AON

A&O SHEARMAN

# La asegurabilidad de las multas cibernéticas

España

# Resumen Ejecutivo

Los incidentes cibernéticos están proliferando en todos los sectores y jurisdicciones, lo que ha dado lugar a nuevas regulaciones destinadas a promover la resiliencia, así como a multas y sanciones para las empresas, los ejecutivos y los miembros de los consejos de administración.

El seguro cibernético es un pilar fundamental de la estrategia de gestión de riesgos cibernéticos de cualquier gran organización. No solo ayuda a recuperar las pérdidas financieras, los costes y las responsabilidades tras un incidente, sino que también promueve las mejores prácticas y la resiliencia a través del proceso de suscripción. Si bien el objetivo general de los seguros cibernéticos es proporcionar una protección integral contra la amplia gama de riesgos que pueden derivarse de un incidente cibernético, es igualmente importante comprender los límites de la cobertura.

Hasta hace poco, las obligaciones reglamentarias de las empresas afectadas por incidentes cibernéticos se basaban principalmente en las leyes de protección de datos, y algunas jurisdicciones añadían requisitos de resiliencia operativa de alcance limitado. Ese panorama ha cambiado significativamente y sigue evolucionando. Por ejemplo, Europa ha introducido marcos importantes como DORA y NIS2, mientras que el Reino Unido ha publicado recientemente el proyecto de ley de ciberseguridad y resiliencia.

Hay tendencias claras que están surgiendo. En primer lugar, las fuentes de las multas cibernéticas se han ampliado considerablemente. Más allá de la aplicación de la protección de datos, un número cada vez mayor de regulaciones específicas para el ámbito cibernético y sectoriales aumenta el riesgo de sanciones monetarias sustanciales e introduce sanciones no monetarias, como prohibiciones de gestión y suspensiones operativas.

En segundo lugar, la asegurabilidad de las multas cibernéticas sigue siendo una cuestión incierta y específica de cada jurisdicción. Las leyes nacionales y las políticas públicas dictaminan si dichas sanciones pueden estar cubiertas por un seguro, y algunos países imponen prohibiciones generales. Otros permiten los seguros, excepto en casos de conducta indebida deliberada o imprudente.

En tercer lugar, la aplicación de la ley es cada vez más firme. Los reguladores no solo imponen multas significativas, sino que también examinan la idoneidad de las medidas técnicas y organizativas, la puntualidad de la notificación de las infracciones y la solidez de la respuesta a los incidentes.

Los recientes casos de gran repercusión, que van desde multas multimillonarias a empresas tecnológicas globales hasta la aplicación de la ley en sectores específicos como la sanidad y los servicios financieros, subrayan la necesidad de adoptar un enfoque proactivo y holístico de la gestión de los riesgos cibernéticos. Aún no se sabe con certeza cómo se aplicarán las nuevas normativas, ni si estas darán lugar a un aumento significativo de las medidas coercitivas.

La aparición de mecanismos de reparación colectiva y de demandas colectivas, especialmente tras la aplicación de la Directiva sobre acciones representativas de la UE, añade una nueva capa de riesgo de litigios. Las organizaciones deben ahora anticiparse tanto a las investigaciones reglamentarias como a la posibilidad de reclamaciones coordinadas por parte de las personas afectadas y los grupos de consumidores.

De cara al futuro, se prevé que el entorno normativo sea cada vez más exigente y cambiante. El cumplimiento normativo es un proceso continuo. Es probable que las normas se endurezcan con el tiempo, lo que exigirá una atención y una adaptación constantes por parte de las organizaciones y sus directivos. La Ley de IA de la UE, con sus estrictos requisitos de ciberseguridad para los sistemas de IA de alto riesgo y la posibilidad de sanciones acumulativas junto con el RGPD, ejemplifica esta tendencia.

Las nuevas normativas imponen una mayor responsabilidad a los consejos de administración y a la alta dirección, con responsabilidad directa y mayores expectativas en materia de supervisión e inversión en ciberresiliencia.

Este informe destaca la importancia de comprender los matices legales locales, la necesidad de una estrecha colaboración entre las funciones jurídicas, de riesgo y de seguros, y la imperiosa necesidad de adelantarse a la evolución normativa. A medida que el panorama de las amenazas sigue evolucionando, también deben hacerlo las estrategias para gestionar la exposición legal y financiera.

Esperamos que este informe sirva de recurso práctico para los gerentes de riesgos, los asesores jurídicos internos y los profesionales de los seguros a la hora de afrontar los retos del riesgo cibernético en un mundo cada vez más regulado.

**Charlie Weston-Simons**
A&O Shearman

**Pablo Constenla**
Aon

# Índice de Contenidos

## España

# 1 ¿Cuáles son las principales fuentes de multas cibernéticas?

## Resumen del capítulo

En todas las jurisdicciones mundiales, la exposición a multas tras incidentes cibernéticos viene determinada por la privacidad, la ciberseguridad y los regímenes y normativas sectoriales, que cada vez se solapan más.

En la UE, el RGPD es el marco dominante, que impone importantes multas administrativas por violaciones de datos, accesos no autorizados y fallos en la protección de datos.

Las leyes nacionales complementan el RGPD, y las autoridades locales de protección de datos están facultadas para hacer cumplir la normativa e imponer multas de hasta 20 millones de euros o el 4% de la facturación global por infracciones cibernéticas graves.

La Directiva NIS2 y sus implementaciones nacionales amplían las obligaciones de resiliencia cibernética a sectores críticos, introduciendo multas adicionales por fallos en la gestión de riesgos de ciberseguridad y la notificación de incidentes. Las normativas específicas de cada sector, como DORA para los servicios financieros y la Ley de Resiliencia Cibernética para los productos digitales, amplían aún más el panorama de posibles multas. Esta combinación de protección de datos, resiliencia operativa y normativas específicas de cada sector se reproduce en el Reino Unido.

Fuera de la UE y del Reino Unido, países como Sudáfrica, Arabia Saudí y Turquía han promulgado sus propias leyes de protección de datos y ciberdelincuencia, con diversos grados de alineación con las normas de la UE y del Reino Unido.

Las multas varían tanto por jurisdicción como por sector. Pueden ser administrativas o penales, y algunas jurisdicciones permiten la responsabilidad personal de los directores y la dirección. Se está produciendo un aumento de la complejidad y la severidad de las multas cibernéticas, impulsado tanto por la armonización de la normativa de la UE como por la diversidad de enfoques nacionales.

También existe una tendencia hacia sanciones máximas más elevadas, una cobertura sectorial más amplia y la creciente importancia de las sanciones no monetarias, como las suspensiones operativas y las prohibiciones de gestión. También estamos observando límites máximos más elevados y una aplicación más granular y técnica, especialmente en sectores críticos y en infraestructuras digitales.

El mercado de los seguros cibernéticos ha adoptado un enfoque flexible para cubrir las multas cibernéticas, siempre que dicha cobertura sea legalmente admisible. Cuando es posible imponer multas cibernéticas a los directores o altos ejecutivos (por ejemplo, en virtud de la NIS2), los seguros de responsabilidad civil para directores y consejeros (D&O) deben responder de forma similar.

## Medidas prácticas que las organizaciones deben considerar

Supervisar los cambios normativos: mantenerse al día sobre las nuevas leyes (por ejemplo, la Ley de Resiliencia Cibernética, la Ley de IA de la UE).

