Instituto de Auditores Internos de España

www.auditoresinternos.es

NÚMERO 139 | Julio | AÑO 2025

AI Auditoría Interna

REVISTA EDITADA POR EL INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

La encrucijada de la geopolítica y la ciberseguridad

La nueva Guerra Fría ya está aquí

Entrevistamos a:

Antonio Garamendi

Presidente de CEOE.

Retos y realidades de riesgos emergentes

Trump hackea el sistema internacional

II Premios IAI España

Premios IAI 25

Premios a la confianza en el valor de la Auditoría Interna

Sumario

Instituto de Auditores Internos de España

Presidenta:
Sonsoles Rubio

Comisión Editorial:
Gabriela González-Valdés: directora general
Jesús Lafita:director de Contenido Técnico

Coordinadora Editorial:
María Cano: directora de Marketing y Comunicación
Rocío Barrie Aladrén: coordinadora de Marketing y Comunicación

Colaboradores:
Enrique Sueiro
Miguel Ángel Serrano
Raúl Chaudon Segura
Ekaterina Nikolaeva
Alfonso Medina Cotes
Ignacio Bazarra
Javier Sánchez-Rico
Federico Steinberg
Pablo Martín-Alonso
Yago Casal
Encarnación Jurado Cano

Santa Cruz de Marcenado, 33 - 28015 Madrid
Teléfono: 91 593 23 45

iai@iai.es
www.auditoresinternos.es

Diseño y realización:
Blondas de Papel S.L.

La geopolítica marca la agenda de la ciberseguridad

Sonsoles Rubio
CIA, CRMA, CFE, LPEC
Presidenta del Instituto de Auditores Internos de España

En un mundo cada vez más conectado, interdependiente y volátil, la frontera entre la geopolítica y la ciberseguridad se difumina cada vez más y, a menudo, es indistinguible.

Los conflictos internacionales, las tensiones políticas y las alianzas estratégicas se trasladan al ámbito digital, intensificando la exposición a posibles ciberataques dirigidos a organizaciones, gobiernos y empresas. Un panorama que cambia constantemente y que obliga a adaptarse a nuevos escenarios.

Esto significa que las amenazas de ciberseguridad no solo son técnicas, sino también políticas y estratégicas, e implica estar siempre alerta, entender el contexto global y asegurar que los sistemas de control interno sean robustos y adaptados a estos desafíos. Y, todo ello, en un entorno regulatorio cada vez más exigente. Es el caso de la Directiva NIS2, DORA o el Reglamento Europeo de Inteligencia Artificial (RIA).

En nuestro informe Risk in Focus 2025, la ciberseguridad y la seguridad de los datos se mantienen como el riesgo prioritario para las organizaciones y se prevé que siga así a tres años vista. Si se quiere llegar a ser resiliente en este sentido, la función de Auditoría Interna juega un papel crucial.

Para ello, es realmente importante que la función de Auditoría Interna se asegure de contar con los recursos, las competencias profesionales y tecnológicas necesarias para abordar los riesgos de ciberseguridad. En este contexto, tiene sentido que el primer requisito temático publicado por el IIA Global en el marco de la actualización del Marco Internacional para la Práctica Profesional (MIPP) haya sido precisamente el relativo a la Ciberseguridad.

Este nuevo elemento del MIPP proporciona un enfoque coherente y exhaustivo para evaluar el diseño y la aplicación de los procesos de gobierno, gestión de riesgos y los procesos de control de la ciberseguridad. Y con ello, mejorar la protección de la información y los sistemas frente a accesos o usos no autorizados, con el fin de proporcionar confidencialidad, integridad y disponibilidad de dicha información.

Para ello, debemos tener visión estratégica, conocer lo que está pasando, ser ágiles, proactivos y ser capaces de trabajar con una visión a largo plazo y de forma colaborativa. Aunque la ciberseguridad se haya convertido en una gran preocupación debido al aumento e intensidad de los ciberataques en un mundo cada vez más interconectado, desde Auditoría Interna tenemos esa oportunidad de contribuir al fortalecimiento de la capacidad de las organizaciones para afrontar estos riesgos.

Riesgos Geopolíticos y de Ciberseguridad en la industria del automóvil: Un enfoque desde la Auditoría Interna

El contexto geopolítico actual ha evidenciado la fragilidad de un modelo de producción globalizado. Paralelamente, la creciente digitalización de los vehículos ha abierto la puerta a amenazas cibernéticas sin precedentes y aquí la función de Auditoría Interna adquiere un papel estratégico.

La industria del automóvil se encuentra en un momento decisivo. La transformación digital ha convertido a los vehículos en plataformas tecnológicas sobre ruedas, altamente dependientes de software, conectividad y componentes electrónicos. Esta evolución ha traído consigo una serie de beneficios, pero también ha expuesto al sector a **nuevos y complejos riesgos, especialmente en los ámbitos geopolítico y de ciberseguridad.**

Las tensiones internacionales, los conflictos armados y las disrupciones en la cadena de suministro —como las provocadas por la pandemia de COVID-19, la guerra en Ucrania o las fricciones entre China y Taiwán— han evidenciado la **fragilidad de un**

Raúl Chaudon Segura. *Director de Auditoría Interna SEAT/CUPRA.* *Raul-jorge.chaudon@seat.es*
Ekaterina Nikolaeva. *Manager Auditorías Financieras y áreas Administrativas SEAT/CUPRA.* *Ekaterina.Nikolaeva@seat.es*
Alfonso Medina Cotes. *Manager Auditorías Técnicas e Investigaciones Especiales SEAT/CUPRA.* *alfonso.medina@seat.es*

> **La Auditoría Interna debe integrarse plenamente en la gobernanza tecnológica de las organizaciones automotrices.**

modelo de producción globalizado. La alta concentración de proveedores de semiconductores y tecnología en regiones específicas ha dejado a muchos fabricantes vulnerables ante eventos externos que escapan a su control.

Paralelamente, **la creciente digitalización de los vehículos ha abierto la puerta a amenazas cibernéticas sin precedentes.** Los automóviles modernos incorporan sistemas avanzados de asistencia al conductor (ADAS), actualizaciones remotas (OTA), *infotainment* (Infoentretenimiento) y conectividad permanente, lo que los convierte en objetivos atractivos para ciberataques. Estos ataques no solo comprometen la privacidad de los usuarios, sino que también pueden poner en riesgo la seguridad física y la continuidad operativa de las empresas.

En este contexto, **la función de Auditoría Interna adquiere un papel estratégico.** Más allá de su rol tradicional de control, se convierte en **un agente clave para anticipar, evaluar y mitigar estos riesgos emergentes.** Desde la identificación de vulnerabilidades en la cadena de suministro hasta la evaluación de la madurez en ciberseguridad, la Auditoría Interna debe integrarse plenamente en la gobernanza tecnológica de las organizaciones automotrices, así como la evaluación del cumplimiento de las regulaciones aplicables en los diferentes mercados (por ejemplo, EU Data Act, EU Supply Chain Act, normativas en materia de Derechos Humanos y temas medioambientales, etc).

Este artículo explora los **principales riesgos geopolíticos y de ciberseguridad que enfrenta el sector,** y propone un enfoque integral desde Auditoría Interna, incluyendo tanto las funciones de asesoramiento como aseguramiento, para fortalecer la resiliencia y sostenibilidad de la industria.

Dependencia de Proveedores Extranjeros

La industria del automóvil global se ha estructurado **en torno a una cadena de suministro altamente especializada y distribuida,** donde los fabricantes dependen de una red de proveedores para componentes críticos como semiconductores, sensores, baterías y software. Esta dependencia, especialmente de proveedores ubicados en Asia, ha expuesto al sector a riesgos geopolíticos significativos.

Según un informe de la Comisión Europea, más del 70% de los semiconductores utilizados en la industria del automóvil europea provienen de Asia oriental, principalmente de Taiwán y Corea del Sur.

Esta concentración geográfica ha generado cuellos de botella severos, como se evidenció durante la pandemia de COVID-19 y la posterior crisis de chips, que provocó una caída de hasta el 30% en la producción de vehículos en Europa en 2021.

La UE ha comenzado a responder a esta vulnerabilidad con iniciativas regulatorias y estratégicas.

Además, la guerra en Ucrania afectó el suministro de gases industriales como el neón, esenciales para la fabricación de chips, y paralizó temporalmente fábricas de cableado para el sector en la región, afectando a diferentes marcas y al Grupo Volkswagen.

La Unión Europea ha comenzado a responder a esta vulnerabilidad con **iniciativas regulatorias y estratégicas:**

- **Ley Europea de Chips (European Chips Act):** Adoptada en 2023, esta legislación busca movilizar más de 43.000 millones de euros en inversiones públicas y privadas para duplicar la participación de Europa en la producción mundial de semiconductores al 20% para 2030.
- **Reglamento de Ciberseguridad (UE) 2019/881 y su actualización de 2024:** Establece un marco de certificación europeo para productos y servicios TIC, incluyendo componentes críticos de automoción, con el objetivo de garantizar la seguridad y resiliencia de la cadena de suministro digital.
- **Ley de Ciberresiliencia (Cyber Resilience Act):** Complementa las normativas existentes al exigir que los productos con elementos digitales, como los vehículos conectados, cumplan con requisitos mínimos de ciberseguridad durante todo su ciclo de vida.

Diferencias regulatorias entre mercados clave

Las regulaciones sobre ciberseguridad y gestión de la cadena de suministro varían significativamente entre regiones, lo que impacta directamente la estrategia de cumplimiento y gestión de riesgos de las empresas automotrices.

Europa se ha consolidado como líder en la regulación de la ciberseguridad y la gestión de la cadena de suministro en la industria del automóvil. Con un enfoque altamente armonizado, la región ha implementado normativas obligatorias como UNECE R155/R156 e ISO/SAE 21434, que exigen a los fabricantes garantizar la seguridad cibernética de los vehículos durante todo su ciclo de vida. Además, iniciativas estratégicas como la European Chips Act buscan reducir la dependencia de proveedores asiáticos en componentes críticos como los semiconductores, fortaleciendo así la resiliencia tecnológica del sector automotriz europeo.

