MOLINS

Defensa Penal **Compliance**

Compliance Newsletter

Julio de 2024

Índice

MOLINS
Compliance

I. Introducción **3**

II. Novedades legislativas **4**

III. Tribunales **10**

IV. Otros acuerdos y resoluciones sancionadoras en materia de *Compliance* **13**

V. Guías, resoluciones institucionales e informes de interés **16**

VI. Publicaciones del Departamento de *Compliance* **20**

MOLINS compliance

Introducción

El cumplimiento normativo, o *Compliance*, es esencial para asegurar la integridad y sostenibilidad de las organizaciones en un entorno regulatorio tan complejo y cambiante como el actual. Mantenerse informado es más que una obligación: es una **necesidad estratégica** para asegurar el adecuado y continuo progreso de las empresas.

A lo largo del primer semestre del año 2024, hemos sido testigos de importantes avances en materia de *Compliance*. Entre ellos, destacan las novedades en materia de sostenibilidad y responsabilidad corporativa, así como la creciente regulación en materia de protección de datos y privacidad. A su vez, se han introducido cambios legislativos significativos, se han dictado sentencias relevantes por parte del Tribunal Supremo y otras instancias judiciales, y se han publicado múltiples informes y guías de interés por parte de diferentes autoridades en la materia.

El Departamento de *Compliance* de **Molins Defensa Penal** ha elaborado el presente *newsletter* a modo de recopilación de los hitos más significativos en materia de *Compliance* de este semestre. Su contenido es el siguiente:

- Se llevará a cabo un análisis de las **principales novedades legislativas** con incidencia en la configuración de los Sistemas de *Compliance*.
- A continuación, se expondrán diferentes **resoluciones del Tribunal Supremo y del Tribunal Constitucional de interés** en materia de *Compliance* dictadas recientemente.
- Asimismo, se examinarán otros **acuerdos y resoluciones sancionadoras** importantes en materia de *Compliance*.
- Se continuará con una breve exposición de diferentes **guías, resoluciones institucionales e informes** de interés en materia de *Compliance*.
- El presente *newsletter* concluirá con el **catálogo de publicaciones** del Departamento de *Compliance* referentes al primer semestre de 2024.

Novedades legislativas

MOLINS Compliance

- Directiva sobre Diligencia Debida para la Sostenibilidad Corporativa (CSDDD) nº2022/2464.
- Directiva (UE) 2022/2557 del parlamento europeo y del consejo relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo (CER).
- Nueva "*Foreign Extortion Prevention Act*" (Ley de Prevención de Conductas de Extorsión en el Extranjero; FEPA).
- 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 (NIS 2).
- Proyecto de Real Decreto por el que se aprueba el Estatuto de la Autoridad Independiente de Protección del Informante.
- Nuevo paquete de medidas de PBC-FT de la Unión Europea, 30 de mayo de 2024:
  - Reglamento (UE) 2024/1624, de 31 de mayo de 2024, relativo a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo.
  - Reglamento (UE) 2024/1620, de 31 de mayo de 2024, por el que se crea una Autoridad Europea de Lucha contra el Blanqueo de Capitales y Financiación del Terrorismo (AMLA por sus siglas en inglés).
  - Directiva (UE) 2024/1640 del Parlamento Europeo y del Consejo, de 31 de mayo de 2024, relativa a los mecanismos que deben establecer los Estados miembros a efectos de la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, por la que se modifica la Directiva y (UE) 2019/1937 y se modifica y deroga la Directiva (UE) 2015/849.
  - Directiva (UE) 2024/1654, de 31 de mayo de 2024, por la que se modifica la Directiva (UE) 2019/1153 en lo que respecta al acceso de las autoridades competentes a los registros centralizados de cuentas bancarias a través del sistema de interconexión y a las medidas técnicas destinadas a facilitar el uso de los registros de operaciones.
- Reglamento del Parlamento Europeo y del Consejo de Inteligencia Artificial (AIA, por sus siglas en inglés - *Artificial Intelligence Act*).

MOLINS compliance

MOLINS Compliance

Directiva (UE) 2022/2464 sobre Diligencia Debida para la Sostenibilidad Corporativa (CSDDD)

La **CSDDD** establece **obligaciones de reporte y medidas de diligencia debida** en el ámbito de la **sostenibilidad** para las organizaciones, abordando tres dimensiones específicas: **ambiental, social y buen gobierno**, conocidas como **ESG**.

Dicha Directiva obliga a las organizaciones a hacer frente a los impactos adversos sobre los derechos humanos y el medio ambiente derivados de **sus propias operaciones, las de sus filiales y las de sus socios comerciales**. Estas obligaciones pretenden cumplir con el **pacto Verde Europeo** y se fundamentan en los ***European Sustainability Reporting Standards*.**

Por ende, las organizaciones deberán implementar **sistemas diligentes de gestión de riesgos en materia de derechos humanos y medioambiente** y deberán informar de los mismos en sus informes de sostenibilidad.

El **control de cumplimiento de las disposiciones de la CSDDD** se llevará a cabo por el órgano especializado correspondiente de la administración pública que tendrá las siguientes facultades:

- Poder de **investigación**.
- Adopción de **medidas cautelares**.
- Imposición de **sanciones**.

¿Con qué estándares de autorregulación pueden escoger cumplir las organizaciones a los efectos de facilitar el cumplimiento de estas obligaciones? Entre otros, con los siguientes:

- **Dimensión ambiental**: la UNE-EN ISO 14064-1 de gases de efecto invernadero (inventario) y la ISO 59020 de medición y evaluación de la circularidad, entre otras.
- **Dimensión social**: normativa orientada a asegurar un entorno laboral estable, como la norma UNE 19604 de sistemas de gestión de *Compliance* socio laboral.
- **Buen gobierno**: en el ámbito penal, la norma UNE 19601 de sistemas de gestión de *Compliance* penal; en el tributario, la UNE 19602 de sistemas de gestión de *Compliance* tributario; en materia de prevención de la corrupción, la ISO 37001 de sistemas de gestión antisoborno, entre otras.

