige principalmente:

- La **revisión exhaustiva de las directrices** y políticas de aplicación de la FCPA, tanto para casos en curso como pasados, a fin de "**restaurar los límites adecuados**".
- La **emisión de nuevas directrices**, alineadas con la política exterior del país, la competitividad económica de EEUU y una utilización racional de recursos federales (*ver siguiente apartado, relativo a las nuevas directrices dictadas en la materia*).
- **Suspensión de nuevas investigaciones**, salvo autorización expresa de la *Attorney General* en casos de "excepción individual".

Nuevas Directrices por parte del DOJ de EEUU en materia de investigaciones y aplicación de la FCPA

El Departamento de Justicia de EEUU emitió el pasado 9 de junio de 2025 un nuevo memorando, con el objetivo de **alinear la aplicación de la FCPA con las directrices fijadas** por la OE de 10 de febrero, firmada por el presidente Trump. El documento **reafirma expresamente la necesidad de contar con una autorización excepcional y previa para iniciar cualquier nueva investigación**.

Establece un **marco de actuación más selectivo de aplicación de la FCPA**, orientado a:

- Limitar las cargas indebidas sobre empresas estadounidenses que operan en el extranjero.
- Focalizar las actuaciones sancionadoras en aquellas conductas que comprometan directamente los "intereses nacionales".

Los fiscales deberán **priorizar la investigación de casos con indicios sólidos de conducta delictiva atribuible a personas físicas**, evitando imputaciones genéricas a estructuras corporativas, y ponderar los posibles efectos colaterales sobre trabajadores.

Además, **toda nueva investigación sobre la FCPA deberá contar con autorización previa del *Assistant Attorney General*** o de una autoridad superior. Entre los **factores** clave que orientarán la decisión de iniciar o continuar investigaciones se incluyen:

- La **lucha contra cárteles y organizaciones criminales transnacionales**, especialmente cuando el soborno facilite sus operaciones, se empleen mecanismos de blanqueo de capitales o estén vinculados a funcionarios públicos.
- La **protección de la libre competencia**, en casos de perjuicio económico a entidades estadounidenses.
- La salvaguarda de la **seguridad nacional**, en sectores estratégicos.

- La gravedad de la conducta, **excluyendo prácticas comerciales rutinarias o cortesías permitidas**, y centrando la investigación en pagos significativos, así como en esquemas sofisticados de ocultación y fraude.

Finalmente, se advierte que estas directrices no son exhaustivas y que **todas las investigaciones actuales y futuras deberán ajustarse a estos nuevos criterios**.

Real Decreto 102/2025 y Real Decreto 328/2025

Con el objetivo de cumplir con la **Ley 2/2023**, en 2024 se estableció el Estatuto de la Autoridad Independiente de Protección del Informante (en adelante, A.I.P.I). La A.I.P.I. es una **autoridad administrativa independiente de ámbito estatal** y cuenta con personalidad jurídica propia. Entre sus fines, la A.I.P.I. pretende **garantizar la protección de la persona informante**, servir de **pilar institucional esencial en la lucha contra la corrupción**, **actuando** para ello en **coordinación**, en su caso, con **otros organismos administrativos u organismos de supervisión, control**, **inspección** o **investigación** que tengan funciones semejantes, ya existentes en el ámbito estatal y autonómico, así como con autoridades con funciones similares en sus respectivos ámbitos.

El pasado 18 de febrero, mediante el **Real Decreto 102/2025**, se modificaron diversos aspectos del Estatuto. Concretamente, se añadió un nuevo apartado al artículo primero que indica que la A.I.P.I tendrá su sede en la ciudad de Madrid, se le otorgan nuevas funciones y se le permite solicitar informes técnicos, tanto a los organismos públicos afectados por las circulares, como a órganos internos de la A.I.P.I.

Finalmente, mediante el **Real Decreto 328/2025**, el 15 de abril de 2025, se nombró Presidente de la A.I.P.I al catedrático **D. Manuel Villoria Mendieta**.

Directiva (UE) 2025/794 del Parlamento Europeo y del Consejo, de 14 de abril de 2025, por la que se modifican las Directivas (UE) 2022/2464 y (UE) 2024/1760 en lo que respecta a las fechas a partir de las cuales los Estados miembros deben aplicar determinados requisitos de presentación de información sobre sostenibilidad y de diligencia debida por parte de las empresas

El 14 de abril de 2025 se aprobó la **Directiva (UE) 2025/794**, conocida como "***Stop the Clock***" o **Directiva de suspensión temporal**. Esta norma introduce un aplazamiento en la entrada en vigor de diversos requisitos de presentación de información corporativa y de diligencia debida en materia de sostenibilidad, con el objetivo de otorgar más tiempo a las empresas para adaptarse a estas obligaciones sin incurrir en costes desproporcionados.

La Directiva se enmarca dentro del llamado Paquete Ómnibus, una iniciativa de la Comisión Europea destinada a simplificar y reducir las cargas administrativas para las empresas en materia de sostenibilidad, especialmente las pequeñas y medianas empresas.

Entre las principales medidas que incorpora la Directiva, destaca el aplazamiento de dos (2) **años** en la aplicación de los requisitos de información previstos por la **Directiva sobre Información Corporativa en Materia de Sostenibilidad (en adelante, CSRD)** para determinadas empresas:

- A partir del **1 de enero de 2027**, las grandes empresas que aún no estuvieran sujetas a la Directiva de información no financiera deberán presentar sus informes de sostenibilidad en el ejercicio de 2028.
- A partir del **1 de enero de 2028**, las PYMES cotizadas, las aseguradoras cautivas consideradas grandes, y las entidades de crédito pequeñas y no complejas deberán presentar sus informes en el ejercicio del 2029.

Asimismo, la norma **aplaza en un (1) año** la entrada en vigor de la **Directiva sobre Diligencia Debida de las Empresas (en adelante, CSDDD).**

Resolución legislativa del Parlamento Europeo en lo que respecta a determinados requisitos de presentación de información

El pasado 16 de diciembre de 2025, el Pleno del Parlamento Europeo aprobó un importante **acuerdo provisional** que podría afectar a varias de las **directivas** que conforman el **paquete Omnibus I,** en concreto, la Directiva CSRD y la Directiva CSDDD. No obstante, este texto deberá ser formalmente validado por el Consejo el próximo enero de 2026.

Desde la perspectiva del *Compliance* corporativo, los cambios introducidos por esta revisión son **significativos** y operan en dos (2) ámbitos principales:

- **Directiva sobre información corporativa en materia de sostenibilidad** (CSRD): Se **eleva considerablemente el umbral de sujeción**, de modo que solo las compañías con **más de 1.000 empleados y un volumen de negocio neto superior a 450 millones de euros** estarán obligadas a presentar informes conforme a la CSRD a partir del 1 de enero de 2027, reduciendo drásticamente el número de entidades sujetas.

Además, se **limita la información que puede solicitarse en la cadena de valor**, introduciendo criterios de proporcionalidad y razonabilidad y reduciendo cargas indirectas para proveedores de menor tamaño.

- **Directiva sobre diligencia debida de las empresas en materia de sostenibilidad** (CSDDD): Como en el caso de la Directiva anterior, se incrementan sustancialmente los umbrales de aplicación de la presente directiva, **reduciendo de manera significativa el número de empresas sujetas a obligaciones de debida diligencia**. Cabe destacar que se producirá el aplazamiento de la transposición y la entrada en vigor de estas obligaciones para la mayoría de las empresas hasta julio de 2029, ofreciendo un periodo transitorio más amplio para su implementación.

Esta revisión refleja un **enfoque de simplificación normativa** que busca **equilibrar la exigencia de transparencia y diligencia debida** con una **reducción del ámbito subjetivo de su aplicación**, **flexibilización de obligaciones de reporte** y **mayores plazos de adaptación**, lo que impactará de forma relevante en las estrategias de *Compliance* corporativo de las empresas europeas y con operaciones en la UE.

En España, la incertidumbre regulatoria en materia de sostenibilidad es más pronunciada que en otros Estados miembros. A la revisión de la normativa comunitaria se suman los efectos derivados del retraso en la transposición de la **CSRD** y la **Directiva *Stop the Clock***, lo que complica aún más el panorama empresarial.

Anteproyecto de Ley para el buen uso y la gobernanza de la Inteligencia Artificial

El pasado 11 de marzo de 2025 el Consejo de Ministros aprobó el **Anteproyecto de Ley para el buen uso y la gobernanza de la IA**, en respuesta al **Reglamento (UE) 2024/1689**. Pese a la aplicabilidad directa del Reglamento, muchas de sus disposiciones requieren de desarrollo legislativo nacional para su correcta implementación.

En este contexto, se regulan específicamente cuestiones como:

- Los **encargados de la supervisión y potestad sancionadora** de los sistemas de IA dependiendo del ámbito sectorial. Por ejemplo, la Agencia Española de Protección de Datos para sistemas de seguridad o el Consejo General del Poder Judicial para sistemas de la Administración de Justicia.
- La **designación como autoridad notificante** de la Secretaría de Estado de Digitalización e Inteligencia Artificial.
- El nombramiento de la Agencia Española de la Supervisión de Inteligencia Artificial como **autoridad nacional competente responsable del establecimiento de un espacio controlado de pruebas** para la IA.

Orden PJC/908/2025, de 8 de agosto, por la que se determina la fecha de puesta en funcionamiento de la Autoridad Independiente de Protección del Informante

Como se ha mencionado anteriormente, la **Ley 2/2023**, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, **autorizó en su título VIII la creación de la A.I.P.I.**

A tal efecto, mediante el Real Decreto 1101/2024, de 29 de octubre, se **aprobó el Estatuto de la A.I.P.I.** La Disposición Transitoria del Real Decreto mencionado, establece un plazo de **dos meses para comunicar el nombramiento del Responsable del Sistema interno de información**. A estos efectos, se informa que la A.I.P.I. comenzará a computar dicho plazo desde el momento en que se publique en su portal web oficial el formulario específico de notificación del responsable del canal interno (que a fecha de la presente *Newsletter*, todavía no se ha publicado).

Cabe destacar que todos los sujetos obligados deberán remitir a la A.I.P.I. la comunicación del Responsable del Sistema interno de información, con independencia de su remisión a las autoridades autonómicas que pudieran existir.

La citada Orden estableció como fecha de puesta en funcionamiento de la A.I.P.I. el **1 de septiembre de 2025**. Asimismo, con el fin de garantizar su operatividad en la fase inicial, se acordó que, **hasta el 1 de noviembre de 2025**, el Ministerio continuara prestándole determinados servicios de apoyo, a efectos de que pudiera desarrollar su actividad durante dicho periodo con **pleno respeto a su autonomía funcional e independencia**.

Reglamento Delegado (UE) 2025/2003 de la Comisión, de 8 de septiembre de 2025, por el que se modifica el Reglamento (UE) 2021/821 del Parlamento Europeo y del Consejo en lo que concierne a la lista de productos de doble uso

El Reglamento Delegado de 8 de septiembre de 2025 marca un **hito significativo** en la evolución de la política europea en materia de control de bienes de doble uso.