Asia presenta **un panorama regulatorio diverso y fragmentado** en materia de ciberseguridad y cadena de suministro. China lidera con un enfoque estricto centrado en la soberanía digital, imponiendo leyes de localización de datos y control estatal sobre productos conectados. En contraste, países como Japón y Corea del Sur han adoptado estándares internacionales como ISO/SAE 21434, aunque con menor rigidez normativa. A pesar de ser el principal productor mundial de componentes electrónicos, la región carece de una armonización regulatoria común, lo que obliga a los fabricantes a adaptar sus estrategias de cumplimiento a cada jurisdicción nacional.

Latinoamérica enfrenta desafíos significativos en materia de regulación de ciberseguridad y gestión de la cadena de suministro en la industria del automóvil. Aunque países como Brasil y México son actores clave en la producción regional, la mayoría de los marcos regulatorios aún están en desarrollo. Las empresas suelen depender de estándares corporativos internacionales y certificaciones voluntarias, lo que genera una implementación desigual. Además, la limitada infraestructura tecnológica y la escasez de recursos especializados dificultan la adopción efectiva de prácticas avanzadas de ciberseguridad, lo que incrementa la exposición a riesgos en un entorno global cada vez más exigente.

Las empresas deben adaptar sus estrategias de auditoría y cumplimiento a cada entorno normativo. La armonización de estándares y la colaboración internacional son claves para una gestión de riesgos eficaz y global. Por eso, desde el Instituto de Auditores se ha promovido como el primer Requisito Temático el tema de ciberseguridad (Cybersecurity Topical Requirement | The IIA).

Para reducir la exposición a estos riesgos, las empresas automotrices están adoptando **diversas estrategias:**

1 DIVERSIFICACIÓN DE PROVEEDORES

- Establecer relaciones con múltiples proveedores en distintas regiones geográficas.
- Fomentar el desarrollo de proveedores locales o regionales dentro de la UE.

2 EVALUACIÓN DEL RIESGO

- Integrar el análisis de riesgos geopolíticos en la planificación estratégica y en los procesos de compras.
- Utilizar herramientas de inteligencia geopolítica y simulaciones de escenarios.

3 ACTIVIDADES DE CONTROL

- Adoptar modelos de “nearshoring” o “friendshoring” para acercar la producción a mercados estables.
- Invertir en tecnologías de trazabilidad y digitalización para mejorar la visibilidad y la capacidad de respuesta.

4 INFORMACIÓN Y COMUNICACIÓN

- Desde la Auditoría Interna, realizar evaluaciones periódicas de los proveedores más estratégicos, considerando no solo aspectos financieros, sino también ciberseguridad, continuidad operativa y cumplimiento normativo.
- En este contexto, la Auditoría Interna debe desempeñar un papel activo en la identificación de vulnerabilidades, la evaluación de controles y la promoción de una cultura de anticipación y adaptación.

Un ecosistema digital interdependiente

La digitalización del vehículo ha dado lugar a una arquitectura compleja, donde múltiples sistemas —desde el motor hasta el infoentretenimiento— están interconectados y dependen de software sofisticado. Esta evolución ha traído consigo una serie de riesgos que deben ser gestionados de forma integral.

Vulnerabilidad del código

El software moderno en las centralitas de los vehículos puede contener millones de líneas de código, lo que incrementa la probabilidad de errores, puertas traseras o configuraciones inseguras.

La falta de revisiones de seguridad en el ciclo de desarrollo puede permitir que vulnerabilidades lleguen a producción.

Conectividad y exposición a ciberataques

Interfaces como Bluetooth, Wi-Fi, redes móviles y actualizaciones OTA amplían la superficie de ataque.

Un atacante puede explotar una vulnerabilidad en un sistema no crítico (como el infotainment) para acceder a funciones sensibles del vehículo.

Protección de la información

Los vehículos recopilan y transmiten datos personales, de geolocalización y comportamiento del conductor.

La falta de cifrado, autenticación débil o almacenamiento inseguro puede comprometer la privacidad del usuario y la reputación de la marca.

Uso de proveedores externos de software

La subcontratación de desarrollo de software a terceros introduce riesgos de calidad, cumplimiento normativo y seguridad.

La falta de visibilidad sobre el código fuente y los procesos del proveedor puede dificultar la trazabilidad y la respuesta ante incidentes.

Riesgos asociados al uso de la nube

Muchas funciones del vehículo conectado dependen de servicios en la nube para navegación, actualizaciones, diagnóstico y más.

La interrupción de servicios Cloud, la pérdida de datos o accesos no autorizados pueden afectar la operatividad del vehículo y la experiencia del cliente, así como las aplicaciones y sistemas relacionados con la operatividad de la compañía.

Cesión de datos personales a proveedores

Pueden existir procesos en la compañía, cuando los datos personales, tanto internos como de terceros (p.ej. clientes) se ceden a proveedores externos y son tratados o almacenados en sus sistemas.

En estos casos es de vital importancia asegurar y comprobar que los proveedores cuentan con las medidas técnicas y organizativas que garanticen el tratamiento correcto de los datos en cumplimiento de GDPR. Una de las medidas que se puede requerir a los proveedores es obtener una certificación, en caso de la industria automóvil se utiliza la certificación TISAX (Trusted Information Security Assessment Exchange) – una certificación estándar de seguridad de la información para la industria automóvil, desarrollada por la Asociación Alemana de la Industria del Automóvil (VDA).

Desde Auditoría Interna, estos riesgos deben abordarse mediante:

1 AUDITORÍAS DEL CICLO DE VIDA DEL SOFTWARE

- Evaluar prácticas de desarrollo seguro, pruebas de seguridad y gestión de vulnerabilidades.
- Auditorías de software regulares.

2 EVALUACIÓN DE PROVEEDORES TECNOLÓGICOS

- Verificar el cumplimiento de estándares como ISO/SAE 21434 y capacidad de respuesta ante incidentes.

3 REVISIÓN DE ARQUITECTURA DE CONECTIVIDAD Y CLOUD

- Analizar la segmentación de Redes, autenticación, cifrado y cumplimiento de servicios Cloud
- Implementación de protocolos de seguridad robustos.
- Monitoreo continuo de la red y detección de intrusiones.
- Evaluaciones de seguridad periódicas y pruebas de penetración.

Rol de la Auditoría Interna

La Auditoría Interna, como tercera línea, desempeña un **papel estratégico en la mitigación de riesgos geopolíticos,** sobre todo en este momento en donde el panorama internacional se encuentra en una situación volátil, así también sobre los riesgos de ciberseguridad debido a una etapa de apertura de nuevos mercados y con una presión constante de nuevos competidores.

De **vital importancia,** nos ha servido **la estrecha colaboración y comunicación con los departamentos que componen la segunda línea** (Risk Management, Compliance, Servicios Legales, CISO y DPO). Estar alineados ayuda a la identificación temprana de los riesgos y preparación de una respuesta solida de medidas de mitigación de riesgos detectados y los controles relacionados.

Desde nuestro punto de vista algunas de las estrategias que hemos utilizado en los últimos años, nos hemos enfocado en la realización de **auditorías específicas sobre la resiliencia de la cadena de suministro,** enfocándonos en la dependencia de proveedores críticos en zonas geopolíticamente inestables. También dentro de nuestros trabajos de auditoría **hemos verificado si la organización ha implementado estrategias de diversificación de proveedores,** así como puntualizar los riegos de dependencia de proveedores y planes de contingencia. Además, **recomendamos que se integren herramientas de inteligencia geopolítica como mapas de riesgo por países** en donde debería de haber una evaluación automática de riesgo alto. Como tercera línea también hemos marcado **un claro posicionamiento de soporte a las unidades de negocio, bajo el rol de asesoramiento,** con actividades mediante las cuales estamos ofreciendo orientación a las partes interesadas, sin asumir funciones de gestión.

La Auditoría Interna, como tercera línea, desempeña un papel estratégico en la mitigación de riesgos geopolíticos.

En lo que respecta a los **riesgos de ciberseguridad** se debería de **auditar el ciclo de vida del Software,** incluyendo revisiones de código, revisión del control tanto de software usado en los procesos operativos de la compañía, así como también el control llevado a cabo sobre las aplicaciones desarrolladas para el coche, evitando con esto tener "shadow IT", pruebas de penetración para verificar que los controles sobre los accesos estén trabajando como deberían y gestión de vulnerabilidades. Es crucial evaluar la arquitectura de conectividad del vehículo, asegurando la segmentación de redes, el cifrado y la autenticación. También se debe verificar la implementación de protocolos de seguridad en servicios de Cloud y la gestión de accesos.

Otro gran desafío dentro de la práctica de la Auditoría Interna en ambientes internacionales está relacionado con el **cumplimiento de leyes y regulaciones en los diferentes países,** en lo referente a la conectividad del vehículo, el coche recolecta diferentes datos de los usuarios como son agenda, nombre, datos de geolocalización, etc. Por esto es muy importante llevar a cabo auditorías relacionadas con el cumplimiento de las regulaciones del manejo y almacenamiento de datos, así también con el cumplimiento del uso de herramientas de Inteligencia Artificial, usadas generalmente en este marco para analizar datos de clientes y de uso, por esto recomendamos auditar la aplicación de regulaciones como (UNECE, EU Data Act, EU AI Act), y además de estas también tenemos que tener en cuenta aquellas regulaciones como (Supply Chain Act, EU Deforestation Act) y otros riesgos relacionados con el medio ambiente. Es importante evaluar la preparación de la organización para responder a auditorías regulatorias en diferentes regiones (UE, Asia, LATAM).

Finalmente, debemos de **evaluar la efectividad de los programas** de información y concientización en materia de ciberseguridad, **promover la integración** de la gestión de riesgos en la cultura organizacional y **recomendar mejoras** en la gobernanza tecnológica y la toma de decisiones basada en riesgos. Dependiendo del grado de madurez de la compañía se tiene que decidir que enfoque sería el más adecuado. Nuestra recomendación es realizar **auditorías de aseguramiento cuando los procesos ya son robustos,** mientras que la función de asesoramiento y al mismo tiempo acompañamiento puede ayudar a las áreas menos maduras y con procesos en fase de desarrollo.