Esta Directiva entrará en vigor el **26 de julio de 2024.**

Directiva (UE) 2022/2557 del parlamento europeo y del consejo relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo (CER)

La **Directiva CER** tiene el objetivo de **establecer medidas específicas armonizadas que garanticen la prestación, sin obstrucciones, de servicios esenciales para el mantenimiento de las funciones sociales o actividades económicas vitales**. Ello, a través de una **mejora de la ciber resiliencia de entidades críticas** y la mejora de la **cooperación transfronteriza**.

La **ciber resiliencia** es la capacidad de una entidad para la protección, resistencia, mitigación, absorción, adaptación y recuperación en caso de un incidente (va más allá de la ciberseguridad).

La Directiva CER establece, entre otras, **obligaciones en las siguientes materias**:

- Deber de **evaluación de riesgos**.
- Medidas de **resiliencia-ciberseguridad, respuesta, recuperación, etc.**
- **Comprobación de antecedentes.**
- **Notificación de incidentes.**

La Directiva CER resulta de aplicación a las **entidades críticas, que deberán ser objeto de identificación por los Estados miembro, en atención a los siguientes criterios:**

- Entidades que **presten uno o más servicios esenciales**;
- Entidades que operen en el **territorio de dicho Estado miembro y su infraestructura crítica está situada en él**, y
- Entidades que, en caso de **producirse un incidente**, causarían **efectos perturbadores significativos en la prestación de uno o más servicios esenciales, o en la prestación de otros servicios esenciales que dependan de dicho servicio**.

El plazo de transposición de esta Directiva finalizará el **17 de octubre de 2024**.

MOLINS Compliance

Novedades legislativas

MOLINS
Compliance

La nueva "*Foreign Extortion Prevention Act*" (Ley de Prevención de Conductas de Extorsión en el Extranjero; FEPA)

La **FEPA** complementa la Ley de Prácticas Corruptas en el Extranjero y establece, por primera vez, la **responsabilidad penal de los funcionarios extranjeros** que soliciten o acepten sobornos de personas o entidades a las que sea de aplicación la Ley de Prácticas Corruptas en el Extranjero (se sanciona el lado de la demanda).

Es destacable que los efectos de la presente normativa **no se limitan al territorio de los Estados Unidos**, sino que se extiende a la **solicitud y aceptación de sobornos por parte de funcionarios extranjeros cuando tuvieran un nexo con los Estados Unidos**.

Los funcionarios extranjeros que violen la FEPA podrían enfrentar una sanción de hasta 250.000 dólares, tres veces el valor del soborno, prisión de hasta 15 años, o incluso ambas.

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 NIS 2)

La **Directiva NIS 2** establece medidas que tienen por objeto **alcanzar un elevado nivel común de ciberseguridad** en toda la Unión con el objetivo de **mejorar el funcionamiento del mercado interior**.

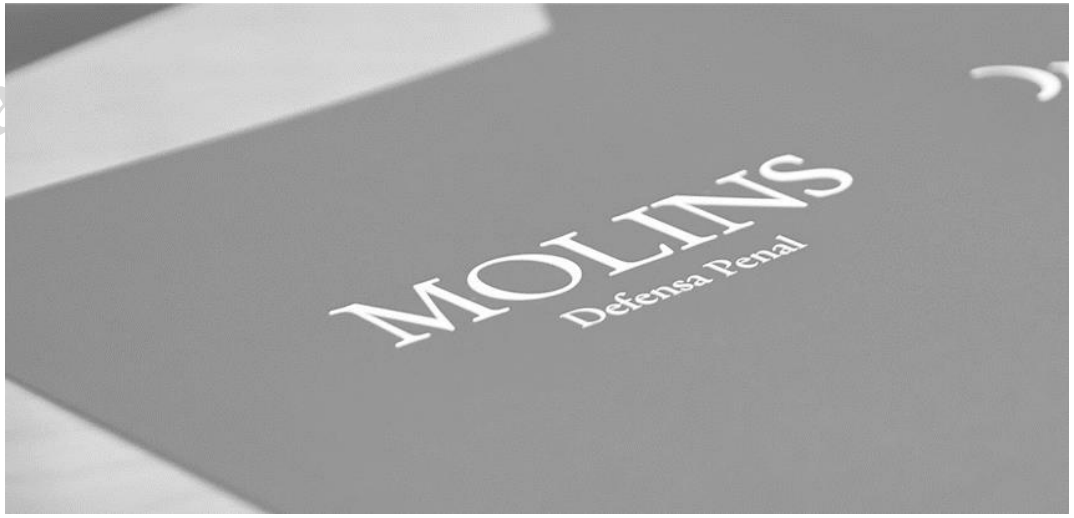
Para ello, la Directiva establece:

- La obligación estatal de adoptar una **estrategia nacional de ciberseguridad**.
- **Medidas para la gestión de riesgos de ciberseguridad y obligaciones de notificación para entidades obligadas**.
  - Se regulan en el **artículo 21** e incluyen, entre otros, la gestión de **incidentes**; **políticas de ciber higiene** y **formación de ciberseguridad**; el uso de **sistemas de autenticación multifactorial o de autenticación continua**; y la **seguridad en la cadena de suministros**, incluidos los aspectos relacionados con la **seguridad** en las relaciones entre entidades y sus proveedores.

A grandes rasgos, la Directiva NIS 2 aplica a **un total de 18 sectores** (Anexo I y II), divididos en:

- **Sectores de alta criticidad:** energía; transporte; banca; infraestructuras de los mercados financieros; sector sanitario; agua potable; aguas residuales; infraestructura digital; gestión de servicios TIC (B2B); entidades de la Administración Pública (con exclusión del poder judicial, los parlamentos y los bancos centrales); y espacio.
- **Otros sectores críticos:** servicios postales; gestión de residuos; fabricación, producción y distribución de sustancias y mezclas químicas; producción, transformación y distribución de alimentos; fabricación; proveedores de servicios digitales; e investigación.

El plazo de transposición de esta Directiva finalizará el **17 de octubre de 2024**.