Establecer procedimientos sólidos de respuesta a incidentes y notificación de infracciones

- Asegurar que la alta dirección sea consciente de los riesgos de responsabilidad personal.
- Realizar un ejercicio de mapeo de riesgos jurisdiccionales: identificar qué leyes se aplican a tus operaciones en todos los países y sectores.
- Nombrar a un responsable de cumplimiento: asignar la responsabilidad de supervisar los cambios normativos y coordinar las respuestas.
- Revisar periódicamente y asegurar que se cumple con el RGPD, INIS2, DORA y las normativas específicas del sector.
- Realizar simulacros: simular escenarios de incumplimiento para poner a prueba la preparación de la respuesta y el compromiso normativo.
- Realizar auditorías periódicas de ciberseguridad y formación del personal: demostrar un cumplimiento proactivo.
- Mantener registros actualizados del tratamiento de datos y las medidas de seguridad en caso de una revisión o investigación reglamentaria.
- Colaborar de forma proactiva con los reguladores: establecer relaciones con las autoridades de protección de datos y las agencias de ciberseguridad para facilitar una gestión más fluida de los incidentes.
- Asegurarse de obtener la mejor cobertura de seguro posible para cubrir las multas cibernéticas en la medida de lo posible.

## España

### Leyes y reglamentos sobre protección de datos y privacidad (por ejemplo, la Ley de Protección de Datos de 2018, el RGPD del Reino Unido y la legislación de aplicación de la Directiva sobre privacidad electrónica [PECR] en Inglaterra y Gales).

La fuente principal de exposición monetaria tras un incidente cibernético está relacionada principalmente con el Reglamento General de Protección de Datos (RGPD) de la UE y la Ley Orgánica 3/2018 de Protección de Datos y Derechos Digitales (LOPDGDD) de España. La Agencia Española de Protección de Datos (AEPD) puede imponer multas administrativas en el nivel más alto del RGPD, hasta un máximo de 20 millones de euros o el 4% de la facturación anual mundial para las infracciones graves, y en el nivel más bajo para otras obligaciones, junto con órdenes correctivas que incluyen órdenes de cumplimiento, advertencias y prohibiciones de tratamiento.

Las normas procesales y de clasificación españolas en virtud de la LOPDGDD complementan esos límites máximos de la UE y prevén la publicación de sanciones por encima de determinados umbrales.

En la práctica, las sanciones tras incidentes cibernéticos que se consideran violaciones de datos personales se basan con frecuencia en el principio de confidencialidad del artículo 5, apartado 1, letra f), del RGPD y en el artículo 32 (seguridad del tratamiento), junto con, en algunos casos, los artículos 25 (protección de datos desde el diseño y por defecto), 33 (notificación a la autoridad de control) y 34 (comunicación al interesado) cuando se detectan deficiencias en el diseño del tratamiento y en la notificación.

La regulación de los servicios de la sociedad de la información en virtud de la Directiva sobre privacidad electrónica y la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI) es un segundo vector de exposición administrativa que suele surgir junto con las investigaciones de incidentes o tras ellas. La LSSI prevé sanciones pecuniarias de hasta 600 000 euros para las infracciones muy graves y límites máximos inferiores para las infracciones graves y leves, acompañadas de publicación y, en caso de infracciones muy graves reiteradas, también se puede imponer una prohibición temporal de operar. También se contemplan multas coercitivas diarias para obligar al cumplimiento de las medidas provisionales.

### Leyes y reglamentos específicos y pertinentes en materia de resiliencia cibernética (por ejemplo, NIS, PSTIA y, posiblemente, en un futuro próximo, el proyecto de ley sobre ciberseguridad y resiliencia en Inglaterra y Gales).

La base de referencia actual de España en materia de supervisión de la ciberseguridad es el marco NIS1 establecido por el Real Decreto-ley 12/2018 y desarrollado posteriormente por el Real Decreto 43/2021, que se aplica a los operadores de servicios esenciales y a determinados proveedores de servicios digitales. Impone medidas y obligaciones de notificación de incidentes e incluye una escala de sanciones que alcanza hasta un millón de euros para las infracciones muy graves, con publicación en casos específicos. Las infracciones incluyen la no notificación de incidentes, la no adopción de las medidas de seguridad requeridas, la obstrucción de las auditorías y el suministro de información falsa. En virtud de este marco, los incidentes se notificarán a la CSIRT pertinente a través del proceso en línea centralizado en la Plataforma Nacional de Notificación y Seguimiento de Incidentes Cibernéticos.

España aún no ha completado la transposición de la Directiva NIS2. El Consejo de Ministros aprobó en enero de 2025 un proyecto de ley sobre coordinación y gobernanza de la ciberseguridad para transponer la NIS2, pero hasta la entrada en vigor de la nueva ley sigue siendo aplicable el régimen basado en la NIS1. Una vez transpuesta con éxito, la NIS2 ampliará su ámbito de aplicación y aumentará los límites máximos, de modo que las entidades esenciales se enfrentarán a multas de hasta 10 millones de euros o el 2% de su volumen de negocios mundial, lo que sea mayor, y las entidades importantes, de hasta 7 millones de euros o el 1,4%, lo que sea mayor, junto con la ampliación de las herramientas de supervisión, las instrucciones vinculantes, la divulgación pública y las medidas de responsabilidad de la dirección.

### Leyes y reglamentos específicos del sector (por ejemplo, normas de resiliencia operativa y régimen de terceros críticos que se aplica al sector financiero en Inglaterra y Gales).

Las entidades del sector financiero se enfrentan a una capa adicional en virtud de la Ley de Resiliencia Operativa Digital (DORA), que comenzó a aplicarse en toda la UE desde el 17 de enero de 2025.

DORA establece obligaciones directamente aplicables para la gestión de riesgos de las TIC, la notificación de incidentes graves, las pruebas, la gobernanza y la supervisión de terceros, y crea una supervisión a nivel de la UE para determinados proveedores terceros de TIC críticos.