Miguel Ángel Serrano

Escritor, CEO y Asesor principal en Landguage Consulting

www.landguage.consulting

IA y AI:
Riesgos en inteligencia artificial

IA Y AI:
RIESGOS DE LA INTELIGENCIA ARTIFICIAL

En mi último libro, ***Androiceno: Escribir en la era de la inteligencia artificial,*** dedico un capítulo a hablar sobre algunos riesgos de uso de esa tecnología, no necesariamente de cumplimiento, sobre los que conviene reflexionar desde y más allá de la Auditoría Interna. Una tecnología con un poder disruptivo tan grande necesariamente va a ir evolucionando y destapando nuevos riesgos: por ejemplo, cómo afecta a la marca el uso de contenidos artificiales, la desmoralización de la plantilla o la gran dificultad de controlar la utilización que los empleados pueden hacer desde sus cuentas privadas.

> Una tecnología con un poder disruptivo tan grande necesariamente va a ir evolucionando y destapando nuevos riesgos

¿Qué riesgos hay en la IA?

En el libro trato sobre siete de ellos y sobre otro inherente a la capacidad que la IA tiene como herramienta: el uso que los delincuentes pueden hacer (ya lo están haciendo, desde las estafas online a la suplantación convincente de identidad). Me detengo brevemente sobre cada uno de ellos.

ENTRENAMIENTO CON DATOS PROTEGIDOS POR DERECHOS DE AUTOR

Algunos sistemas de inteligencia artificial han sido entrenados de modo ilegal: esto está en proceso de litigación en varios países del mundo, especialmente EE. UU. Es evidente que supone un problema de cumplimiento para el usuario.

En mi último libro, *Androiceno: Escribir en la era de la inteligencia artificial*, dedico un capítulo a hablar sobre algunos riesgos de uso de esa tecnología

Asociado al anterior, la **INSEGURIDAD JURÍDICA,** pues dependiendo del tenor y vector de los fallos judiciales, las empresas desarrolladoras de IA pueden encontrarse con problemas de continuidad más que severos, con daño para sus clientes.

CONFIDENCIALIDAD DE LOS DATOS

Los *prompts* y diálogos con estos *softwares*, especialmente en sus versiones gratuitas o de open source, pasan también al entrenamiento de las máquinas. Es importante comprobar la confidencialidad. También se está detectando riesgo por el uso individual de empleados que no utilizan las licencias corporativas sino las personales.

SEGURIDAD DE LOS DATOS

Como con cualquier almacenamiento, los datos no están exentos de ataques o robos. Los procesos de concentración en unos pocos proveedores hacen que el riesgo de ciberseguridad se concentre y aumente.

SESGOS Y PROBLEMAS ÉTICOS

Es sabido que los programas de inteligencia artificial tienen sesgos y estereotipos que provienen de los datos de entrenamiento, o del propio algoritmo. El problema es que en el *output* estos sesgos pueden suponer sobre-ponderaciones o, directamente, injusticias.

ALUCINACIONES

La definición más sencilla es la de los errores que los programas de inteligencia artificial cometen al generar textos o imágenes tras la petición de los usuarios. En realidad, estos programas están diseñados para contestar rápidamente, de modo que no es inhabitual que se inventen datos y respuestas, con el evidente riesgo de calidad y reputación que eso conlleva.

Es un tema que debe preocupar a los consejos de administración y a Auditoría Interna.

FALTA DE EXPLICABILIDAD:

Algunas de las iteraciones lógicas que llevan a cabo estos programas no son replicables o incluso explicables. En la comunidad científica se asume que hay un riesgo de “caja negra” que implica que no sabemos exactamente qué pasa en algunas de esas máquinas. Esto parece que empeorará según aumente la autonomía de las máquinas.

Hay muchos otros riesgos (la atrofia de pensamiento, la captura cognitiva…). Sin duda, **es un tema que debe preocupar a los consejos de administración y por supuesto, a los estamentos de control como Auditoría Interna.**

Antonio Garamendi

Presidente de la Confederación Española de Organizaciones Empresariales (CEOE)

> Es esencial que el auditor interno mantenga una postura crítica y objetiva y que esté orientado a la mejora continua de la empresa

Por Ignacio Bazarra
Fotos: CEOE

En noviembre de 2024, el **Instituto de Auditores Internos de España se integró en CEOE** con el objetivo de promover la profesión de la Auditoría Interna como función clave del gobierno de las empresas. En este número de la revista Auditoría Interna **entrevistamos a su presidente, Antonio Garamendi** (Getxo, 1958), con una larga trayectoria empresarial y al frente de CEOE desde 2018.

¿Cuál es el balance que hace de la figura de la Auditoría Interna en las empresas en los últimos años?

En primer lugar, creo que es importante poner en valor **el papel de la Auditoría Interna como garante de la transparencia, la ética y la gestión eficaz de riesgos** tanto en las empresas como en la administración. Dicho esto, su figura ha ganado **relevancia estratégica** en los últimos años, especialmente en momentos de crisis, en los que su importancia se incrementa.

¿Han mejorado los controles y la gestión de riesgos?

Sí, sin lugar a duda. **La Auditoría Interna ha evolucionado hacia un enfoque más multidimensional, preventivo y estratégico**, con un papel activo en la evaluación de riesgos críticos y en la promoción de una cultura organizacional sólida. Esta evolución tiene que ver con el hecho de que las organizaciones han avanzado significativamente en el fortalecimiento de sus sistemas de control interno y gestión de riesgos. Este progreso ha sido impulsado por la **necesidad de adaptarse a un entorno más complejo, donde los riesgos no solo son financieros, sino también éticos, reputacionales y operativos.**

¿Qué valor añadido aporta la Auditoría Interna a las empresas?

La inestabilidad y la volatilidad del entorno económico y geopolítico actual hace que sea preciso **establecer nuevos estándares y mecanismos que garanticen un control interno más eficiente,** así como una gestión de riesgos integral que tenga en cuenta las múltiples variables que influyen en el funcionamiento de las compañías. En ambos casos, **la independencia y la transparencia son las variables claves.**

Por tanto, la implementación de marcos sólidos de gestión de riesgos no sólo permite optimizar recursos y mejorar el rendimiento, sino también **aumentar la confianza de inversores y grupos de interés.** Asimismo, la evaluación continua de los riesgos, junto con controles específicos y una cultura organizacional alineada con los valores éticos, refuerza la capacidad de las empresas para anticiparse a situaciones adversas y garantizar su sostenibilidad a largo plazo.

> La figura del Auditor Interno ha ganado relevancia estratégica en los últimos años, especialmente en momentos de crisis.

Seguramente a lo largo de su vida empresarial ha trabajado con muchos auditores internos. ¿Qué características y cualidades cree que son más relevantes en estos profesionales?

Independencia junto con una buena dosis de escepticismo. Es esencial que el auditor interno tenga la capacidad de mantener una **postura crítica y objetiva.** También es necesario que el auditor interno esté orientado a la **mejora continua de la empresa.** Es decir, que su labor no sea tan solo detectar fallos, sino que proponga mejoras y anticipe los riesgos, para ello deberá contar con un amplio conocimiento, no sólo técnico sino también multidisciplinar en áreas como riesgos, contabilidad, normativa mercantil, tecnología y ESG. Todo lo anterior se debe complementar con **una buena capacidad de comunicación y un fuerte compromiso con la ética y la cultura organizacional.**

> Las cualidades más relevantes del Auditor Interno: independencia y una buena dosis de escepticismo.

¿Cómo valora la incorporación del Instituto de Auditores Internos a CEOE?

Para CEOE es un privilegio contar con una organización como el Instituto de Auditores Internos, que cuenta con 4.000 asociados, y cuya bandera son la transparencia y la ética, dos valores esenciales para la gobernanza y la competitividad de las empresas y elementos diferenciadores que contribuyen a construir mejores organizaciones. Por tanto, estamos muy satisfechos y agradecidos por su incorporación a nuestra casa, la de todas las empresas españolas. Estamos convencidos de que **esta alianza servirá para ayudarlas a que operen con los estándares más altos de gobernanza, transparencia y ética.**

Uno de los riesgos crecientes en las empresas es todo lo relacionado con la ciberseguridad. Los empresarios la citan como una de sus máximas preocupaciones. ¿En qué posición se encuentra España en esta materia?

Efectivamente, los ciberataques han escalado posiciones en el ranking de las mayores preocupaciones de los empresarios. No es de extrañar si tenemos en cuenta que **el 45% de las empresas españolas han sido víctimas de** un ciberataque. **Sólo en 2024 se produjeron más de 97.000 incidentes** de los cuales **cerca del 33% afectaron a empresas**, la gran mayoría de ellas pymes y micropymes. Las cifras, en sí, representan un reto, sin embargo, el verdadero reto se encuentra en cómo responder a este problema. **En CEOE creemos que la respuesta radica en el talento.** Según los datos de Fundación Telefónica, en España faltan 50.000 personas especializadas en ciberseguridad. Es ahí donde tenemos que actuar. No obstante, esta es una responsabilidad común que requiere de proyectos como +Ciberseguridad, que impulsamos Fundación CEOE e INCIBE y en cuya estrategia participan las organizaciones territoriales de CEOE, Guardia Civil, Policía Nacional y Fundación Hermes.

> La respuesta al reto de la ciberseguridad radica en el talento. En España faltan 50.000 personas especializadas en ciberseguridad. Es ahí donde tenemos que actuar.

> Los bajos niveles de productividad son la raíz de la que se alimentan el resto de los lastres de nuestra economía.

Más de 11 años al frente de CEPYME y CEOE le otorgan una visión panorámica y transversal de la economía española. ¿Cuáles cree que son los problemas estructurales que lastran nuestra economía?