MOLINS Compliance

Proyecto de Real Decreto por el que se aprueba el Estatuto de la Autoridad Independiente de Protección del Informante

La **Autoridad Independiente de Protección del Informante** (A.A.I.) es un ente estatal con **autonomía e independencia funcional** cuyo objetivo es cumplir con el **mandato de la Ley 2/2023.**

Las **funciones** de la A.A.I. son las siguientes:

- **Tramitación de informaciones y comunicaciones** que se lleven a cabo a través del canal externo de la propia A.A.I.
- Adopción de **medidas de protección y apoyo** a los informantes.
- **Inicio, instrucción y resolución de procedimientos sancionadores**.
- Elaboración de **circulares (de carácter vinculante) y recomendaciones**.
- Establecer **relaciones de colaboración con otras autoridades semejantes** (*v.g.*: Oficina Antifraude de Cataluña).
- Elaborar una **memoria anual y de información estadística agregada**.
- Contribuir en la **creación y fortalecimiento de una cultura de la información**.

Una de sus **funciones más relevantes** es la de **sancionar los incumplimientos en materia de protección del informante**, de la **Ley 2/2023**. A pesar de esto, la A.A.I. no puede ejercer funciones propias de jueces o fiscales (no puede investigar hechos de carácter penal) y debe **suspender sus actuaciones** cuando dichos órganos inicien una investigación.

En el Proyecto de Real Decreto se prevé la **habilitación de un canal externo de denuncias de acceso universal** y al que puede dirigirse cualquier persona interesada, cuando su comunicación no haya sido debidamente gestionada o no existe el canal interno.

Nuevo paquete de medidas de PBC-FT de la Unión Europea, 30 de mayo de 2024

El nuevo paquete de medidas de la Unión Europea para la prevención del Blanqueo de Capitales y la financiación del terrorismo consta de las siguientes normas:

1. **Reglamento (UE) 2024/1624, de 31 de mayo de 2024, relativo a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo:**

- Incluye **requisitos para las entidades obligadas**, principalmente las entidades financieras y de crédito y las empresas y profesiones no financieras designadas (por ejemplo, abogados y contables).
- **Amplía el listado de entidades obligadas** a:
  - Los **comerciantes de coches de lujo, aviones, yates y bienes culturales** (como obras de arte).
  - Los **proveedores de servicios de criptoactivos**.
  - Las **plataformas de *crowdfunding***.
  - Los **intermediarios de créditos hipotecarios y créditos al consumo** que no tengan consideración de entidades financieras.
  - Los **operadores de migración por inversión** que trabajen en representación de nacionales de terceros países para obtener permiso de residencia en la UE.
  - Los **clubes y agentes de fútbol profesional**. Sin embargo, dado que el sector y su riesgo están sujetos a grandes variaciones, los Estados miembros dispondrán de flexibilidad para retirarlos de la lista si representan un riesgo bajo.
- Establece la obligación de las entidades obligadas de **disponer de un "director de cumplimiento normativo"** y de un **"responsable del cumplimiento normativo"** en materia de prevención de blanqueo de capitales.
- Exige a las **entidades obligadas** que apliquen **medidas reforzadas de diligencia debida a las operaciones ocasionales** y a las **relaciones comerciales** en las que participen terceros países de alto riesgo.

MOLINS Compliance

2. **Reglamento (UE) 2024/1620, de 31 de mayo de 2024, por el que se crea una Autoridad Europea de Lucha contra el Blanqueo de Capitales y Financiación del Terrorismo (AMLA por sus siglas en inglés):**

- Se crea una nueva Autoridad de Lucha contra el Blanqueo de Capitales (ALBC) con el fin de **mejorar la supervisión** de la lucha contra el blanqueo de capitales y la financiación del terrorismo en la UE y apoyar la cooperación entre las UIF. Tendrá las siguientes funciones:
  - **Función de coordinación y armonización**: emitirá guías técnicas para facilitar la cooperación y el intercambio de información entre las unidades de inteligencia financiera de los Estados miembros; mejorará los sistemas electrónicos utilizados por las unidades de inteligencia financiera y Europol para el intercambio y verificación de información.
  - **Función de supervisión**: supervisará directamente a entidades obligadas, especialmente aquellas con alto riesgo de blanqueo de capitales; actuará a petición de las unidades de inteligencia financiera de los Estados miembros o de oficio si hay un interés de la Unión en supervisar a determinadas entidades.
- La ALBC tendrá su **sede en Fráncfort** y empezará a funcionar a **mediados de 2025**.

Este Reglamento se aplicará a partir del **1 de julio de 2025**, salvo algunos de sus preceptos que ya son de aplicación desde el **26 de junio de 2024** o lo serán a partir del **31 de diciembre de 2025**.

3. **Directiva (UE) 2024/1640 del Parlamento Europeo y del Consejo, de 31 de mayo de 2024, relativa a los mecanismos que deben establecer los Estados miembros a efectos de la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, por la que se modifica la Directiva y (UE) 2019/1937 y se modifica y deroga la Directiva (UE) 2015/849:**

- Establece **medidas específicas** para **sectores expuestos al blanqueo de capitales a nivel nacional**. Estas medidas incluyen requisitos para el registro, identificación y control de la alta dirección y titulares reales de las entidades obligadas.
- **Amplía la información** que debe incluirse en estos registros centrales, abarcando **cuestiones de seguridad y cuentas de criptoactivos**.
- Los **mecanismos centralizados automatizados estarán interconectados por medio del sistema de interconexión de registros de cuentas bancarias** (BARIS, por sus siglas en inglés), que desarrollará y gestionará la Comisión antes del 10 de julio de 2029. La Autoridad contra el Blanqueo de Capitales (AMLA), las unidades de inteligencia financiera estatales y las autoridades supervisoras nacionales en materia de prevención de blanqueo de capitales y financiación del terrorismo (AML/CFT) tendrán acceso directo a BARIS.

El plazo de transposición de esta Directiva finalizará el **10 de julio de 2027**.

4. **Directiva (UE) 2024/1654, de 31 de mayo de 2024, por la que se modifica la Directiva (UE) 2019/1153 en lo que respecta al acceso de las autoridades competentes a los registros centralizados de cuentas bancarias a través del sistema de interconexión y a las medidas técnicas destinadas a facilitar el uso de los registros de operaciones:**

- Pretende garantizar que las autoridades policiales nacionales también tengan acceso a los registros centralizados de cuentas bancarias mediante el punto de acceso único.

