Síguenos en

JORNADA IA Y CIBERSEGURIDAD

Las nuevas exigencias europeas de ciberseguridad elevan las sanciones hasta el 7% de la facturación

El Reglamento de IA contempla multas de hasta 35 millones de euros o el 7% de la facturación mundial para las infracciones más graves, mientras que NIS2 introduce responsabilidades para los órganos de dirección

El uso de herramientas de IA fuera del control corporativo y la creciente autonomía de estos sistemas obligan a las empresas a reforzar sus mecanismos de supervisión

Grant Thornton y la Cámara de Madrid analizan las nuevas obligaciones empresariales ante los riesgos digitales y la necesidad de acreditar una respuesta diligente frente a los ciberataques



Madrid, miércoles 18 de noviembre de 2026

La nueva regulación europea sobre inteligencia artificial y ciberseguridad está ampliando las obligaciones de las empresas y el alcance de las responsabilidades de sus órganos de dirección. Los distintos marcos normativos contemplan sanciones que, e**n los supuestos más graves del Reglamento de IA, pueden alcanzar los 35 millones de euros o el 7 % de la facturación mundial anual**. A estas exigencias se suma la necesidad de acreditar qué riesgos habían identificado las organizaciones, qué medidas adoptaron para reducirlos y cómo respondieron ante un posible incidente.

Estas han sido algunas de las principales cuestiones abordadas en la jornada **«IA y ciberseguridad: nuevas reglas, nuevas responsabilidades»,** organizada por **Grant Thornton** y **Cámara de Madrid**. El encuentro ha contado con la participación de **Cristina Muñoz-Aycuens**, socia de Ciberseguridad y Forensic de Grant Thornton, y **Eloi Font**, socio de Legal y Derecho Digital de la Firma, con la apertura institucional de **Elena Hernández**, gerente de Club Cámara de Madrid.

La sesión ha abordado las implicaciones del **Reglamento Europeo de Inteligencia Artificial (RIA), la Directiva NIS2 y el Reglamento de Ciberresiliencia**, con especial atención a cómo trasladar estas exigencias a la gestión diaria de las compañías y qué responsabilidades corresponden a sus órganos de dirección.

La necesidad de reforzar estas capacidades queda reflejada en el informe *Cómo mejorar la gestión del riesgo digital*, publicado recientemente por Grant Thornton. Según el estudio, **el 70 % de las empresas españolas encuestadas** no están satisfechas con su capacidad para detectar y gestionar ciberataque**s**, mientras que **el 39 % de los directivos señala que sus empleados no tienen claro de qué riesgos son responsables**.

Identificar el uso de la IA para poder supervisar sus riesgos

La expansión de la inteligencia artificial está añadiendo nuevas capas de complejidad a la gestión empresarial. Su utilización no se limita a las herramientas que las compañías autorizan o **ponen a disposición de sus trabajadores**. También está presente en **aplicaciones corporativas**, como los

sistemas de gestión de clientes, recursos humanos o marketing, y en **soluciones de proveedores** que incorporan modelos de IA.

A ello se suma el fenómeno conocido como ***Shadow AI***: el uso individual de herramientas de inteligencia artificial por parte de los empleados al margen de los mecanismos de supervisión de la empresa. Esta práctica puede exponer información confidencial y generar riesgos que la organización desconoce, especialmente cuando se introducen datos sensibles en plataformas externas sin evaluar previamente sus condiciones de uso y seguridad..

Cristina Muñoz-Aycuens ha señalado que "el primer riesgo que tenemos es no saber dónde se está utilizando la inteligencia artificial en nuestra organización y, sobre todo, para qué y con qué información". En este sentido, ha destacado la importancia de elaborar inventarios que incluyan tanto las herramientas empleadas como sus casos de uso, los datos tratados y el grado de autonomía de cada sistema.

Esta supervisión adquiere especial relevancia con el desarrollo de la denominada **IA agéntica, capaz de ejecutar acciones de forma autónoma**. A medida que estos sistemas pasan de generar recomendaciones a intervenir directamente en procesos empresariales, aumentan las exigencias sobre los permisos de acceso, la trazabilidad de sus actuaciones y los mecanismos de control. La intensidad de estas medidas debe ajustarse a la autonomía de la herramienta, la sensibilidad de la información y el impacto de sus decisiones.