Los bienes de doble uso comprenden aquellos **productos**, incluido los *softwares* y la tecnología que pueden tener **aplicaciones** tanto **civiles**, como **militares** o **nucleares**.

La Lista de Control, que se suele actualizar **anualmente**, incorpora en esta revisión un **nuevo bloque normativo** centrado específicamente en las **tecnologías cuánticas** y **criogénicas**, reconociendo su creciente relevancia.

Además, se han incluido dentro de los bienes de doble uso equipos y materiales para la fabricación y prueba de **semiconductores**, **circuitos integrados avanzados y ensamblajes electrónicos**, **recubrimientos** para aplicaciones a altas temperaturas, **máquinas** de **fabricación aditiva** (impresión en 3D), entre otros.

Desde una perspectiva de *Compliance*, esta actualización refuerza la necesidad de que las organizaciones **integren de forma efectiva los controles de exportación** en sus **Sistemas de *Compliance***, incorporando mecanismos de identificación, evaluación y gestión de **riesgos regulatorios asociados** a la **comercialización internacional de bienes de doble uso**, en línea con un enfoque de prevención y diligencia debida reforzada.

Real Decreto-ley 10/2025, de 23 de septiembre, por el que se adoptan medidas urgentes contra el genocidio en Gaza y de apoyo a la población palestina

El Real Decreto-ley 10/2025, de 23 de septiembre, **entró en vigor el pasado 24 de septiembre de 2025** y fue convalidado por el Congreso de los Diputados el 8 de octubre de 2025. Este Real Decreto-ley, regula cuatro (4) aspectos fundamentales:

- **Artículo 1. Prohibición de transferencias de material de defensa y de doble uso:** Este artículo establece la prohibición de exportar a Israel e importar desde allí material de defensa y productos de doble uso, conforme los anexos del Real Decreto 679/2014, de 1 de agosto. Algunos de los productos incluidos en los mismos son:

(i) compuestos químicos; (ii) reactores, tanques y equipos de mezclado diseñados para manipular sustancias químicas peligrosas; (iii) equipos y válvulas de contención de gases corrosivos o tóxicos; (iv) equipos de control de flujo y presión con precisión industrial o militar; (v) materiales reactivos mediante el sintetizado selectivo por láser. Asimismo, se impone la obligación de denegación de las solicitudes de autorización de tránsito del material mencionado.

- **Artículo 2. Combustibles de uso militar con destino Israel**: El Real Decreto-ley extiende la prohibición al tránsito de combustibles susceptibles de uso militar hacia Israel. Por ello, se suprime la excepción previa aplicable a los combustibles aeronáuticos JP-4, JP-5 y JP-8, de modo que su tránsito también será denegado. Asimismo, cualquier otro combustible con potencial uso final militar, si tiene como destino a Israel, también será objeto de denegación automática.
- **Artículo 3. Prohibición de importación aduanera de productos originarios de asentamientos israelíes:** El Real Decreto-ley prohíbe la importación de productos originarios de asentamientos israelíes en el Territorio Palestino Ocupado. Desde el 25 de septiembre de 2025, toda declaración aduanera de mercancías originarias de Israel deberá incluir información detallada sobre el lugar de origen de las mismas, incluyendo código postal y localidad de origen. La Agencia Estatal de la Administración Tributaria tendrá la potestad de denegar la importación de productos de estos asentamientos, y los incumplimientos se sancionarán conforme a la Ley Orgánica 12/1995, de Represión del Contrabando, con penas de prisión y multas.
- **Artículo 4. Publicidad ilícita**: El Real Decreto-ley considera ilícita la publicidad de productos y servicios originarios de asentamientos en el Territorio Palestino Ocupado.

Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, para la transposición de la Directiva (UE) 2024/1226 del Parlamento Europeo y del Consejo, de 24 de abril de 2024, relativa a la definición de los delitos y las sanciones por la vulneración de las medidas restrictivas de la Unión, y por la que se modifica la Directiva (UE) 2018/1673

El 25 de marzo de 2025, el Gobierno aprobó el **Anteproyecto de Ley Orgánica de modificación del Código Penal**, con el objetivo de transponer la **Directiva (UE) 2024/1226,** la cual establece las normas mínimas para tipificar como delitos penales las **infracciones graves a las medidas restrictivas impuestas por la UE, los cuales podrán ser penalmente responsable las personas jurídicas.**

Novedades legislativas

Las principales **novedades del Anteproyecto** son las siguientes:

- **Aumentar la pena en su mitad superior del delito de receptación y blanqueo de capitales** cuando los bienes provengan del incumplimiento de las medidas restrictivas de la UE.
- Creación de un nuevo título: **Título XXIII *bis* en el Libro II del Código Penal denominado "Delitos contra el espacio de libertad, seguridad y justicia de la Unión Europea"**, que garantiza que las conductas en él tipificadas sean constitutivas de delito cuando sean intencionadas y vulneren una prohibición u obligación que constituya una medida restrictiva de la UE.
- **Delito de vulneración de medidas restrictivas de la UE**: sanciona las operaciones ilícitas cuando el valor de los bienes o servicios supera los 10.000 euros, o siempre que afecten a material militar o productos de doble uso.
- **Delito de elusión de medidas restrictivas**: castiga el incumplimiento del deber de informar sobre fondos o recursos económicos sujetos a restricciones.
- **Delito de facilitación de entrada o tránsito**: penaliza permitir que personas físicas sancionadas ingresen o transiten por el territorio de la UE.

Asimismo, el **31 de octubre de 2025** tuvo lugar la **publicación oficial del Proyecto de Ley Orgánica para la transposición de la Directiva 2024/1226 relativa a la definición de delitos y las sanciones por la vulneración de las medidas restrictivas de la Unión en el Boletín Oficial de las Cortes Generales**. El objetivo principal es armonizar la legislación española con la normativa europea, fortaleciendo la eficacia de las sanciones impuestas por la UE.

A fecha de la publicación de esta *Newsletter*, el Proyecto de Ley se encuentra en el proceso de enmiendas realizado por la Comisión de Justicia.

Tribunales

- Sentencia de la Audiencia Nacional, Sala de lo Penal, Sección Apelación, 4/2025 de 21 de enero de 2025, Rec. 23/2024.
- Sentencia del Tribunal Supremo, Sala Segunda, de lo Penal, 223/2025 de 12 de marzo de 2025, Rec. 5765/2025.
- Sentencia del Tribunal Supremo, Sala Segunda, de lo Penal, 372/2025 de 11 de abril de 2025, Rec. 7151/2022.
- Sentencia del Tribunal Supremo, Sala Segunda, de lo Penal, 379/2025 de 30 de abril de 2025, Rec. 4603/2022.
- Sentencia del Tribunal Superior de Justicia de Cataluña, Sala de lo Contencioso-Administrativo, Sección 5ª, 1572/2025 de 5 de mayo de 2025, Rec. 809/2023.
- Sentencia del Tribunal Supremo, Sala Tercera, de lo Contencioso-Administrativo, Sección 4ª, 704/2025 de 4 de junio de 2025, Rec. 2188/2023.
- Sentencia del Tribunal Superior de Justicia de Madrid, Sala de lo Social, 441/2024 de 5 de junio de 2025, Rec. 441/2025.
- Auto de la Audiencia Provincial de Oviedo, Sección 2ª, 410/2025 de 18 de junio de 2025, Rec. 180/2025.
- Sentencia de la Audiencia Nacional, Sala de lo Penal, 9/2025 de 2 de julio de 2025.
- Sentencia del Tribunal General de la Unión Europea, Sala Décima, de 3 de septiembre de 2025. T-533/2023 (Latombe V. Comisión)
- Sentencia del Tribunal Supremo, Sala Segunda de lo Penal, Sentencia 768/2025 de 25 de Septiembre, Rec. 1008/2023
- Sentencia del Tribunal Supremo, Sala Segunda de lo Penal, Sentencia 836/2025 de 14 de Octubre, Rec. 432/2023.
- Auto de la Audiencia Nacional, Sala de lo Penal, Sección 2ª, 753/2025 de 10 de diciembre de 2025, Rec. 598/2025

Sentencia de la Audiencia Nacional, Sala de lo Penal, Sección Apelación, 4/2025 de 21 de enero de 2025, Rec. 23/2024

Esta sentencia se pronuncia sobre la posible aplicación de la **atenuante del art. 31 *quater* d) Código Penal** (en adelante, CP), en un caso donde una mercantil fue condenada por un delito de fraude fiscal, utilizando la estructura del **fraude carrusel** e involucrando operaciones comerciales intracomunitarias.

En su recurso, la mercantil solicitó la aplicación de dicha atenuante, argumentando que, **tras la comisión de los hechos delictivos y antes del inicio del juicio oral, había implantado un Sistema de Gestión de *Compliance* y designado a un *Compliance Officer***.

La Audiencia Nacional **rechazó la aplicación de la atenuante ya que consideró que no evidenciaban una voluntad real y efectiva de colaboración y reparación del daño** por parte de la compañía. El razonamiento del tribunal se basa en que el precepto 31 *quater* CP exige que dichas actuaciones demuestren un compromiso claro y efectivo con la prevención de potenciales delitos aplicables. El Tribunal percibió las medidas que la mercantil adoptó como **medidas formales o de apariencia (*Paper Compliance*)** con el simple objetivo de conseguir la atenuante y sin demostrar la intención de implantar una cultura de cumplimiento real.

Sentencia del Tribunal Supremo, Sala Segunda, de lo Penal, 223/2025 de 12 de marzo de 2025, Rec. 5765/2025

Esta sentencia confirma la **condena por delito de alzamiento de bienes a dos administradores** (uno de hecho, y el otro de derecho) y declara la **responsabilidad civil subsidiaria de la persona jurídica *ex* art. 120.4 CP**. El caso ilustra con claridad cómo la existencia de una estructura societaria, sin necesidad de que se haya declarado responsabilidad penal de la persona jurídica, **no exime a la sociedad de responder civilmente por los daños ocasionados por sus representantes**.

La sociedad fue utilizada como vehículo para realizar operaciones inmobiliarias que generaron ingresos significativos en concepto de IVA (más de 700.000 euros). Estas cantidades fueron sustraídas generando un perjuicio directo tanto para la Hacienda Pública como a otros acreedores. **La sociedad, pese a no haber sido penalmente condenada, fue declarada responsable civil subsidiaria por los actos cometidos en su seno**.

El Tribunal Supremo no entra a valorar si la sociedad contaba con un Sistema de *Compliance* con controles internos, remarcando que **la atribución de responsabilidad civil del art. 120.4 CP opera de forma objetiva cuando el delito se comete en el ejercicio de funciones o actividades sociales.** De este modo, **la implementación de Sistemas de *Compliance* no es invocable para la exención del pago de indemnizaciones**, especialmente cuando los administradores utilizan la estructura societaria para la comisión delictiva.

Esto refuerza la importancia de integrar en los Sistemas de *Compliance* herramientas de prevención de delitos transversales como la gestión desleal, insolvencias punibles u otros fraudes económicos.