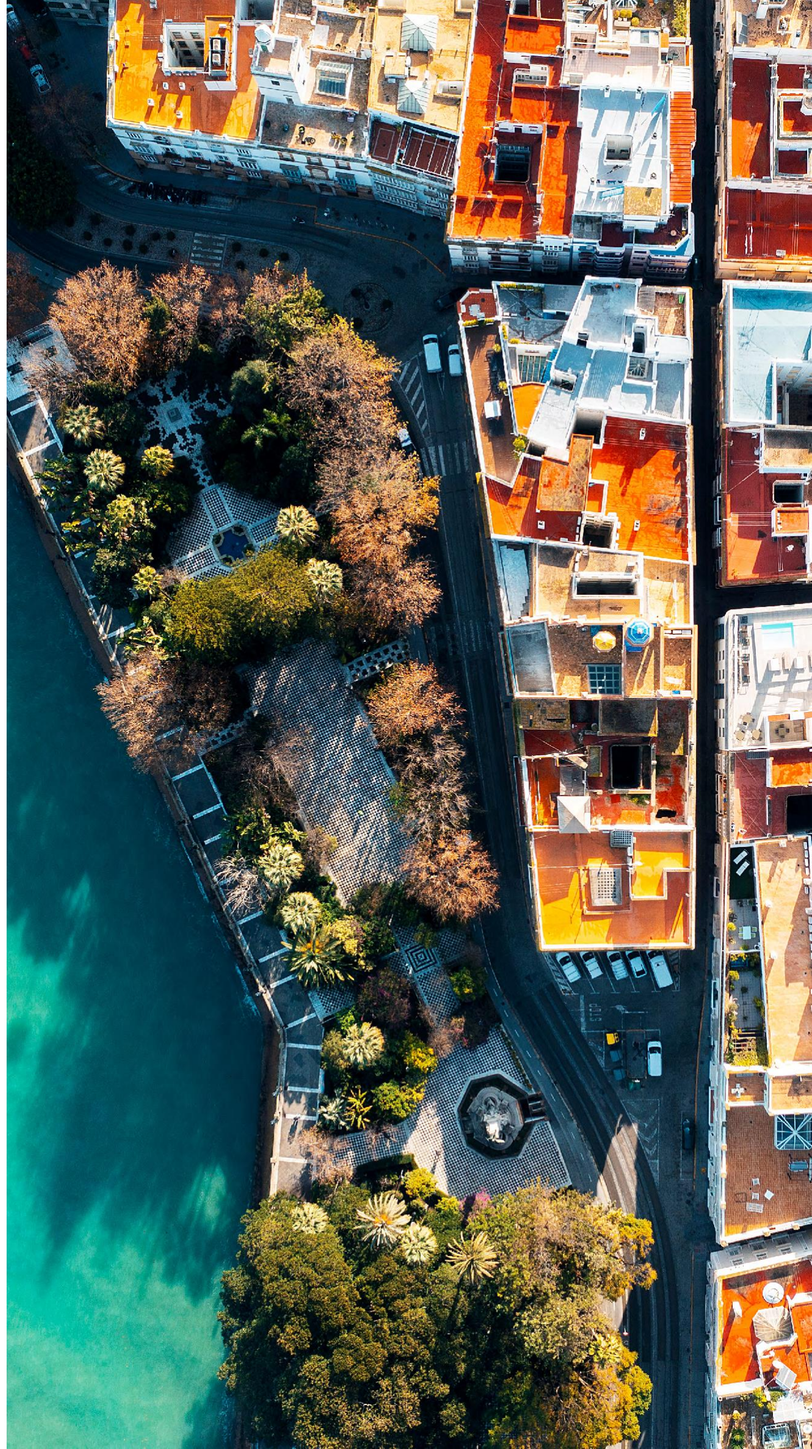
Aunque DORA es directamente aplicable, las sanciones nacionales y la asignación de funciones de supervisión se establecen en la legislación de los Estados miembros. En España, el Consejo de Ministros aprobó en diciembre de 2024 el proyecto de ley sobre la digitalización y modernización del sector financiero (proyecto de ley DORA) para articular el marco sancionador español y designar a las autoridades competentes para la supervisión de DORA. Se prevé que los supervisores sectoriales, entre ellos el Banco de España, la Comisión Nacional del Mercado de Valores (CNMV) y la Dirección General de Seguros y Fondos de Pensiones (DGSFP), estén facultados para imponer tanto multas pecuniarias como medidas no pecuniarias por el incumplimiento de DORA.

En cuanto a las multas, el proyecto de ley DORA apunta a multas de hasta 5 millones de euros o el 5% del volumen de negocios anual para las personas jurídicas, mientras que las personas físicas (es decir, las personas que ocupan puestos directivos) podrán ser multadas con hasta 1 millón de euros o cinco veces el beneficio obtenido. Sin embargo, las escalas específicas de multas españolas por incumplimientos de DORA aún deben confirmarse tras la promulgación definitiva de la ley final.

Las obligaciones específicas del sector en materia de ciberseguridad y seguridad operativa también están presentes en los contextos de las telecomunicaciones y el sector público. Los proveedores de telecomunicaciones están sujetos a obligaciones legales, entre ellas las de seguridad y notificación de incidentes al Ministerio de Economía y Transformación Digital, en virtud de la Ley General de Telecomunicaciones. En el sector público, el Esquema de Seguridad Nacional (ENS) impone unas normas básicas de seguridad técnica y la notificación de incidentes, que se aplican mediante facultades administrativas.

Los sectores de infraestructuras críticas, como la energía, el agua, el transporte y la salud, están sujetos al régimen NIS/NIS2 y, en su caso, a los reguladores sectoriales.

Por último, cabe señalar que, aunque la Directiva sobre la resiliencia de las entidades críticas (CER) impone obligaciones sustanciales de notificación de incidentes, España aún no ha transpuesto la CER a la legislación nacional; y la normativa sobre entidades críticas actualmente aplicable, a saber, la Ley 8/2011 y el Real Decreto, no impone ningún requisito de notificación de incidentes.



2

# ¿Son asegurables las multas cibernéticas?

## Resumen del capítulo

La asegurabilidad de las multas cibernéticas depende en gran medida de la jurisdicción. El panorama se caracteriza por la incertidumbre jurídica y las variaciones significativas.

En todos los mercados, las aseguradoras cubren habitualmente los gastos de defensa, investigación, notificación, relaciones públicas, interrupción de la actividad comercial y restauración, así como las multas civiles, en la medida en que sean asegurables por ley.

En la mayoría de los países de la UE y en el Reino Unido, las multas penales y administrativas con fines punitivos o disuasorios no son asegurables. Esto refleja la preocupación de las políticas públicas por que los seguros no socaven el efecto disuasorio de la aplicación de la normativa. Los pagos por multas que no entran en conflicto con estas preocupaciones y las exclusiones de las pólizas por actos intencionados o de negligencia grave son poco frecuentes y están sujetos a interpretación judicial.

Fuera de la UE, los enfoques varían: Sudáfrica y Arabia Saudí se basan en el derecho consuetudinario y la aprobación reglamentaria, con exclusiones similares para las faltas intencionadas.

En general, es de vital importancia tener en cuenta los matices de la legislación local y la redacción de las políticas, y apreciar los límites de la cobertura para este tipo de exposición.

## Medidas prácticas que las organizaciones deben considerar

- Revisar las pólizas de seguro cibernético para ver si hay exclusiones relacionadas con multas y definiciones de eventos asegurables.
- Considerar otras pólizas de seguro que puedan ofrecer el nivel adecuado de cobertura, como D&O o indemnización profesional.
- Asegurar que el seguro se amplíe para garantizar la cobertura más amplia posible, sin límites territoriales, sino con cobertura mundial.
- Consultar con un asesor legal para aclarar la asegurabilidad en las jurisdicciones pertinentes.
- Formar a los directivos sobre las limitaciones del seguro: asegurar que los ejecutivos comprendan lo que está cubierto y lo que no para evitar suposiciones durante las crisis.
- Cuantificar el perfil de riesgo de la organización, teniendo en cuenta tu sector, industria y exposición al riesgo.
- Preparar un protocolo de reclamaciones para garantizar que se siga el proceso adecuado y se tomen las decisiones correctas en caso de incidente.

## España

La legislación española sobre contratos de seguros y la política de supervisión actúan conjuntamente para que, en la práctica, las sanciones administrativas pecuniarias no sean asegurables. La Ley Española de Contratos de Seguros (SICA) prohíbe la indemnización cuando la pérdida haya sido causada por la mala fe del asegurado (artículo 19 de la SICA) y, en el ramo de gastos de defensa jurídica, excluye expresamente el pago de multas y gastos derivados de sanciones impuestas por autoridades administrativas o judiciales (artículo 76 b) de la SICA). Aunque esta última exclusión es específica del seguro de defensa jurídica, pone de manifiesto la reticencia legislativa a interpretar las sanciones de derecho público como una pérdida asegurable.