En España tenemos **un gran reto** que es el de la **productividad.** Los bajos niveles de productividad son la raíz de la que se alimentan el resto de los lastres de nuestra economía. **Estamos casi cinco puntos por debajo de la media europea.** Este déficit está marcado por tres elementos, la **escasez de capital tecnológico** – con niveles más de 35 puntos por debajo de la media de la UE-, el **escaso tamaño empresarial y el marco regulatorio y fiscal.** A lo anterior hay que añadir el grave problema que representa el **absentismo laboral** para las empresas españolas. En su último informe del mes de junio, presentado en la sede de CEOE, las Mutuas alertan de que el coste de las bajas laborales superará los 32.000 millones de euros al final de este ejercicio, un 10% más que el pasado 2024.

En cuando al mercado laboral, **seguimos estando entre los países europeos con mayores tasas de desempleo juvenil,** un 25,6% y con niveles de rotación que no dejan de aumentar. Además, un 75% de las empresas en España tiene problemas para cubrir sus vacantes por la escasez de talento, lo cual debería llevarnos a replantear el modelo de formación actual, danto mayor cabida a modalidades como, por ejemplo, la FP Dual.

Por otra parte, nos preocupa mucho que la involución que se está produciendo en el diálogo social pase de ser un hecho coyuntural a convertirse en un problema estructural.

> La industria de Seguridad y Defensa es la palanca de la reindustrialización de Europa y clave para la competitividad por su capacidad tractora en términos de innovación.

Desde 2020 se habla mucho en Europa de reindustrialización, pero los resultados no son aún visibles. ¿Qué tiene que pasar para que la industria vuelva a ser el motor de las economías nacionales y recuperemos así cierta autonomía estratégica?

Europa debe garantizar la seguridad económica y recuperar su autonomía estratégica sin caer en un proteccionismo ineficiente. Para lograrlo hay que tener presente que **el papel de las empresas es clave.** Una Europa fuerte necesita empresas competitivas que puedan innovar, mejorar la eficiencia de sus procesos y ser más sostenibles. Y para ello **es imprescindible que se pongan en marcha políticas que fomenten la inversión y generen seguridad jurídica.** Hemos de avanzar en la simplificación normativa, agilizar la toma de decisiones… España y Europa tienen que **redefinir el marco regulatorio,** que asegure que las normativas europeas y nacionales estén alineadas y sean coherentes, sin duplicidades ni contradicciones. **Europa debe apostar por un proyecto de autonomía estratégica** que le permita convertirse en un actor global para poder defender sus intereses. Aquí, quiero referirme, en concreto, a la **industria de Seguridad y Defensa** que, coincidiendo con los informes Letta y Draghi, creemos que es la **palanca de la reindustrialización de Europa y clave para la competitividad** por, entre otras cuestiones, su capacidad tractora en términos de innovación. En CEOE y en BusinessEurope, apoyamos el Plan ReArmar Europa y trabajamos conjuntamente para desarrollar una industria de defensa fuerte, moderna, innovadora y resistente que actúe como motor y agente de transformación de nuestro tejido productivo.

> Tenemos que conseguir más empresas como Airbus en Europa y para ello lo primero que debemos hacer es perder el miedo a las grandes fusiones.

La productividad, como acaba de señalar, es la asignatura pendiente de la empresa española. Y muchas veces se menciona el alto porcentaje de Pymes como un problema, más que como una muestra de riqueza. ¿Cómo valora la estructura empresarial española y qué es lo que realmente lastra la competitividad?

Es cierto que gran parte de la brecha de productividad de España frente al resto de economías europeas y de la OCDE se deriva de que nueve de cada diez empresas en España son pymes o micropymes. Dicho esto, **las empresas españolas tienen ganas de crecer.** Quieren crecer. Para ello necesitamos una carretera sin baches, sin barreras y sin peajes. Un entorno en el que casi el 49% de la recaudación fiscal procede de las empresas, situándonos así como el cuarto país con mayor contribución fiscal tanto de la OCDE como de la UE -tal y como recoge el informe 'Competitividad fiscal empresarial 2025: El nuevo indicador de la contribución fiscal empresarial total', elaborado por el Instituto de Estudios Económicos (IEE)-, y en el que se quieren aprobar medidas como la reducción de jornada laboral a 37,5 horas sin tener en cuenta las singularidades del sector, es un entorno hostil para la inversión y, por tanto, el crecimiento empresarial.

¿Qué le parece la idea de crear "campeones" nacionales o europeos capaces de competir con grandes corporaciones asiáticas y estadounidenses?

En CEOE coincidimos plenamente con esa idea. **Hay que forjar grandes alianzas empresariales de carácter europeo.** Europa necesita que sus empresas sean fuertes para impulsar su autonomía estratégica y, como apunta en su pregunta, esa fortaleza se consigue con grandes

campeones empresariales, especialmente en sectores estratégicos como la industria, la tecnología o la defensa. Un objetivo para el que, además de la simplificación normativa a la que ya me he referido antes, **la colaboración público – privada es clave.** Pensemos en Airbus como ejemplo a seguir, la compañía que es líder del sector aeronáutico en innovación, sostenibilidad y tecnología digital lleva varios años superando a su máximo competidor en pedidos, ventas y entregas, la estadounidense Boeing. Tenemos que conseguir más Airbus en Europa para ello lo primero que debemos hacer es perder el miedo a las grandes fusiones.

La IA he reactivado la producción normativa en Europa y hoy las empresas afrontan nuevas directivas y mecanismos de supervisión relacionadas con su uso. ¿Cree que la IA contribuirá a mejorar la competitividad de las empresas y avanzar en esa autonomía estratégica a la que nos hemos referido?

En primer lugar, me gustaría señalar que en CEOE defendemos que **la transición digital**, entendida como clave de competitividad, **debe ser inclusiva.** Nadie puede quedar al margen. Sólo de ese modo tendremos cada vez más empresas, más grandes, más sostenibles y más resilientes. Herramientas como la IAl o el Big Data contribuyen a mejorar nuestra productividad y, a la vez, los entornos laborales. Permite que las empresas y las personas nos adaptemos de manera más sencilla y menos traumática a los constantes giros de guion a los que estamos sometidos por un contexto en el que las rivalidades geopolíticas están obligando a redefinir la hoja de ruta de las economías. Por otro lado, **estas tecnologías son una cuna para el talento,** otro de los retos que tenemos que afrontar con urgencia. En CEOE creemos que materias como la computación y la IA deben ser prioridades en la estrategia de competitividad española y europea, entre otras cuestiones porque, además, son estratégicas para la ciberseguridad.

En relación con la regulación, cada año se publican en España más de 1 millón de páginas en los distintos boletines oficiales. ¿Es viable emprender en España en un ecosistema tan intensivo de producción normativa?

La producción normativa es otro de los campos de batalla para las empresas que tienen que dedicar multitud de recursos y hacer enormes esfuerzos para adaptarse y mantenerse al día de las novedades y cambios legislativos en perjuicio de su competitividad. Cada año aumentan el número de páginas y normas que se aprueban.

Sin ir más lejos, el informe sobre Producción normativa en 2024 que elaboramos en CEOE destaca que el pasado año se aprobaron 719 normas, un 5% más que en 2023. Y eso teniendo en cuenta la fragmentación del Parlamento. Si queremos que haya más emprendedores, mejorar nuestra competitividad y que nuestras empresas ganen tamaño y se conviertan en campeones europeos **hemos de avanzar en simplificación normativa.** No se trata de desregular sino de regular mejor.

> Las empresas tienen que dedicar multitud de recursos y hacer enormes esfuerzos para adaptarse y mantenerse al día de las novedades y cambios legislativos en perjuicio de su competitividad.

La CEOE está a punto de cumplir 50 años. Su evolución ha ido en paralelo a la de España, un camino de éxito con hitos como los Pactos de la Moncloa, aprobados justo después de su creación, en 1977, la Constitución o la entrada en la Comunidad Europea. ¿Cuál es el papel al que está llamada CEOE en esta nueva era económica, social y tecnológica, tan diferente a la del siglo XX, de la que solo estamos avistando sus primeros brotes?

Lo resumo en una palabra: **diálogo.** Y este se tiene que producir en el espacio que en CEOE consideramos la herramienta democrática más importante, el diálogo social, porque garantiza la cohesión, la paz social y una mejor adaptación a las reformas y cambios legislativos. Es, como definió Ortega y Gasset, "lo que nos une", incluso en los momentos más complejos como este que estamos atravesando. Desde CEOE **vamos a trabajar para dar la vuelta a la involución que estamos percibiendo en el diálogo social.** Vamos a trabajar para que bajo ese marco de diálogo se desarrollen los principios sobre los que pivote la transición **hacia una economía más digital y más sostenible.** En definitiva, vamos a trabajar por **superar ese reto que es la mejora de la productividad y la competitividad, desde la base de la justicia social, el trabajo de calidad y el crecimiento inclusivo y sostenible.**

Enrique Sueiro

Asesor de comunicación directiva
www.enriquesueiro.com

Inyectar distracción con palabrería es una forma de anestesia social que, por goteo, resulta tan perversa como letal.

Apagón por anestesia: propuestas de reanimación

Un apagón salta a la vista. Además del eléctrico, hay otros apagones en los que caer a cero puede ser tan inocultable como predecible. Un apagón de ese tipo, difícil de verlo venir, es el que se produce por anestesia (en sentido amplio). Así lo ilustra el ejemplo de la rana en la cazuela: huye *ipso facto* si percibe el agua hirviendo, pero puede morir cocida si el agua tibia se va calentando poco a poco. **Quienes llevamos algunos decenios en el ámbito de la comunicación directiva identificamos fácilmente ciertos apagones por anestesia.**

Hay muchas vías para inyectar dosis constantes y crecientes de anestesia que desembocan en muerte súbita. En sentido estricto, **lo único repentino es la parada cardiorrespiratoria, último instante de un proceso con final previsible.** *Mutatis mutandis,* lo que vamos conociendo del apagón eléctrico del pasado 28 de abril en España recuerda mucho algo de este proceso. Además, la reacción de euforia autocomplaciente de algunos responsables suscita más preocupación que las dudas que resuelve.