Sentencia del Tribunal Supremo, Sala Segunda, de lo Penal, 372/2025 de 11 de abril de 2025, Rec. 7151/2022

En la presente sentencia, el Tribunal Supremo **estima el recurso de casación** interpuesto por parte de la persona jurídica condenada en instancias previas, por un delito de estafa agravada.

Así, el Tribunal deja claro que **acreditar un defecto estructural en los Sistemas de Gestión de *Compliance* es un elemento esencial e imprescindible en la atribución de la responsabilidad penal a las personas jurídicas.**

Cabe destacar cómo el Tribunal critica abiertamente la sentencia de la instancia previa, al observar cómo la responsabilidad penal a la persona jurídica fue atribuida sin fundamentación individualizada, derivada únicamente de los actos del propio administrador, y obviando la necesidad de acreditar un defecto estructural en el Sistema de Gestión de *Compliance*.

En un primer momento, la organización fue declarada culpable de un delito de estafa consistente en un engaño en la venta de franquicias por parte de su administrador, condenado además a cuatro años de prisión. De manera automática, y sin aportar exigencia probatoria alguna, se atribuyó responsabilidad penal a la sociedad, por los actos llevados a cabo por su administrador.

El Tribunal Supremo recuerda a los jueces y tribunales que **no se debe aplicar el régimen de heterorresponsabilidad en el momento de atribución de la responsabilidad penal**, ya que l**a culpabilidad sólo puede ser proclamada por un hecho propio**, en el presente caso, debería haber sido por la falta de unos planes de prevención o cumplimiento de la sociedad que evitaran el riesgo de que los directivos actuasen al margen de la ley cometiendo así un delito de estafa.

La sentencia subraya también la **importancia de que la persona jurídica cuente con una defensa propia y diferenciada mediante la cual pueda hacer valer el principio de contradicción, y que diferencie los intereses de la persona física (administrador) de los de la persona jurídica.**

Esta sentencia supone una garantía adicional de seguridad jurídica para las organizaciones, ya que se eleva el estándar probatorio necesario para atribuir la responsabilidad penal.

Sentencia del Tribunal Supremo, Sala Segunda, de lo Penal, 379/2025 de 30 de abril de 2025, Rec. 4603/2022

Esta resolución del Tribunal Supremo (en adelante, TS) aborda un caso de lesiones graves ocurridas durante un partido de fútbol amateur, pero lo relevante desde la perspectiva de *Compliance* lo encontramos en las implicaciones que extrae el TS sobre la **posición de garante de las organizaciones que promueven actividades que puedan entrañar algún riesgo**.

Aunque el debate procesal se centra en la vulneración de garantías durante el juicio, lo relevante en materia de *Compliance* es el **llamamiento que hace el Supremo para reforzar la diligencia organizativa de entidades promotoras de eventos**, como en este caso, partidos de fútbol no profesionales. Así, indica que estas asociaciones, que se configuran como personas jurídicas, deben **implementar mecanismos preventivos efectivos que minimicen el riesgo de conductas delictivas por parte de sus miembros o participantes, incluso si se trata de actividades informales, deportivas o lúdicas**.

Este pronunciamiento **amplía la exigencia de prevención de conductas delictivas** sobre entidades sin ánimo de lucro o asociaciones deportivas que igualmente pueden enfrentarse a consecuencias jurídicas si no adoptan medidas razonables de control sobre sus actividades.
Esta sentencia refuerza la necesidad de **ampliar la aplicación práctica de los Sistemas de Gestión de *Compliance* más allá del entorno corporativo clásico**, reforzando la importancia de que asociaciones, organizaciones, y otras personas jurídicas sin ánimo de lucro, establezcan medidas de prevención ante actuaciones indeseables que puedan desencadenar en la comisión de delitos. La ausencia de controles adecuados puede abrir la puerta a responsabilidades civiles subsidiarias, reputacionales e incluso penales.

Sentencia del Tribunal Superior de Justicia de Cataluña, Sala de lo Contencioso-Administrativo, Sección 5ª, 1572/2025 de 5 de mayo de 2025, Rec. 809/2023

La Sentencia aborda la **evaluación de la suficiencia y eficacia de un Programa de Cumplimiento en materia de defensa de la competencia** como elemento determinante para la eventual **revisión de una prohibición de contratar**. El pronunciamiento se dicta en el marco de un **recurso contencioso-administrativo** interpuesto por la parte actora frente a la **desestimación presunta** de su segunda solicitud de levantamiento de las prohibiciones de contratar impuestas en 2021, sustentando su pretensión en la implementación de un Programa de Cumplimiento.

El Tribunal parte de una premisa esencial: **la mera existencia formal de un Programa de Cumplimiento no acredita, por sí misma, su eficacia**. En este contexto, el TSJ **analiza el contenido material y la implementación práctica** del Programa, identificando una serie de **déficits estructurales** que impiden considerarlo eficaz.

En particular, en relación con las **medidas disciplinarias**, el Tribunal destaca: (i) la **ausencia de cláusulas rescisorias** como medida disciplinaria en los contratos de directivos y trabajadores aplicable a toda la plantilla; (ii) que **no basta** con que el personal conozca la posible sanción por incumplir el Código de Conducta u otros documentos del Programa, dado que la introducción de una **cláusula rescisoria**, especialmente respecto de empleados que participaron en las conductas sancionadas, presenta un **mayor efecto disuasorio**; (iii) la **falta de graduación de infracciones** y de identificación clara de conductas infractoras; y (iv) la **ausencia de sanciones** al personal infractor, lo que compromete la credibilidad y capacidad preventiva del sistema.

Respecto a la **comunicación y adhesión al Programa**, se subraya: (i) la **falta de acceso efectivo** de la plantilla a los documentos del modelo y la **ausencia de firma de compromiso**; y (ii) la **inexistencia de cláusulas de compromiso de cumplimiento**.

En materia de **formación y sensibilización**, la Sala concluye que no se acredita un **plan de formación eficaz**, y cuestiona la **ineficacia de la política de incentivos.** En cuanto al **canal de denuncias**, se aprecia la no especificación de cómo remitir **denuncias anónimas vía email.**

Especial atención merecen las consideraciones relativas al responsable del diseño y el control del Programa de Cumplimiento (**Comité de *Compliance* y *Compliance Officer***). El Tribunal aprecia: (i) **falta de independencia** y **conflictos de intereses**, al integrar el órgano personas que habrían sido partícipes de las conductas sancionadas; (ii) **insuficiencia de conocimientos** especializados de sus miembros; y (iii) la **ausencia de apoyo de asesores externos**, factor que, en contextos de elevada complejidad regulatoria, puede resultar determinante para dotar de solvencia técnica y credibilidad al modelo.

Finalmente, en relación con el **mapa de riesgos**, el TSJ identifica carencias sustantivas: (i) no se han incorporado todas las conductas relevantes, incluyendo la infracción vinculada al segundo expediente; y (ii) se aprecia la ausencia de controles necesarios, como la incorporación de una **cláusula de compromiso de cumplimiento de normativa de competencia** en supuestos de participación en una misma licitación de empresas pertenecientes al mismo grupo.

Sentencia del Tribunal Supremo, Sala Tercera, de lo Contencioso-administrativo, Sección 4ª, 704/2025 de 4 de junio de 2025, Rec. 2188/2023

La resolución resulta relevante en los **procedimientos de gestión de investigaciones internas**, bajo el mandato de la Ley 2/2023. El Alto Tribunal recuerda en primer lugar que **los principios inspiradores del Derecho Penal son trasladables al Derecho sancionador administrativo**.

En este sentido, el funcionario público fue sancionado por desobediencia grave al no responder a las preguntas que le hizo el instructor, en el curso de las diligencias informativas, previas a la apertura de un expediente disciplinario, donde los funcionarios públicos se deben al principio de colaboración para esclarecer los hechos.

Ahora bien, el Tribunal destaca que este derecho colisiona con otro derecho de rango constitucional, el derecho de no declarar contra uno mismo como garantía del derecho de defensa. Por tanto, **se debe poner el foco en cada caso para respetar las garantías procesales que revisten estos procedimientos**. En este supuesto, los hechos eran claros y el responsable estaba identificado, coincidiendo con el funcionario que formaba parte de las diligencias informativas.

En este marco, **el TS se pronuncia a favor de la negativa de responder a las preguntas del instructor cuando estas tengan un contenido claramente incriminatorio**. El Tribunal concluyó que este **derecho a la no autoincriminación se extiende al procedimiento presancionador**, y por este motivo, el funcionario no podía ser sancionado.

Sentencia del Tribunal Superior de Justicia de Madrid, Sala de lo Social, 441/2024 de 5 de junio de 2025, Rec. 190/2025

Esta sentencia aborda el despido disciplinario de una Directora General que formuló una denuncia interna contra la Directora de RRHH, acusándola de haber despedido a un empleado por su orientación sexual. Lo relevante desde la esfera del *Compliance* es el análisis que realiza el TSJ sobre el **uso malicioso del canal ético, la buena fe contractual y los límites de la protección a los informantes**.

La investigación interna, tramitada por el Comité de Cumplimiento de la empresa, concluyó que **la denuncia carecía de indicios mínimos y se utilizó para perjudicar por motivos personales a una compañera**. El tribunal destaca que **la finalidad de la denuncia no fue ética ni preventiva, sino reactiva y lesiva** para una compañera, convirtiéndola en una herramienta de presión y descrédito personal.

El TSJ revoca la declaración de despido improcedente del juzgado de instancia y lo califica como procedente, al considerar que se produjo una **transgresión grave de la buena fe contractual.** Asimismo, subraya que no toda denuncia interna goza de protección automática, ya que **cuando se formula una denuncia de forma infundada y con una finalidad perjudicial, ello puede constituir causa válida de despido**.

Encontramos en este caso un claro ejemplo de cómo **la protección frente a represalias o consecuencias que nos ofrece la Ley 2/2023 no cubre denuncias infundadas o maliciosas**.

Auto de la Audiencia Provincial de Oviedo, Sección 2ª, 410/2025 de 18 de junio de 2025, Rec. 180/2025

El Auto resulta de especial interés por la integración de un análisis expreso del marco de **protección del informante previsto en la Ley 2/2023**.

El caso se origina a raíz de la interposición de recurso de apelación contra el sobreseimiento provisional de unas diligencias incoadas tras denunciarse, entre otros hechos no objeto del recurso, la existencia de un **correo electrónico anónimo en el que presuntamente se utilizaban datos personales del denunciante** (números de teléfono, listados de llamadas) y se le imputaban determinadas conductas, revelándose así información personal y hábitos relativos a su vida sexual.

La Sala centra su análisis en un extremo clave: las deducciones realizadas por el emisor del correo —al examinar listados de llamadas asociados a una línea telefónica y cotejarlos con números de contacto publicados en páginas web de prostitución— y la posterior puesta a disposición de dicha información a un medio de comunicación, no integran conducta ilícita, y en particular no pueden subsumirse en los tipos de **difusión, revelación o utilización de datos personales**.