El plazo de transposición de esta Directiva finalizará el **10 de julio de 2027**.

MOLINS Compliance

Novedades legislativas

Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (Reglamento del Parlamento Europeo y del Consejo de Inteligencia Artificial -AIA, por *Artificial Intelligence Act*-)

El **Reglamento IA** busca regular los **usos de la Inteligencia Artificial** para limitar los riesgos que de ellos se derivan.

Su **ámbito de aplicación** se extiende a:

- Los **proveedores** de sistemas de IA que se pongan en servicio o comercialicen dentro de la UE o se utilicen en la UE, independientemente de su origen;
- Los **usuarios** de estos que se encuentren en la UE, considerando usuarios a quienes explotan esos sistemas, y no a los afectados.
- Los **proveedores y usuarios de sistemas de IA** que se encuentren en un tercer país, cuando los sistemas produzcan resultados que se utilicen en la UE.

Entre otras cuestiones, el presente Reglamento **clasifica la IA según el nivel de riesgo**:

- **Riesgo inaceptable (IA prohibida):** se incluyen los sistemas de IA que distorsionen comportamientos humanos, la evaluación y clasificación social, y la identificación biométrica remota en tiempo real (en espacios públicos).
- **Riesgo alto (IA permitida con limitaciones):** cubre la IA aplicable a la educación y formación profesional, a infraestructuras esenciales (*v.g.:* el transporte), a la selección de personal, gestión de trabajadores y acceso al autoempleo, al acceso y disfrute de servicios privados esenciales y servicios y prestaciones públicas, al cumplimiento de la ley, a la gestión de la migración, al asilo y el control de fronteras, y la administración de justicia y procesos democráticos. Para los sistemas de riesgo alto, se establecen diversas obligaciones: contar con un sistema de gestión de riesgos, establecer una gobernanza y gestión de los datos de entrenamiento y prueba, disponer de documentación técnica actualizada que demuestre el cumplimiento de los requisitos exigidos, contar con registros de actividad del sistema, entre otros.
- **Riesgo limitado (IA permitida con menos limitaciones)**: se establece la obligación de garantizar la supervisión humana y la notificación a los usuarios cuando estén interactuando con sistemas de IA.
- **Riesgo mínimo (IA permitida)**: incluye aquellos sistemas de IA que no estén incluidos dentro de las categorías anteriores.

Una de las instituciones clave en la implementación y supervisión de este reglamento es **la Oficina de Inteligencia Artificial de la UE**, creada por la Comisión Europea, que se ocupará de **coordinar actividades regulatorias y de supervisar a nivel europeo**, asegurando una **aplicación coherente en todos los Estados miembros**. Además, también proporcionará orientación técnica y operativa a desarrolladores y usuarios de IA, gestionará informes de incidentes relacionados con IA, entre otras funciones.

Por otro lado, el Reglamento de IA crea un **Consejo Europeo de IA**, con funciones de **asesoramiento y asistencia** a los Estados miembros para asegurar una aplicación coherente.

A nivel nacional, se establece la obligación a los Estados miembros de designar al menos una **autoridad nacional de vigilancia del mercado y una autoridad notificante.**

En este sentido, y ante el **creciente uso de sistemas de IA** en entidades de todos los sectores, resulta crucial el cumplimiento con la normativa regulatoria mediante la protocolización de medidas de gestión y control.

Adoptar **medidas para garantizar la seguridad y la ética** en la aplicación de la IA, permite a las entidades demostrar de manera proactiva su compromiso con la regulación y la responsabilidad social. Ello no solo contribuye a evitar sanciones, sino que también aumenta la confianza de terceros como clientes y socios comerciales.

El Reglamento entrará en vigor el **1 de agosto de 2024** y será de aplicación el **1 de agosto de 2026**, con algunas excepciones.

MOLINS Compliance

Tribunales

MOLINS
Compliance

- Sentencia 179/2023, de 11 de diciembre de 2023 de la Sala Segunda del Tribunal Constitucional
- Sentencia del Tribunal Supremo (Sala de lo Social) 225/2024, de 6 de febrero de 2024.
- Sentencia del Tribunal Supremo 165/2024, de 22 de febrero de 2024.
- Sentencia del Tribunal Supremo 217/2024, de 7 de marzo de 2024.
- Sentencia del Tribunal Supremo 298/2024, de 8 de abril de 2024.
- Sentencia del Tribunal Supremo 874/2024, de 5 de junio de 2024.

MOLINS Compliance

Sentencia 179/2023, de 11 de diciembre de 2023 de la Sala Segunda del Tribunal Constitucional

En la presente resolución, el Tribunal Constitucional se pronuncia sobre el recurso de amparo interpuesto por Banco Santander, S.A., contra los acuerdos del Consejo de Ministros que sancionaron a la entidad por **la falta de comunicación de operaciones sospechosas de blanqueo de capitales**. Esta sanción se originó tras una **inspección del SEPBLAC a Banco Popular, S.A.,** entidad que luego fue **absorbida por Banco Santander**. Se impuso una multa de 1.056.000 euros por una **infracción muy grave del artículo 51.1.a)** de la Ley 10/2010 de prevención de blanqueo de capitales y de la financiación del terrorismo (LPBC), debido a la **omisión de notificación de ciertas operaciones sospechosas**.

Banco Santander alegó que la **sanción violaba el principio de legalidad sancionadora** del artículo 25.1 de la Constitución Española (CE), en sus vertientes de **culpabilidad y personalidad de la pena**. Argumentó la inexistencia de continuidad entre Banco Popular, S.A. y Banco Santander, así como cambios en los procedimientos de prevención del blanqueo tras la absorción y la ausencia de beneficio derivado de la conducta infractora. No obstante, el **Tribunal Constitucional** sostiene que, según la jurisprudencia consolidada del Tribunal Supremo y el Tribunal de Justicia de la Unión Europea, en los casos de fusión por absorción, la **responsabilidad por infracciones administrativas** se **transmite** cuando existe una "**identidad económica sustancial**", asegurando así la continuidad de las responsabilidades al **persistir la misma actividad económica bajo una nueva titularidad jurídica**.