Lo ocurrido recuerda también al que Peter Burke llama síndrome Ch-Ch, referido a dos tragedias de 1986: Chernóbil y el *Challenger.* Los responsables de la central nuclear soviética eran muy conscientes de lo peligroso de la situación, pero siguieron las órdenes de los dirigentes del Partido Comunista, que impusieron fechas y cuotas incumplibles sin correr riesgos adicionales. Los gobernantes querían resultados, pero ignoraban o no querían saber nada de los riesgos adosados.

> Otra vía de anestesia social es crear palabras o cambiar su significado.

Algo similar ocurrió con el transbordador estadounidense que explotó instantes después de despegar. Ambas catástrofes fueron resultado de control de calidad deficiente, presión política, incompetencia y encubrimientos.

Consumado el error, comienza el proceso anestesiante con diversas fórmulas. Una muy efectiva consiste en **inyectar distracciones.** Algunas resultan más difícilmente detectables porque se enmascaran en ropaje de honradez solo aparente, como recurrir al comodín retórico de "investigar", "llegar hasta el final, caiga quien caiga" y palabrería equivalente. Hay modos de investigar que complican la verificación y amplían la distracción.

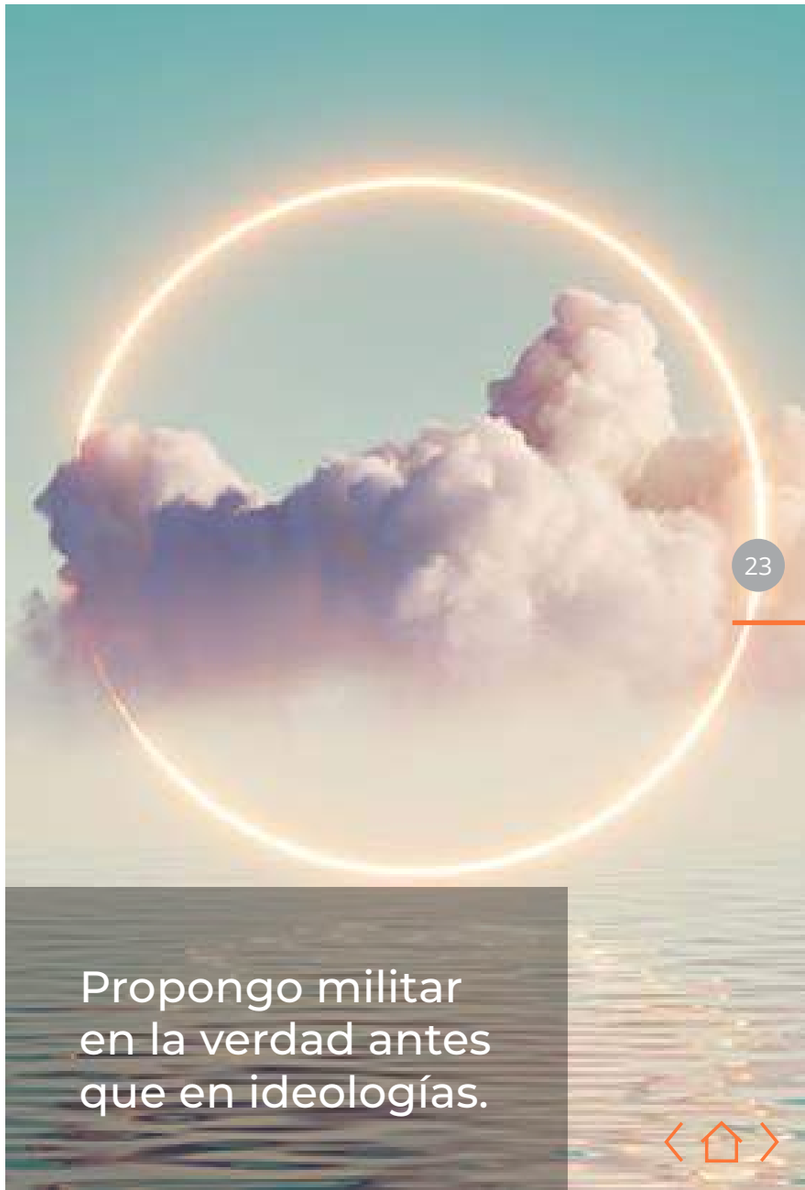
Es difícil, no imposible, resistirse a dosis de anestesia inyectadas por personas, organizaciones y países. ¿Cómo? **Activando mecanismos de reanimación.** Sí, cuando el cuerpo está bajo mínimos, es el momento del reánimo (la vuelta del ánima, del alma). El primer paso es pensar, fijarse, prestar atención, querer conocer la verdad… y vacunarse contra el ruido y la distracción.

Otra señal de alerta preventiva de anestesia es la **tergiversación del lenguaje por dos vías: crear palabras o cambiar su significado.** Alguien que detectó un ejemplo de mutación perversa fue el secretario general de la OTAN, que criticó el intento del presidente del Gobierno de España de modificar el concepto de gasto en defensa: "En la OTAN tenemos una definición clara de lo que es y lo que no es el gasto en defensa, y no vamos a cambiar esa definición". Así respondió a la pretensión española de incluir la protección de fronteras o la lucha contra el terrorismo en el cómputo del gasto en defensa.

Hay que combatir falsedades asumidas como premisas incuestionables.

Del libro **'Verdad organizada: apología de la razón para combatir la ola *fake*'** extraigo tres propuestas como vías de reanimación frente a futuros apagones por anestesia:

1. Recordar que **no siempre las palabras remiten a hechos ni las imágenes a realidades.**
2. **Combatir falsedades asumidas como premisas incuestionables.**
3. **Militar en la verdad antes que en legítimas opiniones o ideologías.**



A las puertas de un nuevo Requisito Temático: Terceras Partes

Una vez cerrado el plazo para revisión y comentarios al borrador el pasado mes de abril, se espera que el documento pueda ser finalmente publicado, en su versión definitiva, en septiembre de 2025.

En febrero de 2025 el IIA Global publicó el borrador de **un nuevo Requisito Temático sobre Terceras Partes,** entendiendo por éstas aquellas personas, grupos o entidades externas con las que las organizaciones mantienen relaciones comerciales.

El documento describe cómo **en el marco de estas relaciones con Terceras Partes, surgen una serie de riesgos** que pueden afectar a las organizaciones, y realiza un planteamiento de cara a evaluar los procesos de gobierno, gestión de riesgos y control sobre los mismos, considerando

Javier Sánchez-Rico. *Responsable de Contenido Técnico. Instituto de Auditores Internos de España.*
jsanchez@iai.es

tanto aspectos operativos (interrupciones del servicio, incumplimiento de los objetivos empresariales...), como de **ciberseguridad, financieros** (insolvencia del proveedor), relacionados con el **cumplimiento y/o jurídicos** (posibles conflictos de interés, disputas o litigios por incumplimiento de contratos), así como los **riesgos reputacionales** y los que pudieran estar relacionados con el **medio ambiente**, entre otros.

El Requisito Temático propone **una visión integral de todo el ciclo de vida de las relaciones que las organizaciones establecen con Terceras Partes.** Desde la selección, la contratación, incorporación, seguimiento y desvinculación de las mismas. Para cada una de estas fases, se plantean una serie de requisitos que los auditores internos deben tener en cuenta al evaluar los procesos de gobierno, gestión de riesgos y control interno.

Una vez cerrado el plazo para revisión y comentarios al borrador el pasado mes de abril, se espera que el documento pueda ser finalmente publicado, en su **versión definitiva, en septiembre de 2025**, si bien habrá que estar atentos a posibles novedades que pudieran ser informadas desde el IIA Global.

Por último, cabe recordar que los auditores internos deben **aplicar los Requisitos Temáticos, en conformidad con las Normas Globales de Auditoría Interna,** siendo obligatoria su **aplicación en los servicios de aseguramiento** y recomendada para los servicios de asesoramiento, evaluándose su conformidad durante las evaluaciones de calidad.

> Este Requisito Temático propone una visión integral de todo el ciclo de vida de relaciones de las organizaciones con terceras partes.

Abierto el período de consulta pública para el borrador del Requisito Temático de Comportamiento Organizacional

El IIA global ha **abierto el período de consulta pública** para el borrador del **Requisito Temático de Comportamiento Organizacional**, que forma parte del Marco Internacional de Prácticas Profesionales (MIPP) y complementa a las Normas Globales de Auditoría Interna.

Este nuevo elemento del MIPP incluye requisitos obligatorios para evaluar y valorar la eficacia de los procesos de gobierno, gestión de riesgos y control sobre temas de riesgo específicos en el ámbito del Comportamiento Organizacional.

El borrador del documento puede ser **consultado desde el 8 de julio hasta el 22 de agosto de 2025** para participar en la encuesta. Los resultados de la consulta pública son fundamentales para la elaboración de la versión final del documento, que estará acompañado por una guía de usuario.

Para profundizar en su implementación, el IIA Global ha organizado un webinar que se celebrará el próximo 6 de agosto de 2025.

Borrador Requisito Temático Comportamiento Organizacional:

Participa en la encuesta

Se fallan los II Premios IAI España a la confianza en el valor de la Auditoría Interna

PRIM, Sofinco España, Sanitas, Victoria Camps y Rafa Durán, ganadores de los II Premios IAI España

El jurado de los II Premios IAI España a la confianza en el valor de la Auditoría Interna ha fallado su segunda edición. Con estos galardones se busca mejorar el conocimiento y la valoración social de la Auditoría Interna en España, de sus profesionales y de los principios éticos que la sustentan.

Rocío Barrie. *Instituto de Auditores Internos.*
rbarrie@iai.es

Premiados 2025

En esta segunda edición, los premios han sido adjudicados de la siguiente forma en las cinco categorías:

2025 Premio **Impulsa**

PRIM

En reconocimiento a su desempeño en el desarrollo de una **cultura organizativa basada en la mejora continua y la responsabilidad corporativa,** liderando iniciativas innovadoras para mejorar la eficiencia operativa de control interno y la gestión de riesgos, y respaldar a la Comisión y al Consejo de Administración en la toma de decisiones fundamentales.

El jurado destaca entre otros méritos, su **posicionamiento dentro de la estructura organizativa de la compañía que le proporciona autonomía** para realizar su trabajo de manera independiente, un elemento crítico para el ejercicio de la Función.