Más importante aún, el supervisor de seguros español (DGSFP) ha sostenido durante mucho tiempo que indemnizar las sanciones administrativas o penales es contrario al orden público, en la medida en que socavaría sus funciones punitivas y disuasorias. Esa posición, aunque se estableció en una consulta de 2008, se tradujo finalmente en la forma en que se han diseñado los productos de seguros y en cómo se han configurado las expectativas de supervisión en todas las líneas de negocio.

Los tribunales españoles han confirmado en contextos adyacentes que determinadas responsabilidades similares a sanciones asignadas personalmente por ley son intransferibles y no asegurables.

Aunque no existe ninguna sentencia del Tribunal Supremo que se pronuncie directamente sobre la indemnización por multas del RGPD/NIS/DORA, el efecto combinado de la prohibición legal por mala fe, la exclusión de los gastos legales y la doctrina del orden público del supervisor significa que las multas administrativas impuestas por las autoridades españolas se consideran generalmente no asegurables, independientemente de si la infracción se caracteriza como negligente y no como intencionada.

Tenga en cuenta también la distinción entre (a) contratar una póliza de seguro cibernético que cubra las multas cibernéticas en la medida en que sean asegurables y (b) recibir una indemnización en virtud de dicha póliza. Tomando como ejemplo E&W, ésta es una distinción relevante porque, si bien (a) está permitido, en ciertos casos existen prohibiciones contra la indemnización, así como principios relevantes que pueden invalidar o hacer inaplicables las disposiciones contractuales.

Las pólizas de seguro cibernético españolas suelen incluir cláusulas que pretenden cubrir «las multas y sanciones reglamentarias en la medida en que sean legalmente asegurables», a menudo junto con exclusiones para multas penales y actos deliberados o fraudulentos. Sin embargo, existe una distinción crucial entre la posibilidad de contratar una póliza de este tipo y la posibilidad de ser indemnizado por una sanción concreta.

Si bien es permisible y habitual suscribir una póliza que haga referencia a la cobertura de multas asegurables, la exigibilidad de la indemnización por multas administrativas impuestas por las autoridades españolas dependerá de la naturaleza y el origen de la sanción, la redacción específica de la póliza y, lo que es más importante, la aplicación de los principios de orden público español.

Dada la posición histórica de la DGSFP, junto con las exclusiones legales, es probable que la indemnización por la mayoría de las multas administrativas (como las previstas en el RGPD, la LSSI o la NIS/NIS2) corra el riesgo de ser denegada o anulada por ser contraria al orden público, independientemente de que la póliza incluya una concesión de cobertura.

A modo de ejemplo, en la práctica, las aseguradoras que operan en España suelen cubrir los gastos de defensa jurídica, los gastos de investigación, los gastos de notificación y las medidas de cumplimiento normativo, pero se resisten a indemnizar las multas en sí. Incluso en el caso de que una aseguradora pagara voluntariamente una multa no asegurable, podría acabar siendo objeto de escrutinio por parte de las autoridades supervisoras. Por lo tanto, es importante que los asegurados comprendan que, si bien es posible contratar una póliza con la cláusula «multas asegurables», la probabilidad real de ser indemnizado por sanciones administrativas es escasa.

También sería necesario caracterizar cuidadosamente la responsabilidad, ya que no todas las exposiciones monetarias de derecho público se consideran «multas», aunque el marco jurídico y normativo vigente apunta al hecho de que la carga financiera de las sanciones administrativas punitivas, por regla general, no puede transferirse a las aseguradoras.

# ¿Ha habido alguna multa cibernética reciente destacable?

## Resumen del capítulo

En los últimos años se han dado casos de multas significativas impuestas por incidentes cibernéticos. También hemos visto una mayor firmeza por parte de los reguladores, el uso de sanciones tanto monetarias como no monetarias y la tendencia a dar publicidad a las medidas coercitivas para aumentar su efecto disuasorio. También se ha prestado una atención creciente a la aplicación de la ley en sectores específicos, en particular en los servicios financieros y la asistencia sanitaria.

Las autoridades de protección de datos han impuesto multas de varios millones de euros a grandes empresas tecnológicas, energéticas y financieras por fallos en la seguridad de los datos, la notificación de infracciones y las medidas organizativas.

Muchas de ellas se han iniciado mediante la aplicación del RGPD. Entre los casos más destacados se encuentran la multa de 251 millones de euros impuesta a Meta en Irlanda, la sanción de 79,1 millones de euros impuesta a Enel Energia en Italia, las importantes sanciones impuestas a empresas de energía y telecomunicaciones en España y Francia, y la multa de 14 millones de libras esterlinas impuesta a Capita en el Reino Unido, reducida desde los 45 millones de libras esterlinas iniciales.

Fuera de la UE, el Regulador de la Información de Sudáfrica ha comenzado a imponer multas por el incumplimiento de las obligaciones en materia de protección de datos, mientras que el regulador de telecomunicaciones de Arabia Saudí ha impuesto sanciones sustanciales por fallos en la seguridad de las redes.

Las multas impuestas suelen estar relacionadas con fallos en los controles de acceso, la notificación de infracciones, medidas de seguridad inadecuadas o reincidencias.

El patrón es constante: las autoridades comprueban los controles básicos, la notificación oportuna y completa y la seguridad/diseño por defecto. Se espera que los nuevos marcos normativos, como NIS2, DORA y la Ley de IA, impulsen un aumento tanto de la frecuencia como de la severidad de las multas cibernéticas.

## Medidas prácticas que las organizaciones deben considerar

- Crear un libro de casos de infracciones: recopilar resúmenes de las principales multas y medidas coercitivas que hayan sufrido otras empresas para informar sus evaluaciones de riesgos internas e identificar los incumplimientos de cumplimiento más comunes en el sector.
- Comparar los controles de seguridad de la organización con los citados en los casos de aplicación de la ley.
- Revisar los protocolos de notificación de infracciones: asegurar que se pueden cumplir los plazos de 72 horas del RGPD con alertas automáticas y vías de escalamiento.
- Realizar análisis posteriores a los incidentes: analizar las infracciones internas y los conatos de infracción para identificar las deficiencias en los controles.
- Utilizar estudios de casos como material de formación: incorporar casos reales en los programas de sensibilización del personal.

## España

La aplicación de la normativa en España (basada especialmente en las sanciones impuestas por la AEPD) muestra una clara tendencia a imponer sanciones de gran impacto en virtud del RGPD por incumplimientos en materia de seguridad del tratamiento, confidencialidad y privacidad/seguridad desde el diseño.

En diciembre de 2023, la AEPD impuso multas por un total de 6,1 millones de euros a una empresa energética. La decisión sancionó las infracciones de seguridad del tratamiento y confidencialidad y los incumplimientos de notificación tras la exposición de credenciales y grandes volúmenes de datos de clientes, junto con deficiencias como la ausencia de autenticación multifactorial (MFA), controles de sesión insuficientes y la desactivación tardía de cuentas comprometidas. El caso subraya la expectativa de la AEPD de que la higiene básica de la seguridad y la contención rápida forman parte del cumplimiento del artículo 32.

