

MOLINS

Defensa Penal **Compliance**

Compliance Newsletter

Julio de 2025

I. Introducción	3
II. Novedades legislativas	4
III. Tribunales	9
IV. Otros acuerdos y resoluciones sancionadoras en materia de <i>Compliance</i>	13
V. Guías, resoluciones institucionales e informes de interés	16
VI. Publicaciones del Departamento de <i>Compliance</i> (enero-julio 2025)	20



En un entorno empresarial cada vez más competitivo, dinámico y severo, **las exigencias legales regulatorias son cada vez más elevadas**. En este sentido, el **Compliance se convierte** tanto en un **aliado de negocio** imprescindible como en un **pilar estratégico** para garantizar la integridad y adoptar una cultura ética que garantice el respeto a la legalidad.

En el transcurso del **primer semestre de 2025**, el ámbito del *Compliance* ha experimentado **desarrollos normativos y estratégicos** de notable trascendencia. Destacan el **Anteproyecto de Ley que modifica la Ley Orgánica del Código Penal** para adecuarla a la Directiva (UE) 2024/1226 y la **Sentencia del Tribunal Supremo 372/2025**, de 11 de abril de 2025, que recuerda que para atribuir responsabilidad penal a la persona jurídica se debe acreditar un defecto estructural en los Sistemas de Gestión de *Compliance*. Además, se resalta la **condena de la AEPD** a pagar 120.000 euros a una empresa por desvelar la identidad de unos denunciantes, así como **las actualizaciones de las Normas técnicas ISO 37001 sobre Sistemas de Gestión Antisoborno** (en adelante también referida como **ISO 37001**) y **UNE 19601 sobre Sistemas de Gestión de Compliance Penal** (en adelante también referida como **UNE 19601**).

En este escenario, el [Departamento de Compliance](#) de **Molins Defensa Penal** elabora el presente *Newsletter*, con los avances más significativos y novedosos en materia de *Compliance* de este primer semestre de 2025. Su contenido es el siguiente:

- Como punto de partida, se analizarán las **principales novedades legislativas** que afectan, en mayor o menor medida, al diseño, implementación o revisión de los Sistemas de *Compliance*.
- Seguidamente se presentarán **resoluciones judiciales de interés**.
- Se analizarán también otros **acuerdos y resoluciones sancionadoras** en materia de *Compliance*.
- Se contará con una síntesis de las **principales guías, resoluciones institucionales e informes** de especial interés.
- En último lugar, se concluirá el presente *Newsletter* con un **catálogo de publicaciones** del Departamento de *Compliance* relativas al primer semestre de 2025.



- ❑ [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.](#)
- ❑ [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 modifican los Estatutos de la Fundación Pluralismo y Convivencia, F.S.P., aprobados por el Real Decreto 45/2021, de 26 de enero, y 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.](#)

- ❑ [Anteproyecto de Ley para el buen uso y la gobernanza de la Inteligencia Artificial, de adaptación al Reglamento \(UE\) 2024/1689 de Inteligencia Artificial.](#)
- ❑ [Anteproyecto de Ley Orgánica de modificación de 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.](#)
- ❑ [Proyecto de Ley 121/46 de 4 de febrero de 2025 de transparencia e integridad de las actividades de los grupos de interés.](#)



Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad

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, antes del 17 de abril de 2025, 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, el **próximo 2 de agosto de 2025** ya tendrán efecto las disposiciones relativas a sanciones, confidencialidad y gobernanza.

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 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**.

Anteproyecto de Ley Orgánica de modificación de 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 normas mínimas para tipificar como delitos penales las infracciones graves a las medidas restrictivas impuestas por la UE.

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 Unión Europea.

- **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.

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 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 año** la entrada en vigor de la **Directiva sobre Diligencia Debida de las Empresas (en adelante, CSDDD)**, por lo que los nuevos plazos de aplicación serán:

- **26 de julio de 2028**, para:
 - Empresas de la UE con más de 3.000 empleados y un volumen de negocio superior a 900 millones de euros.
 - Empresas matrices de grupos que alcancen los umbrales anteriores.
 - Empresas de fuera de la UE con un volumen de negocio superior a 900 millones de euros en territorio comunitario.
- **26 de julio de 2029**, para:
 - Empresas con más de 1.000 empleados y un volumen de negocio superior a 450 millones de euros.
 - Empresas matrices de grupos que cumplan los criterios anteriores.
 - Empresas con franquicias o licencias en la UE cuyos cánones superen los 22,5 millones de euros, siempre que el grupo genere un volumen de negocio superior a 80 millones de euros.

Por último, se establece que los **Estados miembros** deberán **transponer esta Directiva antes del 31 de diciembre de 2025**.

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.

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

A fecha 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 su sector público institucional, las relaciones entre los denominados grupos de interés** (también denominados *lobbies*) y los responsables públicos, 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 influido en cada norma.
- **Código de conducta vinculante** para grupos de interés.

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

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



- ❑ [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 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.](#)
- ❑ [Sentencia de la Audiencia Nacional, Sala de lo Penal, 9/2025 de 2 de julio de 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 heteroresponsabilidad en el momento de atribución de la responsabilidad penal**, ya que **la 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 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.**

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, FEAGA) 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 Dirección General de Industria.

El conflicto recae en que la compañía no informó de la recepción de esta bonificación al FEAGA, 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 FEAGA).

Asimismo, **la compañía solicitó los 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 autenticada 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.**



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

La 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 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 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 ant blanqueo 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.

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 a 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.

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.



- 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 Estatal de Lucha contra la Corrupción de 9 de julio de 2025.](#)
- [Plan Estratégico 2025-2030 de la Agencia Española de Protección de Datos. Innovación responsable y defensa de la dignidad en la era digital.](#)



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.



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.



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 asumirá 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.

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.

- ❑ [La nueva versión de la UNE 19601: una respuesta eficaz a los desafíos de buen gobierno de las organizaciones](#)
- ❑ [Molins *Compliance*: estrategia, prevención y confianza](#)
- ❑ [Denuncias internas: ¿protección del informante o derecho de defensa del investigado?](#)
- ❑ [¿Se puede requerir a la persona jurídica investigada para que identifique a la persona física concreta que tuvo intervención en los hechos presuntamente delictivos?](#)
- ❑ [Nueva edición de la ISO 37001: novedades clave y periodo de transición](#)
- ❑ [Anuario 2024. Recopilación de la normativa y jurisprudencia más relevante del año en materia de investigaciones internas](#)





- ❑ ¿Cómo SEPBLAC está transformando la lucha contra el blanqueo de capitales y la financiación del terrorismo?
- ❑ Un paso más hacia la protección de los denunciantes: la creación de la Autoridad Independiente de Protección al Informante de la Comunidad de Madrid
- ❑ ¿Es posible el tratamiento de los datos personales contenidos en las comunicaciones recibidas a través del Sistema de Información Interno (SII) para otras finalidades distintas de la prevista por la Ley 2/2023?
- ❑ Finalizado el plazo de adaptación del uso de cookies
- ❑ El nuevo Plan Estatal de lucha contra la corrupción

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