2025 Premio **Posiciona**

SOFINCO ESPAÑA

En reconocimiento a su proyecto **'Auditoría Interna: de una función de control a un socio estratégico'.** Alineado con los pilares estratégicos de la compañía, Sofinco España establece un **plan estratégico que impulsa la visibilidad de la Auditoría Interna y posiciona a la función como asesor de confianza y embajador del cambio,** promoviendo dentro de su grupo la implementación de los nuevos estándares globales y las mejores prácticas de Auditoría Interna.

El jurado destaca el **impacto de la iniciativa y el esfuerzo realizado en proporción al tamaño y recursos** de la Dirección de Auditoría Interna de la compañía.

El acto de entrega de los II Premios IAI España tendrá lugar el 7 de octubre, en el marco de las Jornadas de Auditoría Interna.

2025 Premio Transforma

SANITAS

‘Tecnología NLP (Procesamiento del Lenguaje Natural) para auditar Informes publicados externamente’.

En reconocimiento a la creación de una **herramienta propia de NLP** (Procesamiento del Lenguaje Natural) para auditar Informes publicados externamente. Con esta tecnología el equipo de Auditoría Interna ha sido capaz de evaluar y proporcionar información en tiempo real, sobre la `edad media del lector', la similitud del texto con otras compañías del sector, el uso de palabras clave y el impacto (positivo o negativo) que estas pueden tener. El jurado valora el espíritu innovador de Sanitas y el enfoque práctico del proyecto.

Mención especial Premio Transforma: MAPFRE

‘Visión 360° sobre los Procesos Auditados en un entorno Multinacional’

En reconocimiento al desarrollo de una **innovadora herramienta de BI que genera información automática y diaria de los procesos auditados** para todos los niveles necesarios: de auditoría, corporativo y cubriendo la diversidad geográfica del grupo. Su aplicación ha permitido una **mejora del proceso de reporte, control y gestión de la función** de Auditoría Interna, minimizando los tiempos de preparación de la información, simplificando los reportes hasta el mínimo detalle. El jurado destaca la **capacidad para gestionar la diversidad geográfica de la compañía.**

2025 Premio Inspira

VICTORIA CAMPS

En reconocimiento a su **liderazgo ético y compromiso con los valores fundamentales de la profesión,** convirtiéndose en un referente para la comunidad de auditores internos. Especializada en Ética, Filosofía Política y Democracia, ha ejercido una **gran influencia en el ámbito académico y en el debate sobre valores éticos.** Su enfoque filosófico se caracteriza por la defensa de la ética del cuidado y el bienestar, proponiendo un enfoque más humanista y comprensivo de la moral en la vida pública y privada. El jurado **destaca su impecable trayectoria, su gran contribución al debate sobre justicia, igualdad y valores en la sociedad,** así como su **aportación a la Responsabilidad Social Empresarial,** entre otros múltiples aportes.

2025 Premio Comunica

RAFAEL DURÁN

En reconocimiento a su **destacada trayectoria en el periodismo económico español** y a su labor sostenida y especializada en los **ámbitos del buen gobierno, la transparencia empresarial y la sostenibilidad.** Su sección ‘Buen Gobierno’ en el diario Cinco Días ha sido pionera en dar espacio regular a la Auditoría Interna, la evolución de los códigos de buen gobierno, la responsabilidad social corporativa (RSC), la ética empresarial

y los criterios ESG (ambientales, sociales y de gobernanza).

El jurado **destaca su trayectoria profesional, su contribución a la difusión del buen gobierno y de la Auditoría Interna, así como la calidad de los contenidos** publicados.

Entrega de los Premios

El **acto de entrega de los II Premios IAI España** tendrá lugar el **7 de octubre de 2025,** en el marco de las **Jornadas anuales de Auditoría Interna** (IFEMA Madrid).

TODA LA INFORMACIÓN DE LOS II PREMIOS IAI ESPAÑA:

El Jurado

La composición del jurado de los II Premios IAI España la han formado:

- **Federico Buyolo**, director cultural de la Fundación Ortega y Marañón.
- **Emma Fernández Alonso**, consejera independiente en Metrovacesa.
- **José Manuel González Huesa,** director de la agencia de noticias Servimedia.
- **Gabriela González-Valdés**, directora general del Instituto de Auditores Internos de España.
- **María Luisa Jordá**, consejera independiente en Merlin, Bankinter, Bimbo, además de ser la presidenta del consejo asesor del Instituto.
- **Mario Lara,** director de ESADE Madrid y del Center for Corporate Governance de la universidad que dirige.
- **Fernando Pastor Yélamos,** corresponsal económico de El Español.

Además, por parte del IAI, han participado, con voz, pero sin voto, su presidenta, **Sonsoles Rubio**, en calidad de presidenta del jurado, y **María Cano**, directora de Comunicación y Marketing, que ha actuado como secretaria.

Trump hackea el sistema internacional

Federico Steinberg, catedrático Príncipe de Asturias en la Universidad de Georgetown e Investigador Principal del Real Instituto Elcano, aborda en este artículo el contexto geopolítico actual en plena era Trump y cómo está afectando a Europa en el ámbito económico.

Firma Invitada:
Federico Steinberg

El economista Richard Baldwin acaba de publicar un libro titulado **“El gran hackeo”**, en el que explica cómo el presidente Trump, más allá de generar incertidumbre y riesgos de todo tipo para el crecimiento económico, está poniendo patas arriba el sistema internacional. Bajo la excusa de que “el mundo ha tomado el pelo a Estados Unidos”, responde mediante un hackeo del orden internacional tal y como lo entienden los expertos en ciberseguridad. Esto supone que no quiere reformar ni reconstruir nada, sino simplemente **“Saltarse el código, hacer cortocircuitos y aplicar por la fuerza bruta una solución rápida mediante aranceles masivos”.**

Federico Steinberg.
Catedrático Príncipe de Asturias en la Universidad de Georgetown e Investigador Principal del Real Instituto Elcano.

> La geopolítica le ha hecho una OPA hostil a la economía.

El problema para los europeos es que esto pasa por dejar en suspenso la alianza transatlántica, abandonar Ucrania a su suerte y seguir una política económica que podría incluso generar una crisis financiera en Estados Unidos que dañaría a las economías europeas. De hecho, el pasado 26 de febrero, Trump dijo que "La Unión Europea se creó para fastidiar a Estados Unidos. Y ha hecho un buen trabajo", lo que convertiría a Europa en un rival en el mejor de los casos o un enemigo en el peor.

Para entender mejor cómo hemos podido llegar hasta aquí, hay que tener en cuenta que, en los últimos años, **la geopolítica le ha hecho una OPA hostil a la economía.** Hoy es imposible analizar las perspectivas de crecimiento económico y evaluar los riesgos sin tener en cuenta que la racionalidad económica y los sosegados y técnicos análisis coste-beneficio juegan un papel mucho menos importante que durante las décadas de hiperglobalización que precedieron a la crisis financiera de 2008.

Han vuelto el proteccionismo, el nacionalismo y el imperialismo, la política industrial y las preocupaciones de seguridad nacional han pasado a ser primordiales (especialmente en Washington en relación con China, pero también en Europa), y la globalización ha dejado de ser considerada un juego de suma positiva para ser utilizada como arma arrojadiza. En definitiva, el prisma del orden económico liberal basado en reglas en el que la eficiencia y el crecimiento son primordiales ya no sirve para entender el mundo.

Pero esta vuelta de la geopolítica no ha hecho que las leyes de la economía hayan desaparecido. Por lo tanto, cuando Estados Unidos anuncia aranceles indiscriminados como sucedió el pasado 2 de abril en el llamado **"Día de la Liberación"**, los mercados se resienten porque anticipan menos crecimiento, más inflación, disrupciones en las cadenas de suministro, caída de los beneficios empresariales y conflictos políticos internacionales.

Del mismo modo, cuando el Congreso de Estados Unidos aprueba una ley presupuestaria, la llamada **"One Big Beautiful Bill"** propuesta por la Administración Trump y que todavía se está negociando con el Senado, que recorta los ingresos públicos y aumenta los gastos de forma que el déficit y la deuda pública se disparan, la confianza en el dólar empieza a debilitarse. Y con ella, lo impensable, que Estados Unidos pueda sufrir una huida de capitales como le pasa a los países emergentes, se vuelve una posibilidad. Así, aunque Estados Unidos tienen todavía un enorme potencial de crecimiento y una economía muy dinámica, el rápido deterioro institucional que esa sufriendo por los constantes ataques del presidente Trump al estado de derecho y a instituciones independientes como la Reserva Federal podrían generar inestabilidad financiera e incluso erosionar seriamente el papel del dólar como moneda de reserva global.

Reaccionar ante la incertidumbre permanente y los volantazos de la que todavía es la primera potencia económica y geopolítica global no va a ser fácil, sobre todo para los europeos. Pero **es imperativo que en Bruselas y otras capitales internalicen que el orden internacional bajo el que tan cómodos se sentían, se está derrumbando.**

En el **plano geoeconómico**, eso implica reducir riesgos de las dependencias tanto de China como de Estados Unidos, reforzar el mercado interior eliminando barreras internas para aumentar la productividad y buscar nuevos acuerdos comerciales con países del sur plural para diversificar tanto proveedores como mercados de exportación. Pero, sobre todo, **la UE debería completar la unión bancaria y fiscal y emitir deuda conjunta para financiar bienes públicos europeos** – seguridad, defensa, investigación, transición energética e infraestructuras críticas, entre otros – con el objetivo de aumentar la demanda interna y aspirar a liderar un nuevo orden económico internacional liberal, abierto y basado en reglas para el que todavía hay una elevada demanda global. **Sólo así lograría "hablar el lenguaje del poder" y dar significado al elusivo concepto de "autonomía estratégica".** Pero eso requiere mayor integración política, y la gran pregunta es si hay apetito para la misma cuando la extrema derecha nacionalista también gana apoyos en los estados miembros.

> Reaccionar ante la incertidumbre permanente no va a ser fácil.