En febrero y abril de 2024, la AEPD publicó dos decisiones derivadas de un ciberataque perpetrado en marzo de 2022 contra el portal GEA de otro grupo de empresas energéticas y la arquitectura de la base de datos compartida del grupo. La AEPD sancionó a una de las empresas del grupo con 3 millones de euros por infringir el artículo 5, apartado 1, letra f), y el artículo 32 del RGPD, debido a una segregación inadecuada de los datos de las empresas y a medidas preventivas insuficientes. En el caso paralelo, la AEPD sancionó a la otra empresa del grupo con 3,5 millones de euros por infringir la confidencialidad y la seguridad del tratamiento, lo que afectó a aproximadamente 1,35 millones de clientes.

Las dos decisiones juntas ponen de relieve la voluntad de la AEPD de articular las responsabilidades distintas de una empresa matriz del grupo que actúa como encargada del tratamiento y una empresa del grupo que actúa como responsable del tratamiento, de rechazar los argumentos de que una respuesta rápida tras el incidente es suficiente para cumplir el artículo 32, y de tratar los riesgos de separación lógica y arquitectura como obligaciones fundamentales de diseño.

En abril de 2024, la AEPD impuso una sanción de 5 millones de euros a una entidad financiera por un incidente de seguridad en el que los clientes podían ver los detalles de las transferencias realizadas por otros clientes, al considerar que se habían infringido el artículo 5, apartado 1, letra f), el artículo 25 y el artículo 32 del RGPD. La resolución hizo hincapié en las deficiencias de diseño y en la corrección reactiva, en lugar de proactiva. Por otra parte, en 2024 se impusieron sanciones de gran cuantía en los sectores de la energía, las finanzas, las telecomunicaciones y los servicios digitales, incluidas múltiples multas que ascendieron a un total de 5 millones de euros por las infracciones de los principios del RGPD y la responsabilidad de una empresa energética.

En diciembre de 2024, la AEPD impuso una multa de 6,5 millones de euros a una empresa de telecomunicaciones por infringir el principio de integridad y confidencialidad y por no aplicar las medidas de seguridad adecuadas, lo que provocó la filtración y el secuestro de aproximadamente 100 GB de datos personales de hasta tres millones de clientes, antiguos clientes, empleados y proveedores, lo que constituyó una infracción del artículo 5, apartado 1, letra f), y del artículo 32 del RGPD.

En enero de 2025, la AEPD impuso una multa de 4 millones de euros (reducida de 5 millones de euros) a una compañía de seguros por infringir el principio de integridad y confidencialidad, no aplicar medidas de seguridad adecuadas, no aplicar medidas de protección de datos desde el diseño y por defecto, y no llevar a cabo una evaluación de impacto de la protección de datos cuando era necesario, lo que provocó una violación de datos que se produjo en octubre de 2022, en la que se vio comprometida la información confidencial de hasta 1,6 millones de personas, incluidos clientes actuales y antiguos de la empresa. En conjunto, estos factores llevaron a la determinación de que se habían infringido los artículos 5, apartado 1, letra f), 25, 32 y 35 del RGPD.

También en enero de 2025, la AEPD impuso una multa de 3,2 millones de euros a una empresa minorista y de supermercados por no proteger adecuadamente los datos de los clientes después de que unos ataques de «relleno de credenciales» expusieran información sensible de su programa de fidelización. La AEPD consideró que la empresa había infringido el artículo 5, apartado 1, letra f), el artículo 32 y el artículo 34 del RGPD al no aplicar medidas de seguridad suficientes y no notificar adecuadamente a las personas afectadas, lo que dio lugar a la sanción y a la orden de informar a los clientes afectados en el plazo de un mes.

La tendencia es clara: la AEPD está utilizando activamente tanto las obligaciones basadas en principios como las técnicas para sancionar los fallos de seguridad y diseño expuestos por o asociados con incidentes cibernéticos, y está dispuesta a imponer sanciones de alto valor y órdenes correctivas no monetarias en la medida en que sea relevante/apropiado.

# ¿Qué otras sanciones normativas se derivan de los incidentes cibernéticos y son asegurables?

¿Existen otras sanciones reglamentarias a las que puedan enfrentarse las organizaciones como consecuencia de incidentes cibernéticos? ¿Es posible asegurarse contra esas sanciones y sus consecuencias financieras?

## Resumen del Capítulo

Más allá de las multas económicas, las organizaciones se enfrentan ahora a una serie de sanciones reglamentarias adicionales derivadas de los incidentes cibernéticos. Entre ellas se incluyen órdenes correctivas, suspensiones operativas, prohibiciones de gestión, auditorías obligatorias y advertencias públicas.

Los reguladores pueden aplicar una amplia gama de sanciones más allá de las sanciones económicas. Además de las mencionadas anteriormente, también pueden incluir instrucciones vinculantes, órdenes de cese del tratamiento, publicación de decisiones, suspensiones o retiradas de licencias/autorizaciones y multas periódicas por incumplimiento.

Estas sanciones no monetarias pueden tener importantes consecuencias operativas y reputacionales, ya que perturban la continuidad del negocio y dañan la confianza de las partes interesadas.

Si bien no es posible obtener una indemnización directa por sanciones no monetarias como estas, en determinados casos los seguros pueden cubrir las consecuencias financieras, como las pérdidas por interrupción del negocio o los costes de aplicación de medidas correctivas.

Una sólida planificación de la respuesta a incidentes, la claridad contractual con los proveedores de servicios y la colaboración proactiva con los reguladores son factores importantes para mitigar el impacto de las sanciones no monetarias. Las organizaciones deben comprender la interacción entre los diferentes regímenes normativos, ya que la superposición de obligaciones en virtud del RGPD, NIS2, DORA y las leyes sectoriales puede dar lugar a medidas coercitivas acumulativas.

## Medidas prácticas que las organizaciones deben considerar

- Estar preparado para sanciones no monetarias: desarrollar planes para la continuidad del negocio, la defensa legal y la gestión de la reputación en caso de sanciones por parte de los reguladores.
- Ensayar las respuestas a las solicitudes de supervisión, como entregas de documentos, inspecciones in situ o auditorías obligatorias, y asegurar que el manual de estrategias esté listo para activarse.
- Desarrollar un plan de compromiso normativo: estar preparado para auditorías, entrevistas y solicitudes de documentos.
- Incluir el cumplimiento normativo en los contratos: asegurar que los proveedores de servicios y socios estén obligados contractualmente a cumplir las normas de ciberseguridad y a participar en la respuesta a incidentes.

## España

### ¿Existen otras sanciones reglamentarias a las que pueden enfrentarse las organizaciones como consecuencia de incidentes cibernéticos?

En el marco del RGPD/LOPDGDD, la LSSI, la NIS, el próximo marco NIS2 y DORA en el sector financiero, las autoridades despliegan una amplia gama de herramientas no monetarias que pueden aplicarse tras un ciberincidente. Entre ellas se incluyen advertencias y amonestaciones; instrucciones vinculantes; órdenes para que el tratamiento o los sistemas cumplan la normativa en plazos determinados; auditorías obligatorias y revisiones independientes; suspensiones temporales o definitivas del tratamiento o de las autorizaciones; órdenes de notificación a las autoridades y a las personas afectadas; publicación de decisiones; y, en virtud de la NIS2, en casos graves, prohibiciones temporales de gestión para los directores de entidades esenciales.