El Auto añade que la actuación del comunicante se encuadra en el ámbito de protección definido por la Ley 2/2023 al tratarse de una comunicación dirigida a revelar una posible irregularidad: concretamente, el posible uso ilícito de una línea telefónica pública asignada al recurrente, completamente ajeno a los fines propios de su función.

En concreto, **la resolución pone el foco en el ámbito subjetivo y objetivo de la protección, recordando que el artículo 2 de la Ley 2/2023 protege a quienes informen, mediante los procedimientos previstos, sobre acciones u omisiones que puedan constituir infracción penal o infracción administrativa grave o muy grave**.

Sin embargo, el elemento determinante en el supuesto analizado es la mención específica del artículo 27, relativo a la **revelación pública como mecanismo de comunicación**: se enfatiza que el régimen de protección del Título VII resulta aplicable sin necesidad de condición adicional cuando la persona haya revelado información directamente a la prensa en el marco del ejercicio de la libertad de expresión y del derecho a comunicar información veraz, conforme al marco constitucional y su normativa de desarrollo.

Sentencia de la Audiencia Nacional, Sala de lo Penal, 9/2025 de 2 de julio de 2025.

Este mes de julio se ha condenado a una mercantil como autora del delito de fraude de subvenciones del art. 310 CP en relación con el art. 308.1 CP.

La compañía solicitó y obtuvo en 2018 ayudas públicas europeas provenientes del Fondo Español de Garantía Agraria (en adelante, FEGA) con el objetivo de llevar a cabo proyectos de transformación, comercialización y desarrollo de productos agrarios (frutas y vegetales), por un importe total de 3,8 millones de euros. Paralelamente, la compañía solicitó un préstamo de 6 millones al Institut Català de Finances, del cual le fue bonificado un 2% de los intereses por parte de la Direcció General de Indústria.

El conflicto recae en que la compañía no informó de la recepción de esta bonificación al FEGA, incumpliendo así la obligación de declarar otras ayudas públicas recibidas o solicitadas, lo que determinaba la incompatibilidad entre dichas ayudas según la normativa aplicable (se recibió una ayuda autonómica correspondiente a la bonificación de intereses y otra ayuda estatal proveniente del FEGA).

Asimismo, la **compañía solicitó las atenuantes del art. 31 *quater* c) y d) CP.**

En relación con la **reparación del daño** (art. 31 *quater* c) CP, la compañía se limitó a prestar la debida caución económica, pero el juez indicó que, **la reparación del daño exige el pago del principal debido y de sus intereses,** por tanto, **rechazó la aplicación de la misma**.

En cuanto a la aplicación de la atenuante del art. 31 *quater* d) CP, el juez la admitió por la **aplicación de ciertas medidas de prevención de delitos antes del inicio del juicio oral**.

Aun así, el tribunal manifiesta ciertas **dudas sobre la autenticidad del programa de cumplimiento aportado** (una *due diligence* con fecha 2017), **ya que se trata de una simple fotocopia no autentificada presentada repentinamente en el acto del juicio sin haber aportado ningún documento durante la fase de instrucción**, que no fue referenciada por ninguno de los acusados a lo largo de toda esta fase, y de la cual no se hizo mención expresa de su existencia en el escrito de conclusiones provisionales de la condenada.

No obstante, y **a pesar de su contenido genérico y carente de elementos estructurales esenciales** (como responsables de control o protocolos operativos), **el juzgado le reconoce valor atenuante al programa de cumplimiento aportado por haber sido implementado formalmente con posterioridad a los hechos**.

Sentencia del Tribunal General de la Unión Europea, Sala Décima, de 3 de septiembre de 2025. T-533/2023 (Latombe V. Comisión)

El Sr. Philippe Latombe, ciudadano francés y usuario de diversas plataformas digitales que transfieren datos personales a EEUU, interpuso un **recurso de anulación** contra la **Decisión de Ejecución (UE) 2023/1795 de la Comisión Europea**, por la que se aprobó el ***Data Privacy Framework*** **(DPF)** o **Marco de Transferencia de Datos Personales entre la UE y los EEUU**, alegando que dicho marco no garantiza un **nivel de protección de datos sustancialmente equivalente** al exigido por el Reglamento General de Protección de Datos (en adelante, **RGPD**) y la **Carta de Derechos Fundamentales**.

El **Tribunal General de la Unión Europea** desestimó íntegramente el recurso y confirmó la validez de la Decisión, declarando **adecuado** el nivel de protección aplicable a los datos personales transferidos a EEUU en el marco del DPF. Asimismo, por razones de **buena administración de la justicia**, el Tribunal **se abstuvo de pronunciarse** sobre la inadmisibilidad planteada por la Comisión y entró directamente en el fondo, concluyendo que el recurso era **infundado**.

A efectos prácticos, el Tribunal respaldó el estándar ya consolidado por el Tribunal de Justicia de la Unión Europea, reiterando que el artículo 45 RGPD exige que el tercer país garantice un nivel de protección **sustancialmente equivalente, no idéntico**, y que la apreciación de la Comisión en materia de adecuación está sujeta a un **control judicial estricto**.

Sentencia del Tribunal Supremo, Sala Segunda de lo Penal, Sentencia 768/2025 de 25 de septiembre, Rec. 1008/2023

La sentencia aborda la responsabilidad penal de una **sociedad mercantil** acusada juntamente con su administradora por un **delito continuado de estafa**. La persona física había ejecutado maniobras fraudulentas mediante falsas ofertas de empleo que encubrían cursos de formación con ánimo de lucro. En este sentido, **la Audiencia Nacional había considerado que los actos de la administradora eran imputables también a la sociedad, entendiendo que ésta se había beneficiado del fraude**. Sin embargo, el **recurso de casación** planteado por la mercantil cuestionaba precisamente esa extensión automática de responsabilidad, sosteniendo que no se había probado la existencia de ningún defecto organizativo ni de un sistema de control ineficaz que permitiera o facilitara el delito.

Por ello, en su resolución, el Tribunal Supremo delimita con precisión el núcleo de la responsabilidad penal de las personas jurídicas conforme al artículo 31 *bis* del CP, afirmando que **la imputación a una entidad requiere la acreditación de un defecto organizativo grave, es decir, una carencia real en los mecanismos de control o supervisión que revele una infracción del deber de prevención de delitos**. No basta con demostrar que una persona física vinculada a la empresa haya cometido el delito, sino que **es necesario probar que dicho comportamiento fue posible por un fallo estructural propio de la organización**.

Asimismo, el Tribunal subraya que **la responsabilidad penal corporativa no puede ser objetiva ni automática**. De esta manera, rechaza expresamente la responsabilidad vicarial, aclarando que el modelo español no permite trasladar a la persona jurídica la culpabilidad del directivo o empleado de forma directa y que **la entidad solo responde cuando el delito constituye la manifestación de su propia desorganización o de una cultura de incumplimiento**.

Además, **se fija la carga de la prueba en el Ministerio Fiscal, que debe demostrar tanto la comisión del delito por la persona física como la existencia del incumplimiento organizativo por parte de la empresa**.

Por último, el Supremo enfatiza que la presunción de inocencia también ampara a las personas jurídicas, y que la falta de prueba del defecto de control impide la condena. En este caso, **al no acreditarse que la sociedad careciera de un sistema razonable de supervisión ni que existiera una política institucional tolerante con el fraude, el Tribunal concluye que no hubo culpa organizativa y, por tanto, absuelve a la empresa**.

Sentencia del Tribunal Supremo, Sala Segunda de lo Penal, Sentencia 836/2025 de 14 de octubre, Rec. 432/2023

En la presente sentencia, **el Tribunal Supremo absuelve a la persona jurídica por un delito de alzamiento de bienes por no probarse la existencia de un defecto estructural en la empresa que hubiera permitido o facilitado la comisión de dicho delito**.

El Tribunal Supremo enfatiza que **la responsabilidad penal de las personas jurídicas** no se deriva automáticamente de la conducta delictiva de sus miembros, sino que **requiere que se demuestre que el delito fue cometido por una persona física actuando en el contexto de sus funciones dentro de la empresa**, conforme el artículo 31 *bis* del CP. Asimismo, **para que una empresa sea responsable penalmente**, además, **debe probarse que la estructura organizativa de la empresa facilitó o permitió la comisión del delito**.

En este caso, el Tribunal subraya que **no se acreditó que la empresa careciera de controles internos adecuados** ni que su estructura favoreciera la realización del delito de alzamiento de bienes. Es decir, **no hubo evidencia de que la falta de medidas preventivas de la empresa facilitara la acción delictiva de las personas físicas**. Asimismo, el Tribunal Supremo destaca que **la carga de la prueba recae sobre la acusación, que debe demostrar no solo que la persona jurídica no cumplió con sus deberes de supervisión, sino que esa omisión fue grave y esencial para la comisión del delito**.

Dado que no se aportaron pruebas suficientes que indicaran que la empresa facilitó el alzamiento de bienes ni que la estructura organizativa fue deficiente, el Tribunal absuelve a la empresa de responsabilidad penal, concluyendo que **no se demostró que la persona jurídica tuviera un papel activo en la comisión del delito**.

En definitiva, **ambas sentencias mencionadas en la presente *Newsletter* contravienen el criterio de la anterior Sentencia del Tribunal Supremo, Sección Primera, Sentencia 298/2024, de 8 de abril, Rec. 6489/2021**, sobre la responsabilidad penal de la persona jurídica, en la que se establecía la carga de alegar y demostrar la existencia de un Programa de *Compliance* en la defensa. Por ende, **el criterio actual sobre a quién le corresponde la carga de la prueba versa sobre la acusación**.

Auto de la Audiencia Nacional, Sala de lo Penal, Sección 2ª, 753/2025 de 10 de diciembre de 2025, Rec. 598/2025

La resolución ofrece un recordatorio particularmente claro sobre los límites legales de la **responsabilidad penal de las personas jurídicas** y las exigencias mínimas de tipicidad y concreción fáctica para la admisión a trámite de una querella.

La resolución analiza el recurso de apelación interpuesto frente al auto que inadmitió a trámite la querella presentada contra tres multinacionales farmacéuticas por presuntos delitos de manipulación de genes humanos (art. 159 CP), utilización de ingeniería genética para producir armas biológicas (art. 160 CP) y delitos contra la salud pública (arts. 359 a 362 y 378 CP). El núcleo del razonamiento judicial es contundente y evidente**: no todos los delitos del Código Penal son susceptibles de comisión por personas jurídicas**, y la querella no supera este filtro básico.

En primer lugar, la Audiencia confirma que los delitos de los artículos 159 y 160 CP no pueden ser cometidos por personas jurídicas en el ordenamiento penal español. Frente al argumento de la parte recurrente, que invocaba el artículo 162 CP, el Tribunal recuerda que dicho precepto no habilita la atribución de responsabilidad penal a la persona jurídica, sino que se limita a permitir, con carácter facultativo, la **imposición de consecuencias accesorias del artículo 129 CP** cuando el autor del delito sea una persona física integrada en una organización o sociedad.