Desde el punto de vista jurídico, el Reglamento Europeo de Inteligencia Artificial establece un sistema de obligaciones proporcional al nivel de riesgo de cada aplicación. **Los sistemas considerados de alto riesgo**, entre los que se encuentran determinados usos relacionados con la selección de personal, la evaluación de trabajadores o el acceso a servicios esenciales, **están sujetos a requisitos específicos de gestión de riesgos, transparencia, supervisión humana y seguridad.**

En este contexto, Eloi Font ha subrayado la necesidad de que las empresas identifiquen los sistemas que utilizan y determinen las obligaciones que les corresponden. **"Lo primero es saber qué inteligencia artificial se está utilizando. Una vez lo sabemos, hay que regularlo internamente, determinar**

cuál es el papel de la empresa y el nivel de riesgo del sistema e implementar los controles correspondientes", ha explicado.

Ambos expertos han coincidido en la importancia de integrar estas medidas en la gestión empresarial mediante protocolos internos, formación de los empleados y una asignación clara de responsabilidades.

Responder a un ciberataque sin perder las evidencias

Cuando se produce un ciberataque, la presión por recuperar la actividad obliga a tomar decisiones con rapidez. Sin embargo, **actuar de forma precipitada puede comprometer la investigación del incidente** o incluso facilitar que la amenaza vuelva a introducirse en los sistemas.

Decisiones como aislar los equipos afectados, apagar determinados sistemas o restaurar copias de seguridad deben valorar sus posibles consecuencias. Algunas actuaciones pueden provocar la pérdida de información necesaria para investigar lo sucedido, mientras que una recuperación prematura puede reintroducir al atacante si no se ha determinado previamente el alcance de la amenaza.

Por ello, **la respuesta exige coordinar tres líneas de actuación simultáneas:** contener el ataque, investigar su origen y alcance, y recuperar la actividad de manera segura. Esta gestión requiere la participación de los equipos técnicos y de las áreas jurídica, de privacidad, comunicación y dirección, con responsabilidades definidas antes de que se produzca el incidente.

En este sentido, Cristina Muñoz-Aycuens ha advertido de que **"recuperar más rápido no quiere decir que lo hayamos hecho bien y que estemos seguros"**, y ha insistido en la necesidad de preservar las pruebas y comprobar que los sistemas restaurados están libres de amenazas.

La preparación previa resulta determinante. Contar con análisis de riesgos actualizados, copias de seguridad protegidas y probadas, registros de actividad suficientes y planes de respuesta ensayados permite reducir el impacto de los ataques. Durante su intervención, Muñoz-Aycuens ha advertido de que muchas organizaciones disponen de planes de respuesta que nunca han probado, lo que dificulta su aplicación efectiva cuando se produce una crisis.

A estas exigencias se suman las obligaciones de notificación previstas en los distintos marcos regulatorios, que pueden requerir comunicaciones iniciales en plazos reducidos, incluso cuando la investigación continúa abierta. Documentar las actuaciones y conservar las evidencias permite reconstruir lo sucedido y acreditar cómo se gestionó el incidente.

Sanciones millonarias y mayor responsabilidad de los órganos de dirección

El nuevo marco regulatorio europeo establece obligaciones diferenciadas para las empresas según su actividad y los riesgos asociados a sus sistemas y productos digitales. **Su incumplimiento puede dar lugar a sanciones económicas elevadas**, cuya cuantía y aplicación dependen de la normativa y de la gravedad de la infracción.

En el caso del Reglamento de Inteligencia Artificial, **las infracciones más graves pueden sancionarse con multas de hasta 35 millones de euros o el 7 % del volumen de negocio mundial anual**, según corresponda. La regulación también contempla obligaciones específicas para los sistemas de alto riesgo y requisitos de transparencia, con distintos niveles de sanción.