En determinadas situaciones, también se contemplan sanciones coercitivas diarias para obligar al cumplimiento. Estas sanciones no financieras están diseñadas para garantizar el cumplimiento y remediar los riesgos, y pueden tener importantes consecuencias operativas y reputacionales para las organizaciones afectadas. Por ejemplo, la suspensión de una autorización para prestar servicios, las órdenes de cesar las conductas no conformes o la divulgación pública de los incidentes pueden perturbar las operaciones comerciales y dañar la reputación de una organización ante sus clientes y socios.

### ¿Es posible asegurarse contra esas sanciones y sus consecuencias financieras?

Las sanciones no económicas derivadas de incidentes cibernéticos, como órdenes de cesar el tratamiento, prohibiciones de gestión o suspensiones, no pueden «asegurarse» en el sentido de transferir la obligación de cumplirlas o evitarlas (véase la pregunta 2 anterior). El seguro no puede impedir que un regulador emita tales órdenes ni neutralizar su efecto. Sin embargo, las consecuencias económicas asociadas a la respuesta a los procedimientos regulatorios pueden asegurarse, en particular aquellas que implican la suspensión de la actividad o la inhabilitación para ejercer actividades profesionales, en la medida en que puedan calificarse como «otras pérdidas pecuniarias», tal y como se describe en la normativa sobre seguros y respaldado por la jurisprudencia española.

En la práctica, las pólizas de seguro cibernético en España suelen cubrir los costes de investigación de un incidente; los costes de defensa jurídica; las reclamaciones de terceros (clientes/proveedores/interesados) derivadas de una infracción; y los costes de mitigación de la infracción, como, por ejemplo, los gastos de relaciones públicas/comunicación.

# ¿Están los incidentes cibernéticos provocando demandas colectivas por violación de datos?

## Resumen del Capítulo

Las demandas colectivas y los mecanismos de reparación colectiva por violaciones de datos e incidentes cibernéticos están aumentando.

La aplicación de la Directiva de la UE sobre acciones representativas está impulsando un mayor interés por los litigios colectivos, especialmente en los sectores orientados al consumidor.

Las demandas colectivas pueden amplificar el impacto financiero y reputacional de los incidentes cibernéticos, especialmente cuando se combinan con la aplicación de la normativa. Es importante contar con una notificación temprana, una comunicación transparente y estrategias legales y de seguros integrales para gestionar los riesgos que presentan las demandas colectivas.

Jurisdicciones como Portugal, los Países Bajos, Francia e Irlanda cuentan con regímenes de demandas colectivas activos o emergentes, con casos recientes dirigidos a empresas tecnológicas, plataformas de redes sociales y proveedores de atención sanitaria. En Inglaterra y Gales, las demandas siguen presentándose de forma voluntaria, al no existir un procedimiento de exclusión voluntaria.

Los mecanismos procesales varían —opt-in frente a opt-out y los requisitos para las entidades cualificadas—, pero la tendencia es hacia una mayor accesibilidad y coordinación para las personas afectadas.

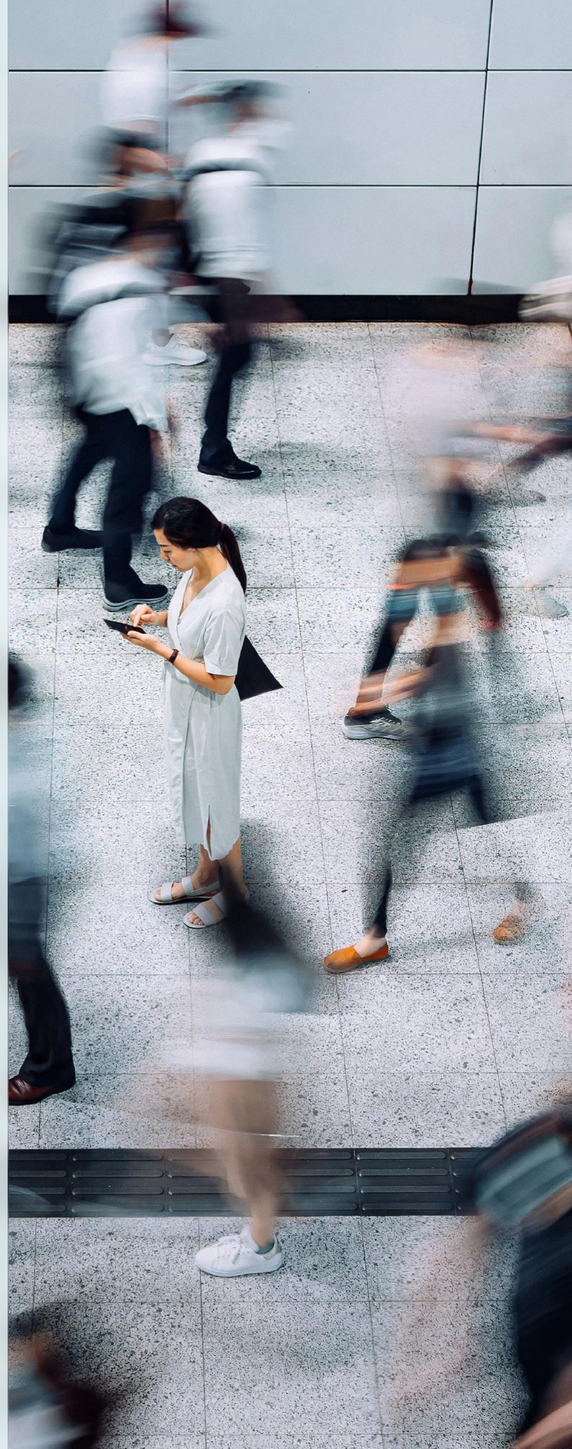
Fuera de la UE, e Inglaterra y Gales, las demandas colectivas son menos comunes, y algunos países carecen de un mecanismo formal de reparación colectiva.

Las reclamaciones típicas se centran en daños inmateriales por angustia y daños a la privacidad, con indemnizaciones per cápita bajas o modestas, pero con altos costes agregados y de defensa, especialmente cuando son las organizaciones de consumidores las que organizan los litigios.

En términos de exposición global, están aumentando los litigios colectivos en Estados Unidos contra empresas europeas. En los casos más recientes, las aseguradoras han proporcionado cobertura, ya que no existían restricciones territoriales o estadounidenses en la redacción de la póliza.

## Medidas prácticas que las organizaciones deben considerar

- Supervisar las tendencias en materia de litigios: suscribirse a alertas legales y realizar un seguimiento de los casos de demandas colectivas y las novedades en el sector.
- Evaluar la exposición a demandas colectivas: evaluar los volúmenes de datos, el historial de infracciones y el alcance de las operaciones orientadas al consumidor.
- Reforzar los procesos de protección de datos y notificación de infracciones para minimizar la posibilidad de que se produzcan demandas colectivas.
- Incluir el riesgo de litigios en los informes de la junta directiva: asegurar que los directores sean conscientes de la exposición potencial y de los planes de mitigación.
- Tener en cuenta la exposición en EE. UU.



## España

El artículo 80 del RGPD permite a los Estados miembros facultar a las asociaciones de consumidores para que emprendan acciones contra las violaciones de los derechos establecidos en el mismo y no exige que dichas asociaciones se constituyan específicamente con el fin de actuar en el ámbito de la protección de datos.

En España, la LOPDGDD no contiene ninguna disposición al respecto.