El Tribunal concluye que la **resolución sancionadora no vulnera los principios de culpabilidad y personalidad de la pena** del artículo 25.1 CE. La "identidad económica sustancial" entre Banco Popular, S.A. y Banco Santander, S.A. justifica la transmisión de la responsabilidad por infracción, y la **ausencia de beneficio no elimina dicha responsabilidad**. En consecuencia, se desestima el recurso de amparo presentado por Banco Santander, ratificando la validez de la sanción impuesta.

Sentencia del Tribunal Supremo (Sala de lo Social) 225/2024, de 6 de febrero de 2024.

El **Tribunal Supremo** aborda en la presente resolución la nulidad de las directrices establecidas por una empresa sobre el uso de dispositivos digitales proporcionados a los empleados, debido a la **falta de participación de los representantes de los trabajadores en la elaboración de la política de usos de dispositivos digitales (políticas IT o TIC).**

Este fallo se basa en el **incumplimiento del artículo 87.3 de la Ley Orgánica de Protección de Datos (LOPD)**, que exige la **participación de los representantes de los trabajadores en la creación de políticas relacionadas con el uso de tecnologías de la información y comunicación**. La empresa argumentó que la nulidad de las instrucciones **vulneraba su derecho al control empresarial** (artículo 20.3 del Estatuto de los Trabajadores), y sostuvo que las instrucciones impugnadas eran solo un recordatorio de políticas previas a la entrada en vigor del artículo 87.3 de la LOPD en 2018.

Sin embargo, el Tribunal Supremo concluyó que, si bien la obligación de incluir a los representantes de los trabajadores en la creación de dichas políticas (art. 87.3 LOPD) no tiene efectos retroactivos, las directrices representaban un cambio fundamental en las normas de uso y su control, confirmando la nulidad de éstas.

Sentencia del Tribunal Supremo (Sala de lo Penal) 165/2024, de 22 de febrero de 2024

En la presente sentencia, el Tribunal Supremo aborda el recurso de casación interpuesto contra una condena por un **delito de alzamiento de bienes**.

Los recurrentes, entre otras cuestiones, alegaban que el **delito de alzamiento** de bienes se configuraba como un **delito especial propio**, cuyo autor debe ser el deudor, y que ellos **no podían ser condenados como tales sin una acusación directa contra la persona jurídica**.

El Tribunal Supremo rechazó este argumento, afirmando que el **artículo 31 del Código Penal extiende la responsabilidad a quienes realicen los actos de ejecución como administradores de hecho de una persona jurídica**, aunque no concurran en ellos las condiciones exigidas para ser sujetos activos del delito.

La sentencia concluyó que ambos recurrentes ejercieron control **efectivo sobre las empresas implicadas y orquestaron la venta de activos para eludir el pago de deudas laborales**, lo que justificaba su condena.

MOLINS Compliance

Sentencia del Tribunal Supremo (Sala de lo Penal) 217/2024, de 7 de marzo de 2024

La presente sentencia del Tribunal Supremo aborda el supuesto de defraudación tributaria y de responsabilidad penal de una sociedad mercantil. Los hechos se encuentran relacionados con la actividad **fiscal de la empresa y de su administrador**, quien fue **condenado por varios delitos de defraudación tributaria** del IVA y del impuesto de sociedades de los años 2011 y 2012.

Específicamente, en cuanto a la responsabilidad penal de la persona jurídica, el Tribunal Supremo confirmó la imposición de **multas significativas y la pérdida de beneficios fiscales para la mercantil**, haciendo hincapié en que la misma, en su conjunto, fue **utilizada para cometer los ilícitos tributarios**. Por último, el Tribunal Supremo aclaró que las **penas impuestas**, tanto a la persona física como a la jurídica, a pesar de los argumentos de la defensa sobre una posible duplicación de la carga financiera, eran absolutamente **proporcionales a la gravedad de los hechos**.

Sentencia del Tribunal Supremo (Sala de lo Penal) 298/2024, de 8 de abril de 2024

La sentencia del Tribunal Supremo, STS 298/2024, resuelve un recurso de casación interpuesto por varios de los condenados por delitos contra la Hacienda Pública y falsedad documental. El caso involucra a principalmente a tres personas jurídicas, y a sus respectivos propietarios.

El Alto Tribunal sostiene que las **mercantiles en cuestión facilitaron la defraudación tributaria mediante contratos simulados y pagos ficticios**. A su vez, discute la aplicación del artículo 31 *bis* del Código Penal, que **extiende la responsabilidad penal a las personas jurídicas cuando sus directivos o empleados cometen delitos en beneficio de la entidad**. En este caso, se concluyó que, efectivamente, las sociedades habían sido **utilizadas para ocultar ingresos y facilitar dicha defraudación**.

Sin embargo, el Tribunal Supremo decidió absolver a las tres personas jurídicas, argumentando que **no había quedado demostrada la existencia de un beneficio directo o indirecto derivado del delito de defraudación tributaria** cometido por las respectivas personas físicas involucradas.

Entre otros, el Tribunal Supremo aclara que el fraude fiscal cometido por una de las personas físicas no solo **no generó beneficios adicionales para estas empresas**, sino que más bien **las perjudicó**. Además, destaca que la doble condena a las empresas y sus directivos, en el presente supuesto, vulneraría el **principio de *non bis in idem***.

Sentencia del Tribunal Supremo (Sala de lo Social) 874/2024, de 5 de junio de 2024

En la presente resolución, el Tribunal Supremo se pronuncia sobre el despido disciplinario de una trabajadora quien fue sorprendida con mercancía sin pagar en su bolso tras sonar la alarma antihurtos.

El **registro del bolso** fue realizado por un **vigilante de seguridad sin la presencia de un representante legal de los trabajadores ni de otro trabajador**, violando el **artículo 18 del Estatuto de los Trabajadores** (ET).

La falta de observancia de dichas garantías legales dio lugar a que, por su parte, el Tribunal Superior de Justicia de Andalucía **declarara nulo el despido**, ya que el registro, sin las debidas garantías, **carecía de valor probatorio**.