Por su parte, **la Directiva NIS2 amplía de siete a dieciocho los sectores comprendidos en el marco europeo de ciberseguridad** e introduce mayores exigencias de gestión de riesgos, protección de la cadena de suministro y comunicación de incidentes. Para determinadas infracciones de las entidades esenciales, contempla **multas de hasta 10 millones de euros o el 2 % de la facturación mundial anual**. Entre sus principales novedades figura **la responsabilidad de los órganos de dirección** de las entidades incluidas en su ámbito de aplicación respecto a la aprobación y supervisión de las medidas de ciberseguridad. En España, su transposición al ordenamiento jurídico nacional continúa pendiente.

Eloi Font ha destacado que este cambio supone una evolución importante en la gestión empresarial de la ciberseguridad. “Hasta ahora, todo quedaba en la mesa del director o del departamento de IT. Ahora el legislador quiere que esto sea una responsabilidad de la empresa y que haya una responsabilidad personal de los directivos”, ha señalado, aunque ha recordado que será necesario concretar su alcance en la normativa española.

El Reglamento de Ciberresiliencia, por su parte, establece requisitos de seguridad para los productos con elementos digitales, incluidos determinados equipos, dispositivos conectados y programas informáticos. Sus obligaciones afectan principalmente a fabricantes, importadores y distribuidores, que deben garantizar la seguridad de los productos a lo largo de su ciclo de vida y gestionar las vulnerabilidades detectadas. **Las infracciones más graves pueden sancionarse con hasta 15 millones de euros o el 2,5 % de la facturación mundial anual**. Las principales exigencias serán aplicables a partir de diciembre de 2027, aunque determinadas obligaciones de notificación ya están vigentes.

Ante este escenario, Font ha insistido en que **la adaptación de las compañías debe ir más allá de la elaboración de políticas y procedimientos**. Las empresas necesitan comprobar periódicamente que las medidas implantadas funcionan y responden a los riesgos reales de su actividad.

La jornada ha puesto de manifiesto que la preparación ante los riesgos digitales exige integrar la ciberseguridad y la supervisión de la inteligencia artificial en los procesos habituales de decisión empresarial. **La resiliencia depende de la capacidad de las organizaciones para anticipar amenazas, responder a los incidentes y mantener la continuidad de su actividad**, con medidas cuya eficacia pueda comprobarse y decisiones que permitan demostrar su diligencia.

Síguenos en

Sobre Grant Thornton

En Grant Thornton España ayudamos a que tu empresa vaya más allá. Servicios profesionales de Auditoría & Assurance, Advisory, Tax, Asesoramiento Financiero, Legal, Laboral y Outsourcing. 12 oficinas y 900 profesionales en nuestro país. Pertenecemos a Grant Thornton Advisors, una plataforma multinacional y multidisciplinar que proporciona una experiencia de cliente única y transfronteriza, con soluciones y capacidades potenciadas por la última tecnología y los mejores equipos. A su vez, formamos parte de Grant Thornton International, una de las redes globales de servicios profesionales líderes, con 80.000 profesionales presente en más de 150 mercados en todo el mundo.

Para ampliar información o hablar con profesionales de Grant Thornton, no dudes en llamarnos:

DEPARTAMENTO COMUNICACIÓN GRANT THORNTON

POLICARPO AROCA
Director de Comunicación, Marketing y Desarrollo de Negocio
T 91 576 39 99
M 650 71 31 21
policarpo.aroca@es.gt.com

JOSÉ MARÍA GÓMEZ VALLEJO
Supervisor de Comunicación Corporativa
T 91 576 39 99
M 681 15 65 13
josemaria.gomez@es.gt.com

MARTA CARDENAL
Técnica de Comunicación Corporativa
T 932 06 39 00
M 608 99 02 14
marta.cardenal@es.gt.com

LEAD BY THOUGHT

GABRIELE CAGLIANI
+34 669 496 103
gabriele@leadbythought.com

MARÍA CUESTA
+34 646 494 090
maria.cuesta@leadbythought.com

GUILLERMO GINÉS
+34 637 916 561
guillermo.gines@leadbythought.com