No obstante, España reconoce un mecanismo de reparación colectiva anclado en el artículo 11 de la Ley de Enjuiciamiento Civil, que permite a las asociaciones de consumidores interponer acciones y solicitar la protección de los intereses colectivos, incluyendo la publicación de un aviso público para que las personas afectadas puedan sumarse a la acción. El modelo que prevalece actualmente se considera de adhesión voluntaria, y España ha experimentado históricamente menos acciones colectivas por daños y perjuicios a gran escala por violaciones de datos en comparación con otros países de la UE.

Si bien ha habido reclamaciones individuales y colectivas, y las asociaciones de consumidores han estado activas en el ámbito de la protección de datos, la ausencia de un mecanismo de exclusión voluntaria ha moderado hasta la fecha la magnitud de los litigios por daños masivos relacionados con la ciberseguridad.

Sin embargo, ese panorama está cambiando ahora como consecuencia de la transposición de la Directiva sobre acciones representativas de la UE.

En febrero de 2025, el Consejo de Ministros aprobó un proyecto de ley para introducir un procedimiento específico de acciones colectivas en la Ley de Enjuiciamiento Civil. El proyecto prevé un mecanismo de exclusión voluntaria para las acciones de reparación por debajo de determinados umbrales por beneficiario, la publicación de anuncios públicos a través de una plataforma electrónica, la posibilidad de que las entidades cualificadas y el Ministerio Fiscal interpongan acciones y el nombramiento de un liquidador para distribuir la indemnización a tanto alzado.

Una vez promulgado, se espera que el nuevo régimen aumente considerablemente el riesgo de litigios por violaciones de datos a gran escala, especialmente en sectores como las telecomunicaciones y los servicios financieros, donde las reclamaciones colectivas ya son más frecuentes.

# ¿Qué otras disputas posteriores al incidente se están observando?

## Resumen del Capítulo

Los incidentes cibernéticos pueden desencadenar una amplia gama de disputas legales, lo que obliga a las organizaciones a adoptar un enfoque holístico de la gestión de riesgos, la gobernanza contractual y la participación de las partes interesadas.

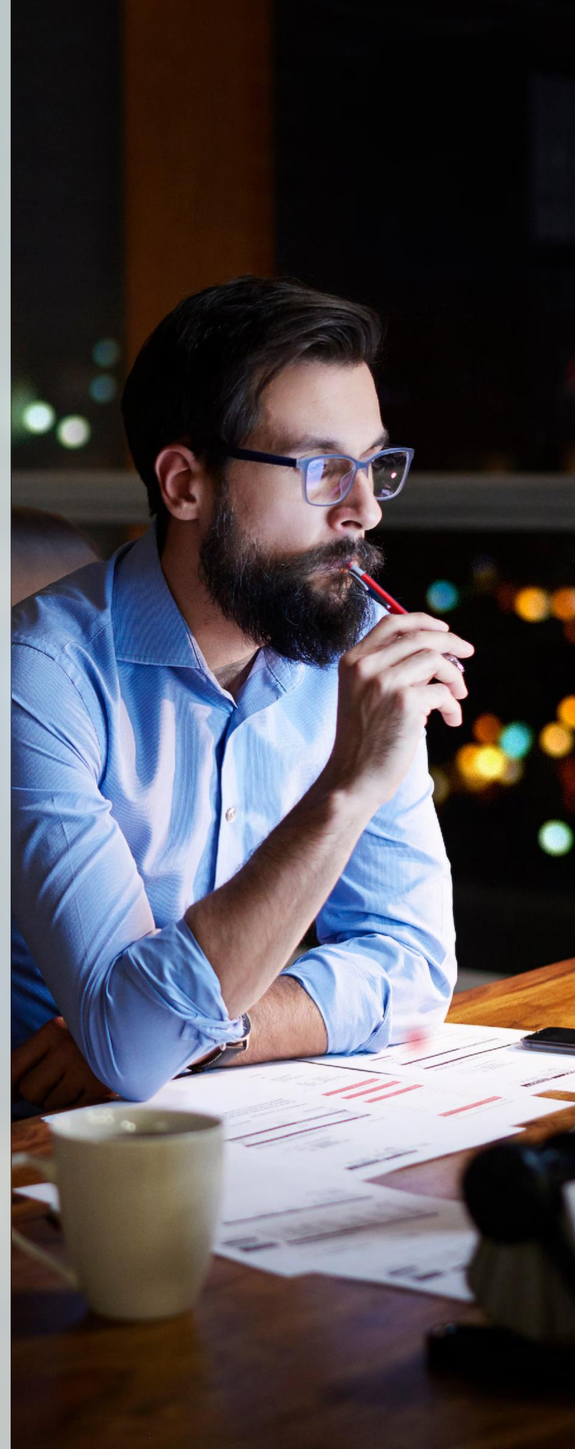
Cada vez se recurre más al arbitraje y a la resolución alternativa de disputas para resolver los conflictos posteriores a los incidentes, y cada vez es más importante incluir cláusulas contractuales claras en los contratos y aplicar una sólida diligencia debida en la gestión de los riesgos de terceros.

Entre los ejemplos de este tipo de litigios se incluyen las disputas contractuales entre las organizaciones y sus proveedores de servicios, en particular en lo que respecta a la adecuación de las medidas de ciberseguridad, la respuesta a incidentes y las obligaciones de indemnización. Existe la posibilidad de que se produzcan litigios sobre investigaciones reglamentarias, la proporcionalidad de las sanciones y la adecuación de las medidas técnicas y organizativas.

También pueden surgir disputas sobre la clasificación de las entidades en los marcos normativos, la asignación de responsabilidades en las cadenas de suministro y la aplicación de disposiciones contractuales, como las cláusulas de fuerza mayor.

## Medidas prácticas que las organizaciones deben considerar

- Revisar los contratos y los acuerdos de nivel de servicio (SLA) en busca de cláusulas relacionadas con la asignación clara de las obligaciones en materia de riesgos cibernéticos y respuesta ante incidentes.
- Asegurarse de que las disposiciones sobre fuerza mayor e indemnización aborden los incidentes cibernéticos.
- Negociar niveles de servicio y soluciones claros: especificar las obligaciones y responsabilidades que deben cumplir los proveedores y socios, así como las normas mínimas de seguridad y los seguros.
- Realizar evaluaciones periódicas de los riesgos de la cadena de suministro: evaluar la resiliencia de los proveedores y su capacidad de respuesta ante incidentes.



## España

Las reclamaciones típicas se centran en daños inmateriales por angustia e invasión de la privacidad, con indemnizaciones per cápita bajas o modestas, pero con elevados costes agregados y de defensa, especialmente cuando son las organizaciones de consumidores las que organizan el litigio.

En términos de exposición global, las demandas colectivas en Estados Unidos contra empresas europeas están aumentando. En los casos más recientes, las aseguradoras han proporcionado cobertura, ya que no existían restricciones territoriales o estadounidenses en la redacción de la póliza.

7

# En virtud de la Ley de IA de la UE

¿Cuáles son las obligaciones aplicables en materia de ciberseguridad? ¿Cuáles son las posibles consecuencias (es decir, multas y sanciones) derivadas de una violación de la seguridad que afecte a un sistema de IA de alto riesgo, incluso cuando la violación de la seguridad implique la pérdida de datos personales?

## Resumen del Capítulo

La Ley de IA de la UE impone requisitos estrictos de ciberseguridad a los proveedores y usuarios de sistemas de IA de alto riesgo. La ley exige medidas cibernéticas sólidas durante todo el ciclo de vida, incluyendo la gestión de riesgos, la resiliencia técnica, la detección y notificación de incidentes y la supervisión humana.