Reinventando la resiliencia empresarial: retos y realidades de los riesgos emergentes

Nos enfrentamos a una realidad donde los riesgos emergentes aparecen con mayor frecuencia y de forma más compleja, ante el que el área de Riesgos y Auditoría Interna debe ir más allá de su rol tradicional para convertirse en un aliado estratégico.

Vivimos en un mundo **donde la incertidumbre se ha convertido en un factor estructural, una constante** que ya no es solo pasajera ni excepcional, sino que define cómo operan hoy las organizaciones y la sociedad.

Los cambios tecnológicos acelerados, las tensiones geopolíticas, las transformaciones sociales y la creciente interconexión global han elevado lo inesperado a la norma. Esto significa que las certezas de ayer —sobre mercados, regulaciones, cadenas de suministro o comportamiento del

Pablo Martín-Alonso Jorge. *Director de Riesgos y Seguros en Globalvia.*
pmartin@globalvia.com

> Los riesgos emergentes aparecen con mayor frecuencia y de forma más compleja.

consumidor— ya no bastan para planificar con seguridad. En su lugar, nos enfrentamos a **una realidad donde los riesgos emergentes aparecen con mayor frecuencia y de forma más compleja**, en un entorno en constante evolución y con múltiples variables entrelazadas.

Ante estas nuevas reglas de juego **las áreas de Riesgos y Auditoría Interna deben ir más allá de su rol tradicional de control y supervisión para convertirse en aliados estratégicos** que potencien la capacidad para anticipar amenazas, responder con agilidad y aportar un valor real y sostenible en un entorno cada vez más volátil y desafiante.

En los últimos años, los riesgos emergentes han dejado de ser amenazas aisladas para transformarse en **escenarios complejos donde factores geopolíticos, sociales, tecnológicos, económicos y ambientales se mezclan y amplifican la incertidumbre global.** Estos riesgos ya no son meras hipótesis, sino realidades palpables y de naturaleza diversa que impactan nuestra vida cotidiana.

Un claro ejemplo es el **apagón masivo** que experimentaron España y Portugal, que evidenció cómo la fragilidad de infraestructuras críticas puede desencadenar una crisis que paraliza a millones de personas y pone en jaque la economía de toda una región. Por otro

lado, las **políticas proteccionistas y los cambios repentinos en el comercio internacional**, impulsados en los últimos meses por la administración Trump, han provocado un efecto dominó que ha desestabilizado cadenas de suministro globales y obligado a muchas empresas a replantear estrategias que hasta entonces parecían inamovibles.

Otro ejemplo que ilustra la diversidad de estos desafíos se encuentra en la geopolítica, donde es bien sabido que **las guerras en Ucrania y las tensiones en Oriente Medio** mantienen un clima constante de inestabilidad. Si alguien piensa que estos conflictos están lejos de afectarle, solo tiene que revisar la factura de la luz o el precio en el supermercado para darse cuenta de lo contrario. El resultado es un aumento sostenido en los precios de la energía y los alimentos, una inflación persistente y economías que luchan por recuperarse, dejando a muchas personas con la sensación de que ahorrar se está convirtiendo en una tarea cada vez más difícil.

En paralelo, surgen nuevos riesgos que reflejan la velocidad y profundidad de las transformaciones actuales. En un mundo donde la velocidad de la innovación marca el ritmo, los riesgos tecnológicos y los vinculados a terceros se han convertido en desafíos ineludibles. La creciente dependencia de proveedores críticos y socios externos amplifica la vulnerabilidad organizacional, como evidencian incidentes

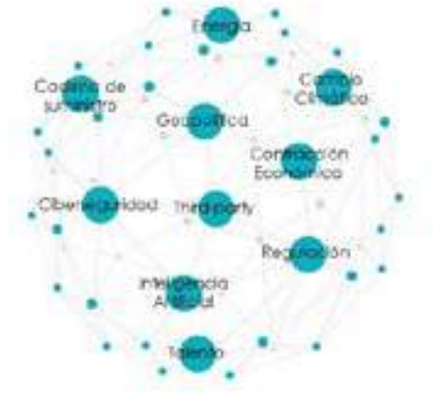
recientes que paralizaron servicios digitales esenciales a nivel global. Esta realidad obliga a las empresas a **fortalecer la gestión de riesgos de terceros**, porque un fallo ajeno puede convertirse en una crisis propia.

Paralelamente, la **rápida evolución de la inteligencia artificial** no solo abre enormes oportunidades, sino que también plantea riesgos inéditos —desde el sesgo algorítmico hasta la falta de regulación clara— que requieren un enfoque estratégico y ético para anticipar y mitigar impactos impredecibles. A este panorama se suma la **escasez de talento especializado**, un cuello de botella que limita la capacidad de las organizaciones para innovar y adaptarse con agilidad. En conjunto, estas dinámicas demandan no solo herramientas avanzadas, sino una mentalidad abierta y una cultura capaz de navegar en la complejidad sin perder el control.

Frente a este complejo mosaico de realidades, **la percepción sobre el futuro es clara y contundente: la inestabilidad global no es un riesgo lejano, sino una amenaza creciente y tangible.** El *Global Risks Report 2025* del Foro Económico Mundial revela que más del 50% de los expertos espera un mundo convulso en los próximos dos años, porcentaje que aumenta al 62% cuando se mira la próxima década, anticipando riesgos sistémicos capaces de transformar radicalmente el orden global.

Estamos frente a una realidad en la que la incertidumbre se ha convertido en un componente endémico de nuestro entorno, y esto nos exige **repensar el papel de las áreas de Riesgos y Auditoría Interna.** Ya no basta con ser vigilantes; debemos convertirnos en motores de resiliencia y transformación. ¿Estamos preparados para liderar esta revolución como motor de éxito?, ¿qué riesgos invisibles estamos dejando pasar que podrían poner en jaque nuestro futuro?

El reto está servido, y la invitación es clara: **la gestión de riesgos emergentes es mucho más que supervivencia; es la llave para reinventar la forma en que entendemos y construimos el éxito en un mundo imprevisible.**



> La inestabilidad global no es un riesgo lejano, sino una amenaza creciente y tangible.

El impacto de la geopolítica en la ciberseguridad

La incertidumbre, característica principal de la geopolítica actual, acentúa los riesgos de la ciberseguridad para los estados y las organizaciones.

La ciberdefensa es un elemento capital en las estrategias nacionales de defensa de los estados a nivel global, tanto por el potencial impacto de los ciberataques en la estabilidad de estados consolidados y en sus procesos legítimos de gobierno, como por su uso masivo en los diferentes conflictos actuales o rivalidades regionales, como la invasión rusa de Ucrania, la guerra israelí o los diferentes ejemplos de procesos de influencia en la opinión pública o de desestabilización mediante información falsa.

Yago Casal. *Socio de Technology & Transformation de Deloitte.* *ycasal@deloitte.es*
Encarnación Jurado Cano. *Socia de Audit & Assurance de Deloitte.* *enjurado@deloitte.es*

Asimismo, en el contexto de las organizaciones privadas, **la ciberseguridad lleva años siendo uno de los principales riesgos en los mapas de las organizaciones,** requiriendo un creciente nivel de atención por parte de los consejos de administración y la dirección de las corporaciones, que a su vez ven incrementada su potencial responsabilidad individual en caso de materializarse un ciberincidente.

> Aumentan las amenazas ciber y se redobla la presión sobre las organizaciones.

La geopolítica actual, caracterizada por la inestabilidad y la fragmentación, se encuentra sumida en una **incertidumbre creciente** y evidencia una ausencia de estabilidad en la gobernanza internacional.

Esto provoca la **erosión en elementos clave para la ciberdefensa,** como son la cohesión de alianzas u organizaciones transnacionales de defensa – como los impactos en la OTAN -, las iniciativas de compartición de inteligencia y la resiliencia de las cadenas de suministro claves en la industria de la ciberseguridad. En paralelo, supone una motivación extra para aquellos actores o estados que se valen de los ciberataques como mecanismos de agresión o de generación de inestabilidad.

Para las organizaciones privadas, y especialmente para aquellas que desempeñan el papel de infraestructura crítica o prestan servicios esenciales en una región o estado, este contexto aumenta las amenazas ciber y, por tanto, **se redobla la presión sobre las organizaciones y se frena el impulso a iniciativas de compartición de inteligencia y a la transversalidad de la cadena de suministro,** provocando un mayor aislamiento en la ciberdefensa.

> La ciberseguridad lleva años siendo uno de los principales riesgos en los mapas de las organizaciones.

En el contexto europeo, el contexto geopolítico ha derivado en la **necesidad de reforzar la autonomía estratégica en diferentes ámbitos, siendo la ciberseguridad uno de los más relevantes.** Existen diferentes retos a la hora de abordar esta iniciativa:

- **La falta de liderazgo en el progreso tecnológico,** especialmente en tecnologías disruptivas como la IA, dependiente de países terceros – especialmente Estados Unidos - y la gestión del conocimiento especializado.

- **La soberanía digital sobre los datos,** que de forma muy significativa está condicionada por los hiperescalares, también mayoritariamente norteamericanos.

- **Los efectos que se puedan derivar** del llamado efecto Bruselas europeo vs. el avance de los gigantes tecnológicos y de ciberseguridad americanos.

> Es necesario continuar incrementando el nivel de madurez en ciberseguridad.

Los **actores europeos** están, por tanto, obligados a ampliar a su vez las estrategias de ciberdefensa, favoreciendo en el proceso la industria europea y nacional de cada uno de los Estados miembros. Los Estados miembros son capitales para ello, a través de programas de inversión público/privada, si bien debe existir una coordinación y esfuerzo conjunto con las organizaciones privadas.

En el primer caso, es ya una realidad al multiplicar la Unión Europea por cinco la partida en defensa en su reciente propuesta de presupuesto para el período 2028-2034.

En el caso del **sector privado**, además de la necesidad de cumplir con los requisitos derivados de la normativa europea en el ámbito de la ciberseguridad (ej.: NIS2, CSA, DORA, etc.), que requiere un **incremento notable de los recursos,** es necesario continuar incrementando el nivel de madurez en ciberseguridad a la vez que se contribuye a la autonomía estratégica regional.