En segundo término, respecto de los delitos contra la salud pública, la Audiencia admite que el **artículo 366 CP sí contempla la posible responsabilidad penal de la persona jurídica** para determinados tipos. Sin embargo, la querella fracasa por **falta absoluta de concreción**: no se identifica qué delito concreto se imputa, qué hechos específicos lo integrarían ni se aporta un mínimo principio de prueba que permita sustentar la imputación. El Tribunal es especialmente claro al **rechazar que la jurisdicción penal pueda servir de cauce para investigaciones prospectivas**, expresamente prohibidas en nuestro sistema.

Otros acuerdos y resoluciones sancionadoras en materia de *Compliance*

MOLINS Compliance

- La AEPD recibió 19.000 reclamaciones en 2024, con la IA, los espacios de datos y los neurodatos entre sus retos prioritarios.
- La AEPD no permite fotocopiar el DNI o pasaporte en hoteles con multas que superan los 10.000 euros.
- Sancionada con 120.000 euros una empresa por desvelar la identidad de unos denunciantes.
- Banca March se enfrenta a una multa de 605.000 euros por infringir la norma antiblanqueo en una cuestión formal.
- Banco sancionado con 28 millones de libras por fallos en controles de delitos financieros.
- La Agencia Tributaria acuerda investigar a los neobancos por posibles vínculos con el Blanqueo de Capitales.
- BBVA, condenada a indemnizar a una clienta víctima de "*phishing*" con la pérdida patrimonial experimentada: 9.900 euros.
- Multas de la CNMC por publicidad encubierta.
- Multa de la CNMV de 10 millones de euros a Deutsche Bank por infracciones al vender derivados de divisas.
- La CNMV sanciona a Bestinver con una multa de 100.000 euros por no informar de forma "clara e imparcial" de las características de un producto.
- La CNMC autoriza con compromisos una *joint venture* en el sector del hormigón
- Reversión automática de las sanciones contra Irán: el Consejo restablece las medidas restrictivas.
- AEPD sanciona con 10 millones de euros a Aena por su sistema de reconocimiento facial en aeropuertos.
- La CNMC (*S/0011/23, Eólica del Alfoz*) fija por primera vez el alcance y la duración de la prohibición de contratar directamente en una resolución sancionadora.
- Multa de la Oficina Antifrau de Catalunya (OAC) a una empresa por adoptar represalias contra una informante.

Otros acuerdos y resoluciones sancionadoras en materia de *Compliance*

MOLINS Compliance

La AEPD recibió 19.000 reclamaciones en 2024, con la IA, los espacios de datos y los neurodatos entre sus retos prioritarios

La Agencia Española de Protección de Datos (en adelante, AEPD) hizo pública su Memoria Anual correspondiente al ejercicio 2024, en la que se examinan los **principales desafíos emergentes en materia de protección de datos**, así como **las tendencias normativas y estadísticas** más relevantes, incluyendo el volumen total de resoluciones adoptadas.

Durante dicho ejercicio, la AEPD registró 18.884 reclamaciones, lo que ha supuesto un descenso del 13% respecto del año 2023, si bien las cifras continúan situándose por encima de los niveles previos a dicho ejercicio. En cuanto a la actividad sancionadora, se concluyeron 414 procedimientos sancionadores y de apercibimiento, de los cuales 281 finalizaron con la imposición de sanción económica. Los **cinco (5) sectores que registraron un mayor volumen** económico sancionador fueron: el sector de la energía/agua (que ha pasado de 115.500 euros en 2023, a 11.680.600 euros en 2024); entidades financieras/acreedoras (5.356.900 euros); servicios de Internet (que ha ascendido a los 4.547.380 euros frente a 1.058.700 euros de 2023); telecomunicaciones (3.330.000 euros frente a 1.942.000 euros de 2023) y contratación fraudulenta (2.538.200 euros).

Estos cinco (5) sectores concentraron en conjunto el 23% del importe total de sanciones impuestas, que en 2024 ascendió a 35.592.200 euros.

Asimismo, la AEPD reconoce también que el reto principal al que se enfrenta es el uso y desarrollo de la IA y el análisis de su impacto en la protección de datos y los derechos fundamentales.

La AEPD no permite fotocopiar el DNI o pasaporte en hoteles con multas que superan los 10.000 euros

La AEPD ha **matizado el Real Decreto 933/2021** que establece la obligación del titular de la actividad de hospedaje de recoger determinados datos de sus huéspedes, defendiendo que esta medida "no autoriza a solicitar una copia del documento de identidad del cliente", argumentando que supondría una **vulneración del principio de minimización de datos**, y supondría un tratamiento de datos de carácter personal excesivo.

Para dar fin a tal práctica, la **AEPD ha venido sancionando a los infractores sistemáticamente durante los últimos meses** y años con multas de hasta 15.000 euros.

Además, la AEPD extiende esta restricción a cualquier otro sector en el que se dé un uso indebido o excesivo de los datos de carácter personal de los terceros con los que se relacionan las personas jurídicas.

Recordamos la reciente sanción a una empresa de grúas, después de que un empleado fotografiara el DNI de un cliente, lo que supuso una multa de 11.000 euros.

Sancionada con 120.000 euros una empresa por desvelar la identidad de unos denunciantes

La AEPD condenó a una empresa funeraria a pagar 120.000 euros, por no garantizarse adecuadamente la confidencialidad de los datos de carácter personal de varios empleados en relación con un caso de acoso laboral y su resolución.

Así pues, tras haberse tramitado el protocolo de acoso, la empresa envió un correo electrónico masivo con la resolución del caso, donde constaba tanto la identidad como el puesto de trabajo de los cinco denunciantes. Como consecuencia de esta comunicación, toda la compañía tuvo conocimiento de los acontecimientos y de las personas que habían participado en ellos.

La AEPD ha considerado que la funeraria **vulneró el artículo 5.1.f) RGPD por no garantizar debidamente la confidencialidad de los datos de carácter personal recabados con el protocolo de acoso**, y la sancionó con una **multa de 200.000 euros**, cantidad que quedó reducida en un 40%, por reconocer la empresa el error y pagar dentro del plazo voluntario.

Banca March se enfrenta a una multa de 605.000 euros por infringir la norma antiblanqueo en una cuestión formal

A finales de enero de 2025, Banca March fue multada con una sanción de un importe que ascendía a 605.424 euros, por infringir la normativa de prevención de blanqueo de capitales. Según el SEPBLAC, la multa responde a **fallos en el procedimiento de diligencia debida** y en la identificación de clientes, lo que elevó el riesgo de operaciones ilícitas dentro de la entidad financiera.

La resolución del SEPBLAC ha sido recurrida ante el TS por la entidad, ya que lo considera un fallo "meramente formal" y defiende su actuación.

La controversia recae en la apertura de una cuenta a unos clientes que ya había regularizado la Agencia Tributaria, y contaban con la validación de la misma. Banca March aceptó el ingreso tras comprobar formalmente su validación por la Agencia Tributaria, pero **sin llevar a cabo las medidas reforzadas de diligencia** debida que impone la legislación de prevención de blanqueo de capitales.

Otros acuerdos y resoluciones sancionadoras en materia de *Compliance*

MOLINS Compliance

Banco sancionado con 28 millones de libras por fallos en controles de delitos financieros

El banco digital MONZO ha sido sancionado por parte de la Autoridad de Conducta Financiera del Reino Unido a una multa **de 28 millones de libras esterlinas** por fallos graves en la prevención del blanqueo de capitales y la financiación del terrorismo. Se pudo constatar que el banco **no había implementado controles adecuados** para la identificación y gestión de riesgos de delitos financieros.

En la misma línea, la Comisión de Supervisión del Sector Financiero de Luxemburgo ha multado con **233.000 euros a la filial luxemburguesa del grupo Allianz** por incumplimiento en sus obligaciones de prevención del blanqueo de capitales y financiación del terrorismo.

Estas sanciones nos permiten ver la **tendencia internacional a reforzar la diligencia debida** en materia de prevención de blanqueo de capitales y financiación del terrorismo. Sobre todo, en un sector tan relevante y expuesto como el sector bancario.

La Agencia Tributaria acuerda investigar a los "neobancos" por posibles vínculos con el blanqueo de capitales

La Agencia Tributaria ha anunciado una investigación a los "neobancos" con el objetivo de **identificar nuevos métodos de blanqueo de capitales**. La regulación menos estricta y el anonimato de algunas de estas nuevas entidades financieras han llamado la atención de las autoridades fiscales y de prevención del fraude.

Así pues, se va a colaborar con la Unidad de Inteligencia Financiera y el Banco de España para el **análisis de patrones sospechosos que puedan encubrir operaciones fraudulentas**.

También se advierte que, si se detectan "brechas regulatorias", podría impulsarse una reforma normativa para endurecer los requisitos de supervisión y trazabilidad de estas entidades. Todo ello **en línea con las tendencias europeas** y siguiendo las recomendaciones de la Autoridad Bancaria Europea.

BBVA, condenada a indemnizar a una clienta víctima de "*phishing*" con la pérdida patrimonial experimentada: 9.900 euros

La víctima recibió un SMS incrustado en el hilo de mensajes del BBVA informándole de una supuesta operación no autorizada y, a continuación, recibió una llamada telefónica por parte de una persona que se identificó falsamente como empleada del banco.

La clienta proporcionó sus credenciales y códigos de seguridad, bajo la creencia simulada del entorno aparentemente legítimo.

La actual doctrina del Tribunal Supremo establece que, **salvo dolo o negligencia grave del cliente, el banco es responsable de las deficiencias en sus sistemas de seguridad.** Además, hay jurisprudencia de la Audiencia Provincial de Santander, que establece que la conducta de un usuario ante un intento de fraude bien elaborado no puede considerarse negligencia si actúa bajo angustia y/o confusión.

La noticia resalta el **deber de diligencia que deben aplicar los bancos**, con el objetivo de evitar operaciones fraudulentas, y advierte de la gravedad de las brechas de seguridad que permiten accesos completos a los datos de los clientes por parte de terceros malintencionados.

Multas de la CNMC por publicidad encubierta

La Comisión Nacional de los Mercados y la Competencia (en adelante, CNMC) ha multado recientemente a diferentes compañías, entre ellas, DAZN y Atresmedia, ambas por emitir publicidad encubierta en su programación, con cuantías de **más de 180.000 euros**.

Ambos sancionados emitieron mensajes y contenidos publicitarios sin cumplir con los requisitos legales de identificación y diferenciación de la publicidad. Según la Ley General de Comunicación Audiovisual, **los contenidos publicitarios deben estar claramente identificados y diferenciarse del resto de programación**, extremos que ambos incumplieron.

Todas las sanciones han sido reconocidas y pagadas anticipadamente para gozar de una reducción sobre los importes de las mismas.

Con ello refuerzan el objetivo de proteger a los espectadores y consumidores, destacando la importancia y obligación de distinguir claramente el contenido editorial y publicitario.

Multa de la CNMV de 10 millones de euros a Deutsche Bank por infracciones al vender derivados de divisas

La Comisión Nacional del Mercado de Valores (en adelante, CNMV) ha sancionado al Deutsche Bank por infracciones "muy graves" en la comercialización de derivados de divisas, imponiéndole una **multa de 10 millones de euros**.