Así, en la presente resolución, **Tribunal Supremo confirma que el artículo 18 del ET exige la presencia de un representante legal de los trabajadores o de otro trabajador para asegurar la objetividad y eficacia de la prueba**.

La ausencia de esta garantía implica que cualquier prueba obtenida en el registro no puede ser utilizada para justificar el despido. Además, se subraya que el cumplimiento de estas normas es fundamental para **proteger los derechos de los trabajadores y mantener la integridad del proceso disciplinario**.

En este supuesto, la responsabilidad penal de la persona jurídica se centra en no haber asegurado desde la misma que el registro del bolso de la empleada en cuestión se realizara conforme a las garantías legales, lo que llevó a la vulneración de los derechos de la trabajadora y la nulidad del despido. Finalmente, la empresa fue **condenada a readmitir a la trabajadora y a abonar los salarios dejados de percibir**.

MOLINS Compliance

Otros acuerdos y resoluciones sancionadoras en materia de *Compliance*

MOLINS
Compliance

- Robo de 23,7 millones de euros mediante un fraude con inteligencia artificial.
- AEPD multa a una empresa española con 365.000 euros por hacer a sus empleados fichar con huella.
- Santander, BBVA y Telefónica despiden a 590 trabajadores por denuncias de compañeros
- Multa de 32 millones a Amazon por ir demasiado lejos en la vigilancia a sus empleados.
- Más de 16 millones de euros en multas por infracciones en privacidad en 2023.
- Directivos de Adidas en China investigados por un caso de presunta corrupción.
- BBVA, sancionado con 200.000 euros por incluir a un cliente en el fichero de morosos sin aviso previo.

MOLINS Compliance

Otros acuerdos y resoluciones sancionadoras en materia de *Compliance*

MOLINS Compliance

Robo de 23,7 millones de euros mediante un fraude con inteligencia artificial

Un **empleado de una empresa financiera** en Hong Kong **transfirió 23,7 millones de euros a lo que creía era la filial británica de su compañía**, engañado por una sofisticada **estafa de inteligencia artificial**.

Los estafadores utilizaron la tecnología ***deepfake*** para simular ser el director financiero y otros colegas durante una videollamada, convenciendo al empleado de la legitimidad de la solicitud de transferencia. La policía de Hong Kong ha realizado seis arrestos relacionados con el caso, destacando la preocupación por el aumento de este tipo de fraudes con el avance de las tecnologías generativas de inteligencia artificial.

AEPD multa a una empresa española con 365.000 euros por hacer a sus empleados fichar con huella

La **Agencia Española de Protección de Datos ha multado con 365.000 euros** a una empresa española por **solicitar la huella dactilar** a los empleados para fichar.

La empresa en cuestión recopilaba los **datos biométricos de los empleados y los almacenaba en el portal del empleado**, sin haberles informado previamente de este hecho.

La empresa alegó que se había **informado del tratamiento de datos correctamente**. Sin embargo, se comprobó que la **información proporcionada no era suficiente y que no se garantizaba el borrado de la huella tras su captura**, almacenándose los datos identificativos del empelado.

Santander, BBVA y Telefónica despiden a 590 trabajadores por denuncias de compañeros

Durante el año 2023, **Santander, BBVA y Telefónica despidieron a un total de 590 empleados por denuncias de compañeros** interpuestas a través de los canales internos de denuncia.

Concretamente, al banco Santander despidió a 366 empleados, mientras que el BBVA a 115 y, por último, Telefónica a 109.

La tramitación de estas situaciones a través del canal de denuncias permite llevar a cabo la correspondiente **investigación de los hechos mediante el procedimiento establecido** preservando las **garantías y derechos de la persona informante**.

Multa de 32 millones a Amazon por ir demasiado lejos en la vigilancia a sus empleados

La **Agencia Francesa de Protección de Datos** (CNIL) ha impuesto a Amazon *France Logistique* una **multa de 32 millones de euros por un sistema de control laboral considerado "excesivamente intrusivo"**.

Este sistema, que involucra escáneres para medir en tiempo real la productividad de los empleados ha sido criticado por **violar el derecho a la intimidad y los principios del Código de Trabajo francés**.

La CNIL también cuestiona la **conservación de datos detallados sobre la actividad de los trabajadores y la falta de adecuada información sobre el sistema de videovigilancia**. Amazon, por su parte, ha defendido estos métodos como estándares de la industria para asegurar la calidad y la eficiencia laboral, anunciando su intención de apelar la decisión.

Directivos de Adidas en China investigados por un caso de presunta corrupción

Varios empleados de Adidas en China acusaron públicamente de **fraude a directivos de la compañía por un presunto caso de sobornos** a gran escala.

Concretamente esta acusación se fundamenta en diversas **capturas de pantalla** en las que se afirma que los **directivos recibían sobornos y otros regalos físicos**, como bienes inmuebles, por parte de proveedores de **servicios externos para conseguir la formalización del contrato entre Adidas y los mismos.**

MOLINS Compliance

Otros acuerdos y resoluciones sancionadoras en materia de *Compliance*

MOLINS
Compliance

Más de 16 millones de euros en multas por infracciones en privacidad en 2023

En 2023, la **Agencia Española de Protección de Datos (AEPD) impuso más de 16 millones de euros en multas** por diversas infracciones de privacidad.

La **sanción más elevada**, de 6 millones de euros, **recayó sobre Endesa** por una **brecha de seguridad** que comprometió los datos de millones de personas. Este incidente subraya la importancia crítica de mantener medidas rigurosas de seguridad de datos. Además, se espera que las multas en 2024 sean menos frecuentes, pero de mayor cuantía, reflejando una tendencia hacia una **aplicación más severa del Reglamento General de Protección de Datos (RGPD) en España**.

Las empresas enfrentan desafíos significativos en la implementación adecuada de medidas de seguridad y protección de datos, particularmente en sectores como servicios financieros y telecomunicaciones, donde **los riesgos de incumplimiento son más elevados debido al manejo de datos sensibles y la necesidad de robustas salvaguardas de seguridad**.