Los proveedores deben realizar evaluaciones de riesgos de ciberseguridad, mantener documentación técnica detallada y garantizar que los sistemas sean resistentes a ataques como el envenenamiento de datos y la evasión de modelos. El incumplimiento puede dar lugar a multas administrativas sustanciales, de hasta 35 millones de euros o el 7 % de la facturación global por prácticas prohibidas, y de hasta 15 millones de euros o el 3 % por incumplimientos de los requisitos de los sistemas de alto riesgo.

Cuando una violación de la seguridad afecta a datos personales, la aplicación paralela del RGPD puede dar lugar a sanciones acumulativas.

Las organizaciones deben integrar la ciberseguridad en el diseño y el funcionamiento de los sistemas de IA, mantener una supervisión y un cumplimiento continuos y prepararse para la aplicación de múltiples

regímenes. También deben ser conscientes de los riesgos operativos y para la reputación asociados a los incidentes cibernéticos relacionados con la IA y de la importancia de una gobernanza proactiva y una colaboración interfuncional.

## Medidas prácticas que las organizaciones deben considerar

- Realizar evaluaciones de riesgos de IA: documentar las medidas de ciberseguridad y estrategias de mitigación y actualizarlas periódicamente.
- Implementar la seguridad desde el diseño y por defecto: asegurar que todos los sistemas de IA sean resistentes a los ataques y las violaciones de datos, y que el personal esté capacitado en los riesgos de ciberseguridad específicos de la IA y los requisitos de cumplimiento.
- Mantener una documentación técnica completa y registros de eventos: facilitar la revisión normativa y la investigación de incidentes y garantizar la notificación inmediata de incidentes graves a las autoridades.
- Estar preparado para el cumplimiento de múltiples regímenes: los sistemas de IA pueden estar sujetos a requisitos superpuestos en virtud de la Ley de IA de la UE, RGPD, NIS2 y las leyes sectoriales.

## España

### ¿Qué obligaciones existen en materia de ciberseguridad?

El Reglamento (UE) 2024/1689 (Ley de IA de la UE) entró en vigor el 1 de agosto de 2024, con una aplicación por etapas.

La mayoría de las obligaciones para los sistemas de IA de alto riesgo entrarán en vigor el 2 de agosto de 2026 o el 2 de agosto de 2027, dependiendo de si el sistema se incorpora a productos regulados.

De acuerdo con el artículo 15 de la Ley de IA de la UE, los sistemas de IA de alto riesgo deben diseñarse y desarrollarse para alcanzar un nivel adecuado de solidez, precisión y ciberseguridad para su finalidad prevista y ser resistentes a los intentos de manipulación del sistema o de sus datos. Los proveedores deben realizar una evaluación de riesgos antes de comercializar el sistema o ponerlo en servicio y documentar los resultados de dicha evaluación, que incluirá una identificación de los riesgos potenciales que plantea el sistema de IA y las medidas adoptadas para prevenir o mitigar dichos riesgos.

Además, los proveedores deberán aplicar medidas de gestión de riesgos y gobernanza de datos a lo largo de todo el ciclo de vida, mantener actualizados la documentación técnica y los registros para demostrar el cumplimiento y permitir la supervisión posterior a la comercialización, garantizar la transparencia para los implementadores y una supervisión humana eficaz, y supervisar el rendimiento tras la implementación, notificando sin demora a las autoridades de vigilancia del mercado los incidentes graves o los fallos de funcionamiento. Los implementadores deben supervisar el funcionamiento, garantizar la idoneidad de los datos introducidos, proporcionar supervisión humana, informar a los trabajadores y usuarios afectados y cooperar con los reguladores.

## ¿Qué sanciones reglamentarias podrían derivarse de una infracción de alto riesgo del sistema?

Una violación de la seguridad que comprometa la solidez o la ciberseguridad de un sistema de IA de alto riesgo puede dar lugar a la aplicación de la Ley de IA, en paralelo con el RGPD y los regímenes sectoriales. La Ley de IA establece niveles de multas significativos. El incumplimiento de las prohibiciones se castiga con una multa de hasta 35 millones de euros o el 7% de la facturación anual mundial, lo que sea mayor.

El incumplimiento de las obligaciones de los proveedores, instaladores, importadores, distribuidores y organismos notificados, incluidas las relativas a la solidez/ciberseguridad, el registro, la supervisión y la notificación de incidentes, se castiga con una multa de hasta 15 millones de euros o el 3%, lo que sea mayor.

El incumplimiento de las obligaciones de los proveedores, implementadores, importadores, distribuidores y organismos notificados, incluidas las relativas a la solidez/ciberseguridad, el registro, la supervisión y la notificación de incidentes, se castiga con una multa de hasta 15 millones de euros o el 3%, lo que sea mayor. El suministro de información incorrecta, incompleta o engañosa a las autoridades se castiga con una multa de hasta 7,5 millones de euros o el 1%, lo que sea mayor.

Las pequeñas y medianas empresas se benefician de ajustes proporcionados. Las autoridades nacionales de vigilancia del mercado imponen sanciones a los operadores; la Oficina de IA de la UE supervisa las obligaciones de los modelos de uso general. Cuando una violación de la seguridad relacionada con la IA afecta a datos personales, se aplica paralelamente la notificación del RGPD a la AEPD y, si es necesario, a los interesados, y un solo incidente puede dar lugar a órdenes correctivas acumulativas y a marcos de sanciones administrativas separados en virtud de ambos instrumentos. Las entidades incluidas en el ámbito de aplicación de la NIS2 se enfrentan a obligaciones y sanciones en materia de gestión de riesgos y notificación de incidentes; las entidades financieras se enfrentan a la supervisión de DORA.

La exposición agregada se convierte en multirregimen y la planificación de la respuesta a incidentes debe anticipar los plazos y los requisitos de contenido de las distintas regulaciones.

# 8 Recomendaciones Generales



## Gobernanza

Establecer una responsabilidad clara en materia de gestión de riesgos cibernéticos a nivel del consejo de administración y la alta dirección.

## Cumplimiento

Mantenerse al día con los marcos normativos en constante evolución en todas las jurisdicciones en las que se opera.

## Respuesta ante incidentes

Desarrollar y probar planes de respuesta ante incidentes, incluyendo la notificación de infracciones y el cumplimiento normativo.

## Training

Formar periódicamente al personal en materia de ciberseguridad, protección de datos y requisitos normativos...

## Seguro

Trabajar con corredores y asesores legales para optimizar la cobertura del seguro cibernético, centrándose en los costes asegurables.

## Gestión de proveedores

Evaluar y supervisar los riesgos de terceros, asegurándose de que los contratos aborden las responsabilidades en caso de incidentes cibernéticos.

## Documentación

Mantener registros detallados de las actividades de cumplimiento, las evaluaciones de riesgos y las respuestas a incidentes.

## About Aon

Aon plc (NYSE: AON) exists to shape decisions for the better — to protect and enrich the lives of people around the world. Through actionable analytic insight, globally integrated Risk Capital and Human Capital expertise, and locally relevant solutions, our colleagues provide clients in over 120 countries with the clarity and confidence to make better risk and people decisions that help protect and grow their businesses.

Follow Aon on LinkedIn, X, Facebook and Instagram.
Stay up-to-date by visiting Aon's newsroom and sign up for news alerts here.

aon.com