En la resolución publicada en el BOE el pasado 29 de enero, la CNMV asocia la sanción a una infracción "muy grave" sobre el cumplimiento de las obligaciones de información a los clientes a los que presta servicios de inversión.

Otros acuerdos y resoluciones sancionadoras en materia de *Compliance*

MOLINS Compliance

Aparte de la sanción económica, **la CNMV también ha suspendido, por un plazo de un año, la actividad de asesoramiento en materia de inversión** sobre productos derivados de mercados OTC (*Over The Counter*) complejos que incorporen estructuras sobre divisas.

Este expediente sancionador nace a raíz de una investigación interna de la matriz de Deutsche Bank a su sucursal española, que destapó una serie de malas prácticas que se materializaron en despidos, indemnizaciones y, finalmente, la sanción de la CNMV.

Por el momento, la resolución de la CNMV solamente ha devenido firme en vía administrativa, y Deutsche Bank ha comunicado su intención de recurrir dicha decisión, confiando en sus procesos y controles internos.

Este es un caso que nos ilustra claramente sobre **la importancia de los procesos y controles internos para evitar incumplimientos o irregularidades** en instancias anteriores a las sanciones penales.

La CNMV sanciona a Bestinver con una multa de 100.000 euros por no informar de forma "clara e imparcial" de las características de un producto

La gestora de fondos Bestinver Gestión, S.A., S.G.I.I.C. (en adelante, Bestinver) ha sido sancionada recientemente por parte de la CNMV por no informar a sus clientes de forma "imparcial, clara y no engañosa" sobre las características de uno de sus productos, constituyendo una infracción muy grave tipificada en el artículo 284.1 de la Ley del Mercado de Valores.

La mercantil mencionada ha decidido no recurrir la sanción en vía administrativa, por lo que dicha sanción ya es firme.

Bestinver ha señalado públicamente que ha colaborado plenamente con la inspección de la CNMV y **ha revisado sus procedimientos para que no vuelva a ocurrir**.

Se destaca de dicha sanción la importancia de **implementar y mantener procedimientos** y protocolos de actuación para prevenir la materialización de irregularidades que puedan conllevar una sanción.

La CNMC autoriza con compromisos una *joint venture* en el sector del hormigón

Cuatro compañías del mismo sector, Ribalta Pujol, Fiasa Mix, Calaf Grup y Gualtosal, plantean a la CNMC la creación de una *joint venture* para gestionar y explotar **15 plantas de producción de hormigón fresco**, centralizando así una parte relevante de su actividad productiva.

En la revisión de la operación, la CNMC identifica como riesgo central que la *joint venture* pudiera ser utilizada como **plataforma para el intercambio de información sensible** entre las empresas **competidoras** en el mercado del hormigón y que, en algunos casos, también participan en mercados relacionados. Asimismo, ello podría generar **riesgos de efectos coordinados**, facilitando alineamientos en precios, condiciones comerciales o estrategias de mercado.

Para neutralizar este riesgo, la CNMC autoriza la operación condicionada al cumplimiento de compromisos obligatorios:

- **Aprobar un Protocolo interno de competencia**, con medidas operativas sobre clasificación y confidencialidad de la información, reglas de tratamiento, definición de responsabilidades y salvaguardas organizativas para asegurar la separación entre el Consejo y el Órgano de gestión y evitar injerencias de las empresas en la gestión diaria; además, su aprobación debe realizarse en los plazos previstos y **cualquier modificación requiere la conformidad previa de la CNMC**.
- **Modificar el Pacto de socios:** incorporando formalmente estas salvaguardas en el marco contractual de gobierno de la *joint venture* y reforzando la independencia y autonomía del órgano de gestión, incluyendo la figura del Director General, como elemento esencial para evitar una gestión influida por intereses competitivos de las matrices.

En definitiva, la CNMC recuerda que **no revisa ni valida automáticamente** todas las cláusulas accesorias del acuerdo y que corresponde a las empresas realizar la **autoevaluación** del encaje competitivo de esas restricciones. La *joint venture* se permite, pero la resolución subraya que la cooperación empresarial tiene **límites estrictos en Derecho de la competencia**, cuya observancia recae directamente en las empresas implicadas.

Otros acuerdos y resoluciones sancionadoras en materia de *Compliance*

MOLINS Compliance

Reversión automática de las sanciones contra Irán: el Consejo restablece las medidas restrictivas

El 14 de julio de 2015, Irán alcanzó con los cinco miembros permanentes del Consejo de Seguridad de las Naciones Unidas (China, Francia, Federación de Rusia, Reino Unido, Estados Unidos), con Alemania y el apoyo de la **Alta Representante de la UE**, el **Plan de Acción Integral Conjunto (PAIC)**, orientado a garantizar que el programa nuclear iraní tuviera fines exclusivamente civiles y pacíficos. Este acuerdo fue refrendado por la **Resolución 2231 (2015)** del Consejo de Seguridad de Naciones Unidas, que establecía el marco y el calendario para **poner fin a las sanciones** vinculadas a actividades nucleares, culminando el **16 de enero de 2016.** En coherencia con ello, la UE adoptó en octubre de 2015 la **Declaración 2015/C 345/01**, retirando las sanciones europeas relacionadas con actividades nucleares, aunque manteniendo expresamente la posibilidad de **reintroducirlas en caso de incumplimientos significativos** de Irán.

El **28 de agosto de 2025**, Francia, Alemania y el Reino Unido notificaron al Consejo de Seguridad de las Naciones Unidas que, a su juicio, Irán estaba incurriendo en un **incumplimiento significativo** de sus compromisos en el marco del PAIC. Esta notificación activó el mecanismo de **"reversión automática**" que prevé la reintroducción de sanciones de las Naciones Unidas tras un periodo de 30 días, salvo que el Consejo de Seguridad adopte una nueva resolución que lo impida. El **29 de agosto de 2025**, la Alta Representante de la UE, Francia y Alemania remitieron al Consejo una recomendación conjunta instando al restablecimiento de todas las sanciones nucleares de la UE que habían sido suspendidas o finalizadas. Al no adoptarse una resolución del Consejo de Seguridad, el **17 de septiembre de 2025** se restableció el régimen sancionador, reintroduciéndose tanto sanciones de las Naciones Unidas (traspuestas automáticamente al Derecho de la UE) como medidas autónomas europeas.

Entre las medidas reintroducidas se encuentran:

- **Prohibición de viaje** para determinadas personas físicas.
- **Inmovilización de activos** de personas y entidades designadas.
- **Sanciones económicas y financieras**, que abarcan los sectores comerciales, financiero y del transporte.

AEPD sanciona con 10 millones de euros a Aena por su sistema de reconocimiento facial en aeropuertos

La AEPD ha impuesto a AENA una **multa superior a 10 millones de euros** por la implantación de un sistema de identificación biométrica mediante reconocimiento facial de pasajeros en ocho aeropuertos españoles, al considerar que se trataba de un tratamiento de datos de **alto riesgo** que se puso en funcionamiento **sin realizar previamente una Evaluación de Impacto en Protección de Datos (EIPD)** en los términos exigidos por el RGPD.

La resolución concluye que AENA llevó a cabo operaciones de tratamiento biométrico destinadas a identificar unívocamente a los pasajeros para permitir su acceso a determinadas zonas aeroportuarias **sin justificar adecuadamente la necesidad y proporcionalidad del tratamiento**. En particular, la AEPD subraya que no se acreditó —ni en el análisis previo ni en el posterior— que el uso de biometría fuese imprescindible para alcanzar la finalidad perseguida, especialmente cuando existían **medios alternativos menos intrusivos** capaces de proporcionar niveles comparables de eficacia y seguridad.

La Agencia admite que el tratamiento podría ser idóneo para verificar la identidad y facilitar el control de accesos, pero insiste en que el elemento determinante es la proporcionalidad, calificada expresamente como un requisito necesario y esencial.

Asimismo, la resolución destaca que el sistema utilizado era de tipo uno-a-varios 1:N, lo que desde la óptica de la protección de datos implica una **búsqueda activa dentro de un conjunto de identidades preexistentes**, incrementando significativamente el nivel de riesgo, en tanto puede afectar de forma más intensa a los derechos y libertades fundamentales de las personas físicas.

Como medida correctiva, la AEPD impone la **suspensión temporal de todo tratamiento de datos biométricos** asociado a dicho sistema de reconocimiento facial para el control de accesos de pasajeros, hasta que AENA lleve a cabo una EIPD conforme al RGPD.

Otros acuerdos y resoluciones sancionadoras en materia de *Compliance*

MOLINS Compliance

La CNMC (S/0011/23, Eólica del Alfoz) fija por primera vez el alcance y la duración de la prohibición de contratar directamente en su resolución sancionadora

La CNMC ha sancionado a Eólica del Alfoz por abuso de posición de dominio y, por primera vez, concreta en la propia resolución sancionadora el alcance y la duración de la prohibición de contratar con el sector público, aplicando los criterios de la Comunicación 1/2023, sobre **criterios para la determinación de la prohibición de contratar por falseamiento de la competencia**, por contravenciones de la Ley 15/2007, de Defensa de la Competencia.

La infracción se basa en la obstaculización del acceso a un punto de conexión eléctrica a un competidor, favoreciendo a una empresa del mismo grupo. Además de una multa de 958.593 euros, se impone una **prohibición de contratar**: (i) en todo el territorio nacional; (ii) frente a las entidades del sector público citadas en el artículo 3 de la LCSP, abarcando en concreto contratos de obras, suministros y servicios relativos a la consultoría, construcción, operación, explotación y mantenimiento de parques eólicos y sus equipos; y (iii) con una duración de **seis meses**, justificada por la ausencia de impacto directo en la contratación pública pese a tratarse de una infracción muy grave.

Este caso pone de manifiesto la relevancia estratégica de los programas de *Compliance* en competencia y de las medidas de protección como mecanismos para prevenir o mitigar este tipo de consecuencias.

Multa de la Oficina Antifrau de Catalunya (OAC) a una empresa por adoptar represalias contra una informante

La OAC ha impuesto por primera vez una sanción a una empresa por adoptar represalias contra una persona alertadora, en aplicación del **régimen sancionador vinculado a la Ley 2/2023**. La resolución afecta a Nora, S.A., empresa del sector de residuos vinculada al Consell Comarcal de la Selva y al Ayuntamiento de Blanes, y culmina con una multa de 600.000 euros, como consecuencia de la comisión de una infracción muy grave.

Los hechos se remontan a finales de 2022, cuando una trabajadora solicitó información interna al sospechar la existencia de posibles irregularidades relacionadas con contrataciones, cobro de pluses y control horario. Entre las personas potencialmente beneficiadas figuraba la responsable de recursos humanos, quien llegó a activar el protocolo interno de acoso contra la propia alertadora.

A comienzos de 2023, la trabajadora puso los hechos en conocimiento de la OAC y solicitó una excedencia voluntaria, pero, transcurrido aproximadamente un mes, la empresa le impuso una sanción disciplinaria de seis días de empleo y sueldo.