BBVA, sancionado con 200.000 euros por incluir a un cliente en el fichero de morosos sin aviso previo

La **Agencia Española de Protección de Datos impuso una multa de 200.000 euros al BBVA** por solicitar la **inclusión de datos personales de un cliente en el fichero de morosos** sin la notificación previa pertinente.

En el presente supuesto, el cliente en cuestión fue **incluido en esta lista por el impago** de **tarjeta de crédito** en calidad de titular. El problema reside en el hecho de que no se le notificó esta inclusión porque la dirección facilitada no era exacta, causándole un grave perjuicio.

Estos hechos constituyen una **infracción del artículo 5.1.d) de Reglamento General de Protección de Datos**, que exige la exactitud de los datos personales recogidos, actualizando los mismos cuando sea necesario.

MOLINS Compliance

Guías, resoluciones institucionales e informes de interés

MOLINS Compliance

- ISO 42001, Sistemas de Gestión de Inteligencia Artificial.
- ISO 45004, Salud y Seguridad en el trabajo. Sistemas de Gestión de Seguridad y Salud en el Trabajo. Evaluación del desempeño.
- UNE 15713, Destrucción segura de material confidencial y sensible.
- UNE 171380, Medición en continuo de CO2 en interiores para la prevención en salud y mejora del bienestar.
- UNE-ISO 10010, Gestión de la calidad. Orientación para comprender, evaluar y mejorar la cultura de la calidad en la organización.
- UNE-ISO 10017, Gestión de la calidad. Orientación sobre técnicas estadísticas para la Norma ISO 9001:2015.
- UNE-ISO 53800, Directrices para la promoción e implementación de la igualdad de género y el empoderamiento de las mujeres.
- La "Guía de cuantificación de daños por infracciones del derecho de la competencia" de la CNMC.
- Dictamen 0077/2023 de la AEPD sobre la viabilidad del 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.
- Publicación de la resolución a las preguntas más frecuentes sobre 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 por parte de la Oficina Antifraude de Cataluña.

MOLINS compliance

Guías, resoluciones institucionales e informes de interés

MOLINS Compliance

ISO 42001, Sistemas de Gestión de Inteligencia Artificial

En respuesta al **auge de la Inteligencia Artificial** (IA) y a los **desafíos** que presenta, las organizaciones ISO e IEC han desarrollado la norma ISO/IEC 42001:2023.

Esta iniciativa responde a la necesidad de **gestionar** adecuadamente los **riesgos** y **maximizar los beneficios** que la IA y el aprendizaje automático pueden aportar a la sociedad y la economía, como la **interpretación avanzada de datos y los diagnósticos remotos**.

La norma ISO/IEC 42001:2023, aplicable a cualquier empresa, tiene por objeto asegurar un **desarrollo y uso responsable** de la IA, promoviendo principios éticos como la **equidad y el respeto a la privacidad**.

La presente norma ISO sirve de ayuda a las organizaciones a identificar y mitigar riesgos, garantizando el cumplimiento legal y la protección de datos. Además, prioriza el bienestar humano y la **seguridad en el diseño y despliegue** de sistemas de IA, contribuyendo así a la **resiliencia y sostenibilidad empresarial**.

ISO 45004, Salud y Seguridad en el trabajo. Sistemas de Gestión de la Seguridad y Salud en el Trabajo. Evaluación del desempeño

La norma ISO 45004:2024 proporciona una guía para que las organizaciones de cualquier tipo dispongan de **indicaciones sobre cómo proceder en los siguientes aspectos**:

- Establecimiento de **procesos de monitoreo, medición, análisis y evaluación del desempeño en salud y seguridad en el trabajo** (SST).
- **Desarrollo de indicadores** relevantes para medir el éxito de sus iniciativas de SST.
- **Determinación del cumplimiento de los resultados y objetivos** en materia de SST.
- Identificación de **áreas de mejora y ejecución de medidas para mejorar** la eficiencia y productividad de la organización.

La implementación de la norma ISO 45004:2024 permite **mejorar el desempeño del SST y demostrar la eficacia de sus sistemas de gestión**, aportar una **mayor confianza a las partes interesadas**, **identificar y abordar los riesgos** de SST de manera proactiva, así como **reducir los accidentes y enfermedades laborales**.

UNE 15713, Destrucción segura de material confidencial y sensible

La **norma UNE 15713:2024** establece **requisitos y recomendaciones** para llevar a cabo de manera segura los **procesos de destrucción física de material confidencial y sensible en el seno de cualquier empresa que procese este tipo de materiales**.

La presente norma regula distintas situaciones, abarcando aspectos como la utilización de equipos móviles en el lugar de uso y el uso de equipos por parte del responsable del tratamiento de datos.

Entre los temas abordados en la norma, se encuentra el **registro del proceso**, desde la recogida hasta la **destrucción, la subcontratación, los acuerdos de confidencialidad del personal, la recogida y transporte de material confidencial y sensible**, así como el **almacenamiento y conservación** de dicho material en la instalación de destrucción.

UNE 171380, Medición en continuo de CO2 en interiores para la prevención en salud y mejora del bienestar

Ante la necesidad de **complementar y mejorar los requisitos establecidos por las normas de calidad y la legislación actual**, se desarrolla la nueva norma UNE 171380:2024.

Este estándar resulta de aplicación en todos los **edificios de uso colectivo**, incluyendo tanto los de nueva construcción como los ya existentes.

La presente norma contempla los **requisitos que deben cumplir los equipos de medición**, el proyecto para su implantación en atención a la tipología y usos del edificio, la **gestión de los datos obtenidos**, así como el establecimiento de los **umbrales de concentración de CO2** previstos para la calidad del aire y los **procedimientos de auditoría** de los mismos.

MOLINS Compliance

Guías, resoluciones institucionales e informes de interés

MOLINS Compliance

UNE-ISO 10010, Gestión de la calidad. Orientación para comprender, evaluar y mejorar la cultura de la calidad en la organización

La **norma UNE-ISO 10010:2024** establece recomendaciones sobre la **evaluación, desarrollo y mejora** de la **gestión de la calidad en una organización**.