Para ello, aspectos como **la apuesta por el conocimiento y las cadenas de suministro europeas,** así como el **impulso del desarrollo tecnológico y la innovación** regionales en el ámbito de la ciberseguridad son claves para garantizar la sostenibilidad de nuestras organizaciones.

> Tenemos que convertir esta amenaza en la oportunidad para posicionarnos como "Partner Estratégico" de la organización.

La pregunta que las funciones de Auditoría Interna tienen encima de la mesa es: **¿Cómo sigo garantizando a mi Comisión de Auditoría que mi organización cuenta con un modelo de control efectivo para mitigar estos riesgos?**

Es específicamente una respuesta compleja dado que, como funciones de Auditoría Interna, estamos muy cómodos hablando de reporting financiero o de procesos de negocio en los que se tienen poca dependencia del exterior, pero esto es tendente a desaparecer y nos debemos preparar para ello. Nos debemos preparar explorando **planes de formación completos** para dotar a nuestras funciones de perfiles especialistas en ciberseguridad y en *third party risk management* (TPRM) y aliándonos con expertos externos que nos ayuden a entender las consecuencias del cambio.

Como conclusión, aunque el reto es relevante, tenemos que c**onvertir esta amenaza en la oportunidad para posicionarnos como "Partner Estratégico" de la organización**, la oportunidad de dar un paso adelante y ser los que promuevan la definición de **modelos robustos para supervisar los controles asociados a procesos externalizados y ciberseguridad,** puesto que, como sabemos mejor que nadie, tenemos una posición privilegiada para ello.

Hitos del IAI España en 2024

MEMORIA 2024

Ya se ha publicado la Memoria del IAI España 2024, que refleja un año de crecimiento, innovación y fortalecimiento institucional. Según destaca, ha sido clave para Auditoría Interna y para el Instituto, reafirmando nuestro compromiso con el buen gobierno, el interés público y la mejora continua de la función. Destaca el crecimiento del ecosistema profesional, con 4.110 socios, 165 actividades con más de 5.300 asistentes, además de la puesta en marcha de nuevas iniciativas como: LAB Innovación, Mentoría Técnica o los Premios IAI España, entre otros.

Más información

Asamblea general del IAI España 2025

EVENTOS

Más información

El 19 de junio de 2025 tiene lugar la celebración de la Asamblea general del IAI España, en la que su presidenta, Sonsoles Rubio, incidió en la incertidumbre institucional actual marcada por la situación geopolítica global, que “lejos de ser un obstáculo, se ha convertido en un motor de fortalecimiento para la profesión, que nos ha permitido reafirmar nuestra valía profesional, nuestra fortaleza, rapidez y flexibilidad de adaptación”. Cabe destacar la incorporación al Consejo del Instituto de José Luis Gurtubay, director general de Auditoría Interna de Mapfre.

Nuevo escenario geopolítico y estrategia de Auditoría Interna

FORO DE EXPERTOS

El Foro de Expertos del IAI España, celebrado en Comet Retiro en Madrid, abordó en esta ocasión el nuevo escenario geopolítico y la estrategia de Auditoría Interna.

Más información

Auditores internos reclaman la colaboración de empresas e instituciones para generar un estado de inestabilidad

ENCUENTRO CONSEJEROS

Más información

Encuentro Consejeros 2025, que, organizado por el Instituto el 23 de mayo. reunió a cerca de 100 consejeros de las grandes compañías españolas. Esta nueva edición abordó la influencia del contexto geopolítico y su impacto en las organizaciones, así como las oportunidades y riesgos de competitividad europea en un nuevo escenario mundial marcado por la incertidumbre.

La Guía SCIIS, ahora en inglés

GUÍAS IMPRESCINDIBLES

El Instituto ha publicado la Guía SCIIS en inglés, la primera guía diseñada para que las empresas puedan reforzar el control de la información sobre sostenibilidad y cumplir con los requisitos impuestos por las regulaciones europeas.

Accede al documento

El IAI participa en el LV Congreso Nacional de Representantes de Estudiantes de la AEALCEE

ALIANZAS

El Instituto de Auditores Internos (IAI) de España ha participado en el LV Congreso Nacional de Representantes de Estudiantes de la Asociación Española de Alumnos de Ciencias Económicas y Empresariales (AEALCEE), un punto de encuentro clave para el fortalecimiento de la representación estudiantil y la creación de sinergias entre estudiantes y el ámbito profesional.

Más información

El Instituto celebra el evento Internal Audit Day 2025 en Barcelona

ENCUENTRO CONSEJEROS

El IAI España, de la mano de Deloitte y con Naturgy como anfitrión, celebró el 13 de mayo en Barcelona una nueva edición de 'Internal Audit Day' en la que se abordaron diversos temas: 'ESG: de la Estrategia al Sistema de Control Interno', 'Retos de la Función de Auditoría Interna en empresas no cotizadas', 'Normas Globales de Auditoría Interna: Principales retos de su aplicación', y 'Auditoría Interna y las Comisiones Delegadas: dinámicas de trabajo conjunto'.

Auditoría Interna del Riesgo Reputacional

LA FÁBRICA DE PENSAMIENTO

El nuevo documento de La Fábrica de Pensamiento plantea cómo abordar este riesgo desde Auditoría Interna, proponiendo diversas actividades orientadas a los principales componentes y dimensiones a considerar de cara a la auditoría del sistema de gestión del riesgo reputacional.

Descarga el documento

Los auditores internos, un vehículo que garantiza el futuro de la empresa familiar

NUEVOS TERRITORIOS

El IAI España reúne en un desayuno empresarial en el diario alicantino Información 'Claves para el futuro de la empresa familiar alicantina: más allá de la operativa' a representantes empresariales, institucionales y académicos para analizar cómo la Auditoría Interna contribuye a la sostenibilidad de las empresas familiares.

Más información

Auditoría Interna: clave para el legado de la empresa familiar

NUEVOS TERRITORIOS

Más información

En el marco de la campaña del Instituto ‘Nuevos Territorios’, participó en la mesa redonda ‘Empresas familiares en Aragón, claves en la profesionalización de la economía española’, organizada por Heraldo de Aragón en Zaragoza. En ella diferentes personalidades a nivel empresarial e institucional abordaron cuestiones como la relevancia de estas compañías en el territorio o el rol que juegan en ellas agentes como los auditores internos.

El IAI y Agers elaboran el informe ‘Situación de gestión de riesgos empresariales en 2025’

CENTRO DE CONOCIMIENTO

El objetivo de este estudio es ofrecer una visión general sobre el grado de madurez en la gestión de riesgos de las compañías en España.

Más información

El IAI participa en el XXIV Premio AECA a la Transparencia Empresarial 2025

ALIANZAS

Más información

La presidenta del IAI España, Sonsoles Rubio, vuelve a formar parte del jurado del Premio AECA a la Transparencia Empresarial 2025, que, con más de dos décadas de recorrido, reconoce el esfuerzo y los resultados de las empresas en materia de transparencia y divulgación de la información financiera, de buen gobierno y sostenibilidad. En esta edición ha recaído en Iberdrola, en la modalidad IBEX 35, y ENCE, en la modalidad IBEX Medium & Small Cap.

Seguimiento del desempeño de Auditoría Interna

LOS LUNES DEL INSTITUTO

Más información

La sesión de marzo de Los Lunes del Instituto de Auditores Internos abordó el desempeño de Auditoría interna a través de la experiencia práctica y metodológica aplicada por Endesa, que compartió con los más de 200 auditores internos participantes, su programa de Aseguramiento y Mejora de la Calidad.

Auditoría Interna del Riesgo Reputacional

LOS LUNES DEL INSTITUTO

Más información

En la sesión de Los Lunes de abril, el IAI España presentó el documento de La Fábrica de Pensamiento 'Auditoría Interna del Riesgo Reputacional'. En ella se abordó qué es el riesgo reputacional y cómo se puede gestionar este riesgo, así como el rol de Auditoría Interna.

Auditoría Continua en el marco de las Normas Globales de Auditoría Interna

LOS LUNES DEL INSTITUTO

Más información

La sesión de mayo de Los Lunes del Instituto de Auditores Internos sirvió como marco de presentación del modelo de Auditoría Continua de Redeia, gestor global de infraestructuras esenciales con cerca de una treintena de auditorías internas de procesos al año.

Impulsa Auditoría Interna: Estrategia y futuro

LOS LUNES DEL INSTITUTO

La sesión de junio de Los Lunes del Instituto de Auditores Internos compartió la experiencia de Auditoría Interna de Sanitas & Bupa en el desarrollo de una estrategia y posicionamiento de la Función, que favorece una influencia activa en la organización y dispone de un equipo global interconectado, preparado para el cambio y en constante desarrollo, innovación y avance en la digitalización.

Más información

¡Inscríbete a las Jornadas de Auditoría Interna!

COLECCIÓN IAI DE ARTE CONTEMPORÁNEO

Más información

Los días 7 y 8 de octubre de 2025 celebraremos nuestras Jornadas Anuales de Auditoría Interna en Ifema – Madrid. Bajo el lema 'El arte de inspirar', el IAI España se convierte en una galería de arte, en la que se exhibirán "obras" de diversas disciplinas y técnicas, con el fin de compartir las ideas más contemporáneas del momento, haciendo un recorrido por las últimas tendencias en la Función.

esfera consejeros

¿CÓMO PUEDO DARME DE ALTA EN ESFERA CONSEJEROS?

Regístrate aquí:

Escríbenos a:
esferaconsejeros@iai.es

Un espacio de análisis, reflexión y conocimiento creado por el Instituto de Auditores Internos de España.

Dirigido a los miembros de la Comisión de Auditoría y al resto de consejeros de nuestros socios corporativos.

IMPULSAMOS LAS PRÁCTICAS DE BUEN GOBIERNO EN ESPAÑA

Instituto de AuditoresInternos de España

Auditoría Interna
REVISTA EDITADA POR EL INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Instituto de Auditores Internos de España.
Santa Cruz de Marcenado, 33 - 28015 Madrid
Tel.: 91 593 23 45

www.auditoresinternos.es