Dicha sanción fue anulada por un Juzgado de lo Social de Girona en diciembre de 2023, al apreciarse que constituía una **represalia directa vinculada a la denuncia de las irregularidades**, condenándose además a la empresa al abono de una indemnización de 7.500 euros. Esta decisión fue confirmada por el TSJ de Cataluña en julio de 2024, reforzando la existencia de una **conexión causal** clara entre la actuación disciplinaria y la condición de alertadora de la trabajadora.

A la vista de estas resoluciones judiciales, la OAC propuso inicialmente una sanción de 800.000 euros, que finalmente se ha reducido a **600.000 euros** tras el trámite de alegaciones, manteniendo la calificación de infracción muy grave.

Guías, resoluciones institucionales e informes de interés

MOLINS Compliance

- ❑ Actualización de la ISO 37001, sobre Sistemas de Gestión Antisoborno.
- ❑ Actualización de la UNE 19601, sobre Sistemas de Gestión de *Compliance* Penal.
- ❑ Nueva ISO 37003, de Gestión del Fraude.
- ❑ Nuevos catálogos de indicadores de riesgo de blanqueo de capitales y financiación del terrorismo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias.
- ❑ Plan Estratégico 2025-2030 de la Agencia Española de Protección de Datos. Innovación responsable y defensa de la dignidad en la era digital.
- ❑ Plan Estatal de Lucha contra la Corrupción de 9 de julio de 2025.
- ❑ Lista de terceros países de alto riesgos por blanqueo de capitales y financiación del terrorismo.
- ❑ Recursos para el uso de la IA.
- ❑ V Plan de Gobierno Abierto.

Guías, resoluciones institucionales e informes de interés

MOLINS Compliance

Actualización de la ISO 37001, sobre Sistemas de Gestión Antisoborno

La Organización Internacional de Normalización (en adelante, ISO) publicó el pasado 28 de febrero de 2025 la segunda edición de la Norma técnica ISO 37001, referente global en Sistemas de Gestión Antisoborno, que introduce novedades para fortalecer la alineación con otros estándares internacionales y mejorar la eficacia de los sistemas de cumplimiento.

Los cambios más destacados son:

- **Integración del cambio climático y la cultura de cumplimiento**: Se exige considerar el impacto del cambio climático dentro del análisis del riesgo de corrupción.
- **Refuerzo en la gestión de conflictos de interés**: Se reconoce al conflicto de interés como un riesgo clave en la prevención de la corrupción y, en la misma línea, se introduce la obligación de mantener un registro de declaraciones de conflictos de interés, con revisión anual.
- **Revisión de elementos clave del sistema**: Se actualizan aspectos estructurales del Sistema de Gestión de Antisoborno como el procedimiento de diligencia debida, auditoría interna, supervisión y revisión del sistema, así como *reporting* en materia de *Compliance*.
- **Alineación con otros estándares ISO**: Se adapta para mantener coherencia con otras regulaciones ISO, lo que facilita su integración en Sistemas de Gestión Globales.

Actualización de la UNE 19601, sobre Sistemas de Gestión de *Compliance* Penal

La Norma técnica UNE 19601, sobre Sistemas de Gestión de *Compliance* Penal, publicada inicialmente en 2017, fue actualizada el pasado 24 de abril de 2025 por la Asociación Española de Normalización. Los cambios más notorios han sido los siguientes:

- **Refuerzo del enfoque cultural del *Compliance***: Se adapta a la definición internacional de cultura organizativa como secuencia de valores, ética, creencias y conductas. La evaluación de la cultura pasa a basarse tanto en indicios objetivos como en la percepción de las partes interesadas.
- **Clarificación de los objetivos de *Compliance* penal**: Se distingue entre objetivos concretos y medibles, y las declaraciones generales que pueden hallarse en las políticas de *Compliance*.
- **Diligencia debida en inversiones**: Se aclara que los procesos de *due diligence* no se aplican a inversiones puramente financieras, delimitando su alcance operativo.
- **Formación vs. concienciación:** Se diferencia la formación técnica interna, dirigida a miembros de la organización, de las acciones de concienciación, aplicables también a socios de negocio, con atención especial a su autonomía.
- **Reubicación de la evaluación de riesgos:** El ejercicio de análisis de riesgos se traslada del capítulo de planificación al de contexto de la organización, en línea con las Normas técnicas ISO 19600:2014 y ISO 37301:2021.
- **Gestión de canales de denuncia:** Se alinean los requisitos con la Ley 2/2023 y la ISO 37002, incorporando medidas avanzadas de protección del informante frente a represalias y otras conductas perjudiciales, incluso cuando estas provengan de negligencias.
- **Gobernanza y función de *Compliance*:** Se especifican las responsabilidades centrales del área de *Compliance* frente a otras que debe impulsar pero que no controla directamente, siguiendo la distinción de la Norma técnica ISO 37301.
- **Estructura armonizada ISO**: Aunque su uso no es obligatorio, la norma española opta voluntariamente por seguir la estructura armonizada ISO, facilitando su integración con otros sistemas de gestión.

Guías, resoluciones institucionales e informes de interés

Nueva ISO 37003, de Gestión del Fraude

El 29 de mayo de 2025 se publicó la Norma técnica ISO 37003, la **primera norma internacional específica sobre Sistemas de Gestión del Control del Fraude.** Esta Norma no es certificable, ya que no impone requisitos obligatorios, sino que ofrece recomendaciones para aquellas organizaciones que quieren prevenir, detectar y responder frente a actos fraudulentos. Asimismo, la ISO 37003 está orientada al fraude que se produce dentro, desde o contra la organización.

Por ello, el contenido se puede aplicar a entidades de cualquier tamaño, sector o naturaleza jurídica, públicas o privadas, con o sin ánimo de lucro, lo que permite que sea una herramienta útil y flexible para distintos contextos organizativos.

Los **principales elementos** de la ISO 37003 son los siguientes:

- Analiza el **contexto organizativo** incluyendo factores internos y externos que influyen en la exposición al fraude.
- Asegura el compromiso del **liderazgo y la gobernanza** mediante la asignación de responsabilidades y coordinación entre *Compliance*, auditoría interna y seguridad de la información.
- **Planifica y evalúa los riesgos** de fraude, identificando amenazas reales y fomentando la colaboración entre áreas.
- Proporciona **recursos adecuados** y promueve la integridad, diferenciando entre formación técnica y acciones de concienciación.
- Establece **controles preventivos** sólidos, incluyendo políticas sobre conflictos de interés, *due diligence* y monitoreo.
- Implementa **mecanismos eficaces de detección** del fraude, mediante el empleo de herramientas tecnológicas y canales de denuncia.
- Define una **respuesta organizada ante incidentes de fraude** a través de evidencias, gestión del impacto reputacional y legal, así como acciones correctivas y sancionadoras.
- Evalúa el desempeño del sistema de forma periódica con **auditorías internas y revisiones** para detectar debilidades.
- Aplica el enfoque de **mejora continua**.

Nuevos catálogos de indicadores de riesgo de blanqueo de capitales y financiación del terrorismo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias

Durante el mes de mayo se publicaron por parte de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias los nuevos catálogos de indicadores de riesgo de nueve grupos de sujetos obligados, con el **objetivo de ayudar a mejorar los sistemas de prevención del blanqueo de capitales y la financiación del terrorismo** implantados por los sujetos obligados, y contribuir a la eficacia de estos.

En ellos se resume un **listado de indicadores de riesgos de blanqueo de capitales y financiación del terrorismo**. La presencia en operaciones concretas de estos indicadores no implica necesariamente la existencia de una actividad ilícita, pero sí que puede ayudar al sujeto obligado a identificar los casos a seleccionar para realizar el examen especial correspondiente.

Los diferentes indicadores que nos ofrecen estos catálogos se encuentran adaptados a la naturaleza de la actividad de cada sector considerado como sujeto obligado, y pretenden ayudar a los mismos a elaborar sus propios catálogos, con éstos como guía.

Estos catálogos **se diferencian** en los relativos a: (i) el proceso de cumplimiento de la diligencia debida; (ii) operaciones concretas; (iii) la titularidad real de los bienes; (iv) los empleados y agentes del sujeto obligado; y (v) la posible relación con actividades delictivas.

Guías, resoluciones institucionales e informes de interés

MOLINS Compliance

Plan Estratégico 2025-2030 de la Agencia Española de Protección de Datos. Innovación responsable y defensa de la dignidad en la era digital

El 3 de julio de 2025, la AEPD publicó el nuevo **Plan Estratégico 2025-2030, Innovación responsable y defensa de la dignidad en la era digital,** que marcará el rumbo de la AEPD durante los próximos años, teniendo presente las nuevas realidades tecnológicas, sociales y geopolíticas. El Plan Estratégico define ocho principios rectores, además de 45 objetivos que se estructuran alrededor de siete grandes ejes.

- **Eje 1 – Una agencia inteligente**: La AEPD quiere mejorar la eficiencia mediante el uso estratégico de indicadores e implementar sistemas avanzados de supervisión apoyados en la adopción de una política de "*AI first".*
- **Eje 2 – Innovación tecnológica con garantías**: La AEPD supervisará las tecnologías emergentes como la IA, los sistemas biométricos o neurotecnologías, especialmente cuando afecten a colectivos vulnerables.
- **Eje 3 – Promover y acompañar el cumplimiento normativo**: La AEPD busca elaborar recursos específicos, como *kits* técnicos, y actualizar sus guías adaptadas a las necesidades de distintos sectores.
- **Eje 4 – Impulsar alianzas y colaboración con entidades profesionales**: La AEPD quiere fortalecer la cooperación con los profesionales de la privacidad y desarrollará una estrategia de intervención transversal orientada a colectivos vulnerables en el entorno digital.
- **Eje 5 – Liderazgo e influencia estratégica internacional y nacional**: La AEPD reforzará su presencia en el ámbito internacional incrementando su participación en los principales foros nacionales e internacionales, especialmente, en el Comité Europeo de Protección de Datos (en adelante, CEPD).
- **Eje 6 – Una administración eficaz y en mejora continua**: La AEPD, como Autoridad de Vigilancia del Mercado de IA, quiere incrementar sus recursos y optimizar la organización a través de un plan integral de desarrollo y retención del talento.
- **Eje 7 – Apertura, cercanía y cultura de protección de datos**: La AEPD quiere mejorar su web implementando herramientas y canales de atención para mejorar la comunicación y escucha activa con sectores profesionales.

Plan Estatal de Lucha contra la Corrupción de 9 de julio de 2025

El 9 de julio, el Gobierno presentó su Plan Estatal de Lucha contra la Corrupción, con el propósito de consolidar un enfoque integral y moderno frente a este fenómeno. Se alinea con las recomendaciones de organismos internacionales como la Organización para la Cooperación y el Desarrollo Económico y la Comisión Europea. El documento se estructura en torno a **cinco pilares** de actuación:

El **primer pilar** (prevención de riesgos y refuerzo de controles públicos) propone como medida estructural clave la creación de una **Agencia Independiente de Integridad Pública**, que asumiría competencias hasta ahora dispersas en materia de transparencia, control de la contratación, supervisión de fondos y protección del denunciante. Por otra parte, en el ámbito contractual, se proyecta una transformación digital del actual portal estatal mediante el **uso de herramientas de IA** y *big data*, junto con la **implementación sistemática de mapas de riesgo** de integridad en la gestión de fondos públicos.