Este estándar contempla los **conceptos fundamentales y principios generales** de gestión de la calidad, así como el **compromiso específico de las personas** que conforman la organización y la necesidad de **liderazgo** de las mismas en este proceso.

UNE-ISO 10017, Gestión de Calidad. Orientación sobre técnicas estadísticas para la Norma ISO 9001:2015

La **nueva UNE-ISO 10017:2024** proporciona **directrices a las organizaciones para gestionar su calidad mediante el control estadístico de sus procesos**. Este control incluye la selección de técnicas estadísticas que promuevan el **desarrollo, implementación, mantenimiento y mejora de un sistema de gestión de la calidad**, de conformidad con lo previsto en la **UNE-EN ISO 9001:2015**.

UNE-ISO 53800, Directrices para la promoción e implementación de la igualdad de género y el empoderamiento de las mujeres

Las persistentes **desigualdades de género dentro de las organizaciones** reflejan la necesidad de desarrollar normativa que erradique la discriminación estructural existente en la sociedad actual. Ante esta situación, la **norma UNE-ISO 53800:2024** proporciona **directrices, definiciones, procedimientos y herramientas** a las **organizaciones públicas y privadas** destinadas a **fomentar y orientar** que las mismas avancen hacia el logro de la igualdad de género tanto dentro de la organización, como fuera de la misma.

La "Guía de cuantificación de daños por infracciones del derecho de la competencia" de la CNMC

La nueva **Guía de Cuantificación de Daños por Infracciones del Derecho de la Competencia, publicada por la Comisión Nacional de los Mercados y la Competencia (CNMC),** establece un marco detallado para calcular los perjuicios económicos causados por violaciones a las normas de competencia en España. Esta guía tiene por **objeto facilitar a los tribunales y a las partes afectadas herramientas precisas y metodologías claras para determinar el alcance de los daños sufridos**, especialmente en casos de prácticas anticompetitivas como acuerdos restrictivos o abusos de posición dominante.

En sus nuevas directrices, la CNMC enfatiza sobre la importancia de **adoptar enfoques robustos y consistentes en la cuantificación de daños**, incluyendo métodos como el análisis comparativo, los modelos econométricos y la evaluación de datos financieros y comerciales. Asimismo, subraya la necesidad de considerar adecuadamente el contexto económico y sectorial en el que se produjeron las infracciones, asegurando que las compensaciones reflejen de manera precisa los perjuicios ocasionados a los consumidores y otras partes afectadas por prácticas contrarias a la competencia leal.

MOLINS Compliance

Guías, resoluciones institucionales e informes de interés

MOLINS Compliance

Dictamen 0077/2023 de la AEPD sobre la viabilidad del 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

La AEPD, en su Dictamen 77/2023, evalúa la posibilidad de **tratar datos personales** recibidos a través del Sistema de Información Interno (SII) para **fines distintos a los establecidos por la Ley 2/2023**, que protege a denunciantes de incumplimientos normativos.

Así, para **entidades obligadas** por esta ley, el **tratamiento está justificado** por el cumplimiento de **obligaciones legales (artículo 6.1**.c) del RGPD), mientras que para las **no sujetas**, el mismo podría basarse en el **interés legítimo del responsable del tratamiento**, siempre protegiendo derechos fundamentales.

Por último, cabe destacar que la Agencia hace especial hincapié en la necesidad de adherirse al **principio de limitación de la finalidad**, asegurando que los datos se recolecten para **fines específicos, explícitos y legítimos (artículo 5.1.b) del RGPD**, evaluando la **compatibilidad de cualquier nuevo tratamiento** con las **expectativas razonables** de los interesados y asegurando siempre la **adecuada protección de los datos personales** según lo establecido por la normativa vigente y los principios de protección de datos.

Resolución de las preguntas más frecuentes sobre 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 por parte de la Oficina Antifraude de Cataluña

La **Oficina Antifraude de Cataluña**, como autoridad autonómica competente en materia de protección de las personas alertadoras, actualiza de forma continua su **compendio de respuestas a las dudas más frecuentes que han sido planteadas en relación con la interpretación de 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.

Entre muchas otras cuestiones, **destacan por su incidencia práctica** las siguientes:

- ¿Qué obligaciones origina la entrada en vigor de la Ley 2/2023?
- Las personas que comuniquen una infracción comprendida dentro del ámbito de la Ley 2/2023, mediante el canal interno de una entidad no obligada, ¿gozan de protección ante esta entidad?
- ¿Cómo debe notificarse a la Oficina Antifraude el nombramiento y el cese de la/las persona/s responsable/s del Sistema Interno de Información?. Sobre este aspecto, es relevante destacar que la Oficina Antifraude de Cataluña **ha actualizado el formulario** para comunicar el nombramiento y cese de la persona física o personas que forman parte del órgano colegiado designado como responsable del sistema interno de información. Este formulario está **disponible en su página web**.

MOLINS Compliance

Publicaciones del Departamento del *Compliance* (enero-julio 2024)

MOLINS
Compliance

- Actualidad en materia de *Compliance*: la publicación de la UNE 19603 sobre sistemas de gestión de *Compliance* en materia de libre competencia.
- Finalizado el plazo de adaptación del uso de *cookies.*
- La nueva *Foreign Extortion Prevention Act.*
- Sobre el delicado equilibrio entre la normativa de igualdad y de *Compliance* en relación con los Protocolos de actuación ante el acoso laboral y sexual.
- ¿Existe sucesión en la responsabilidad administrativa en M&A? Breve comentario de la Sentencia 1769/2023, de 11 de diciembre de 2023, de la Sala Segunda del Tribunal Constitucional.
- El reto de la presentación de información de sostenibilidad corporativa para las organizaciones en relación con el nuevo informe "Apoyo de las normas para el reporte ESG".
- Más del 80% de las empresas catalanas no cumplen con la Ley 2/2023.
- España continua su lucha contra la corrupción: Un análisis detallado de los avances judiciales en 2023.
- Tres apuntes en materia de responsabilidad penal de las personas jurídicas: la Sentencia núm. 298/2024 de 8 de abril de 2024.
- Avance en la implementación de la Autoridad Independiente de Protección del Informante.
- ¿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?

MOLINS Compliance

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