El **segundo** contempla una **ampliación significativa de las garantías ofrecidas a los informantes**. A pesar de los avances establecidos por la Ley 2/2023, se considera necesario reforzar la protección de quienes alertan sobre irregularidades, incluyendo a quienes lo hagan directamente ante el Ministerio Fiscal, cuerpos policiales o instancias judiciales. Asimismo, se prevé **extender la protección durante un periodo de cinco años** tras el cese de los **gestores de canales** de denuncia, establecer el derecho a indemnizaciones proporcionales al perjuicio sufrido y exigir una mayor independencia y efectividad en el funcionamiento de los canales internos.

El **tercero** aborda la investigación y sanción efectiva de las conductas corruptas. Se apuesta por el **fortalecimiento del papel del Ministerio Fiscal** en la fase de **instrucción**, así como por una reforma del Código Penal y la especialización judicial en la materia. Desde una perspectiva de *Compliance*, se destacan tres novedades: (i) la exigencia legal de sistemas de *Compliance* para operadores de gran tamaño; (ii) la imposición de sanciones económicas proporcionales al beneficio ilícito; y (iii) la inhabilitación para contratar con el sector público en caso de condenas por corrupción.

El **cuarto** pilar refuerza la recuperación de activos ilícitos, dotando de mayores capacidades a la Oficina de Recuperación y Gestión de Activos y planteando la posible incorporación del decomiso administrativo preventivo, siguiendo modelos internacionales.

Finalmente, el Plan impulsa la promoción de una cultura de integridad, con **formación obligatoria** para personal público, y campañas institucionales que alienten el uso responsable de los canales de denuncia.

Guías, resoluciones institucionales e informes de interés

MOLINS Compliance

Lista de terceros países de alto riesgos por blanqueo de capitales y financiación del terrorismo

El Grupo de Acción Financiera Internacional (**GAFI) celebró su plenario el 24 de octubre de 2025 en París**, adoptando decisiones relevantes en materia de **evaluación, recuperación de activos y riesgos emergentes**. En el apartado de listas, anunció la **salida de la "lista gris"** de **Burkina Faso, Mozambique, Nigeria y Sudáfrica**, tras completar sus planes de acción y acreditar mejoras sustanciales en la prevención y persecución del **blanqueo de capitales y la financiación del terrorismo**, mientras que la **lista negra** se mantiene **sin cambios**. Aunque se reconoce cierta reactivación por parte de Irán, el GAFI entiende que aún no concurren condiciones suficientes para su exclusión.

En este contexto, la **Unión Europea** ha actualizado la **lista de jurisdicciones de alto riesgo en materia de blanqueo de capitales y financiación del terrorismo**, recordando que las entidades sujetas al marco de prevención de blanqueo de capitales de la UE deben aplicar **medidas de diligencia debida reforzada** en las operaciones en las que intervengan estos países, como instrumento clave para proteger la integridad del sistema financiero de la UE. En esta actualización, se **incorporan Argelia, Angola, Costa de Marfil, Kenia, Laos, Líbano, Mónaco, Namibia, Nepal y Venezuela**, **Bolivia**, **Rusia** y las **Islas Vírgenes Británicas** y se **eliminan Barbados, Gibraltar, Jamaica, Panamá, Filipinas, Senegal, Uganda, Emiratos Árabes Unidos, Burkina Faso, Mozambique, Nigeria, Sudáfrica, Mali y Tanzania**.

La Comisión Europea subraya que la lista se alinea con el trabajo del **GAFI** y su metodología de supervisión reforzada. No obstante, todavía no ha habido una publicación oficial de dicha lista.

Recursos para el uso de la IA.

La **Agencia Española de Supervisión de Inteligencia Artificial** (en adelante, AESIA) es el organismo público encargado de **garantizar el uso ético y seguro de la IA en España**. Este organismo publicó el 10 de diciembre de 2025 diferentes guías desarrolladas en el marco del **piloto español del *sandbox* regulatorio de IA** (el término *sandbox* se refiere un espacio de pruebas supervisado, donde se pueden experimentar nuevas soluciones de IA de forma controlada y segura, antes de aplicarlas a gran escala.)

La finalidad de estas guías es **ofrecer un marco de apoyo práctico** para **facilitar la implantación** y el **cumplimiento de las obligaciones** previstas en la normativa europea de IA.

Cabe destacar que, aunque estas guías **no son documentos vinculantes ni sustituyen o desarrollan el contenido del Reglamento**, sí aportan orientaciones y recomendaciones coherentes con los requisitos regulatorios, especialmente útiles mientras no se aprueben las normas armonizadas que deberán aplicarse de forma común en todos los Estados miembros.

Estas guías consisten en **documentos dinámicos**, sometidos a un proceso continuo de revisión y mejora, que irán evolucionando en función de la evolución de los estándares técnicos y de las directrices que vaya publicando la Comisión Europea.

Se han desarrollado un **total de 17 documentos**, organizados en los siguientes bloques:

- **Guías introductorias**: guías 1 y 2. Ofrecen una comprensión general del Reglamento de IA desde un punto de vista teórico y práctico.
- **Guías técnicas**: guías de la 3 a la 15. Cada una de estas trece (13) guías ofrece orientaciones operativas para traducir los requisitos del Reglamento de IA en medidas **concretas**, facilitando el diseño, implementación y documentación de sistemas de IA.
- **Manual de uso de las *checklist***: guía 16. Explica, de forma práctica, **cómo utilizar las listas de verificación para autoevaluar el cumplimiento** de un sistema de IA con los requisitos del Reglamento de IA y **planificar las medidas necesarias** para corregir posibles carencias.
- **Compendio de *checklist* y ejemplos en archivo zip**. Reúne, en un formato descargable, las **listas de verificación y modelos prácticos** para facilitar su aplicación directa, apoyar la documentación interna y estandarizar la evaluación del cumplimiento en proyectos de IA.

Guías, resoluciones institucionales e informes de interés

MOLINS
Compliance

V Plan de Gobierno Abierto

El **V Plan de Gobierno Abierto 2025–2029**, vigente desde el **6 de octubre de 2025**, consolida un giro relevante para la agenda de **integridad y cumplimiento en el sector público**, al pasar de enfoques principalmente declarativos a un marco con **medidas estructuradas, medibles y con vocación de despliegue efectivo**. El Plan se articula en diez compromisos, destacando en materia de *Compliance* el **Compromiso 3: Integridad y rendición de cuentas**, que incorpora **24 iniciativas** orientadas a reforzar la confianza ciudadana mediante **mapas de integridad, prevención de conflictos de interés, regulación de grupos de interés (*lobbies*), rendición de cuentas y prevención de la corrupción**, incluyendo iniciativas derivadas del **Plan Estatal de Lucha contra la Corrupción**.

En este marco, el Plan impulsa de forma expresa el **Sistema de Integridad de la Administración General del Estado (SIAGE)** —aprobado por Acuerdo del Consejo de Ministros de 28 de enero de 2025—, que pasa a configurarse como **referencia metodológica y operativa** para extender sistemas de integridad al conjunto del sector público. Entre las líneas de actuación más relevantes destacan: (i) la extensión de **mapas y matrices de riesgos de integridad** a toda la Administración, alineados con el **OECD *Public Integrity Framework*** y con especial foco en **contratación pública**, incorporando **mecanismos de alerta temprana ("banderas rojas")**; (ii) el **diagnóstico de madurez del SIAGE** para identificar fortalezas y áreas de mejora; (iii) la promoción de **programas de cumplimiento normativo en la AGE** como herramienta preventiva esencial, con la pretensión explícita de que el modelo sea **replicable** y actúe como **referencia institucional**; y (iv) la incorporación de instrumentos de medición cultural, como **encuestas de clima ético**, para evaluar el impacto real del sistema en la organización.

Asimismo, el Compromiso 3 incorpora iniciativas con fuerte potencial transformador en materia de integridad: el desarrollo de una **Estrategia Nacional Antifraude**; la tramitación del **Anteproyecto de Ley Orgánica de Integridad Pública** (con medidas de refuerzo en contratación pública y endurecimiento penal en corrupción); la posible creación de una **Agencia Independiente de Integridad Pública** con funciones de supervisión, evaluación de riesgos e investigación; el diseño de un **sistema integral de protección de denunciantes**; y la transformación de la **Plataforma de Contratación del Sector Público** mediante ***Big Data* e inteligencia artificial** para detectar patrones irregulares y evolucionar hacia una supervisión estructural y automatizada. Todo ello se acompaña de un eje específico de **cultura de integridad**, con acciones de difusión y formación obligatoria para empleados públicos y altos cargos.

La **idea clave desde el prisma del *Compliance*** debe ser que el V Plan refuerza un estándar emergente en el sector público: la integridad se gestiona como un **sistema de cumplimiento**, basado en **riesgos**, con controles verificables, métricas de madurez, herramientas preventivas y mecanismos de rendición de cuentas.

Publicaciones del Departamento del *Compliance* (enero-diciembre 2025)

MOLINS Compliance

- Un paso más hacia la protección de los denunciantes: la creación de la Autoridad Independiente de Protección al Informante de la Comunidad de Madrid.
- ¿Cómo SEPBLAC está transformando la lucha contra el blanqueo de capitales y la financiación del terrorismo?
- Nueva edición de la ISO 37001: novedades clave y periodo de transición.
- Molins *Compliance*: estrategia, prevención y confianza.
- La nueva versión de la UNE 19601: una respuesta eficaz a los desafíos de buen gobierno de las organizaciones.
- La corrupción bajo lupa: claves del nuevo Plan Estatal de lucha contra la corrupción.
- *ComplianceKeys*#25: Origen del *Compliance* en España.
- *ComplianceKeys*#26: *Compliance*, ética empresarial y cultura organizacional.
- *ComplianceKeys*#27. ¿Cómo afecta el *Compliance* a la reputación de la empresa?
- Delito cometido por la persona jurídica: nuevo cambio de criterio del Tribunal Supremo (STS 768/2025 de 25 de septiembre y 836/2025 de 14 de octubre) sobre la prueba de la ineficacia de los programas de cumplimiento.
- *ComplianceKeys*#28. El *Compliance* en el sector público: integridad y buen gobierno como pilares de la gestión pública.
- *ComplianceKeys*#29. *Compliance* y Sostenibilidad.
- *ComplianceKeys*#30. *Compliance* y blanqueo de capitales.

MOLINS

Defensa Penal **Compliance**

Barcelona Diagonal 399, Planta 1 08008 | Tel. 93 415 22 44

Madrid José Abascal, 56 Planta 6 28003 | Tel. 91 310 30 08

www.molins.eu | compliance@molins.eu