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

www.auditoresinternos.es

40 años Instituto de Auditores Internos de España

NÚMERO 133 | Julio | AÑO 2023

# ESG: llegó la hora de la verdad

La información no financiera ha dejado de ser un cuento para equipararse a las cuentas, a la información financiera.

## Entrevistamos a:

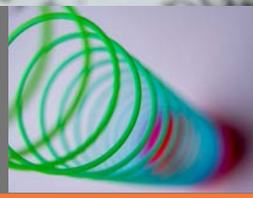
**Alex Grijelmo**

*Escritor y periodista*

**Guía COSO-ACFE riesgo de fraude: una actualización necesaria**

**China nos empuja a repensar el mundo**

**DORA y la función de Auditoría Interna**



# Sumario






40 años Instituto de Auditores Internos de España

**Presidenta:**
Sonsoles Rubio

**Comisión Editorial:**
Gabriela González-Valdés: Directora General
Jesús Lafita: Director Técnico

**Coordinadora Editorial:**
Consuelo Calle
ccalle@iai.es

**Colaboradores:**
Micael Gesto
Julio Ceballos
Ignacio Bazarra
Ángel Navarrete

AENOR ER Empresa Registrada UNE-EN ISO 9001

Santa Cruz de Marcenado, 33 - 28015 Madrid
Teléfono: 91 593 23 45
Fax: 91 593 29 32
iai@iai.es
www.auditoresinternos.es

Diseño y realización:
Blondas de Papel S.L.

# Sostenibilidad en el centro del negocio

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

Aquí estamos de nuevo. Justo en la antesala de las vacaciones de verano. No queremos que os marchéis sin tener otra edición de nuestra nueva revista en vuestras manos. En este número vez hemos abordado en portada un tema que a todos nos ocupa: la información no financiera, sostenibilidad o criterios ESG, como prefiráis llamarlo.

Muchos llevamos tiempo trabajando sobre ello. Y otros, los menos, necesitan pisar el acelerador para estar preparados porque ha llegado la hora de la verdad. Y no hablo solo de contar con adecuados sistemas de control interno de la información no financiera (SCIINF) o con modelos de *reporting* sólidos, como nos exige a casi todos -con diferentes plazos, según tamaño- la Directiva 2022/2464 de Información Corporativa en Materia de Sostenibilidad (CSRD) que -recordemos- aplica a empresas de cierto tamaño en el reporte del ejercicio 2024 y siguientes. Los auditores internos tenemos muchas tareas por delante para que todo funcione a la perfección, como debe ser.

Pero como decía, no me refiero solo a eso. Creo que la clave reside en embeber la sostenibilidad en la estrategia y las operaciones de las compañías. Integrar de verdad, sin adornos superfluos ni exageraciones, porque solo así se podrán evitar las tentaciones de *greenwashing*.

Así que no hay excusas. La información no financiera lleva tiempo escalando a los niveles de la información financiera. Y aunque todavía queden algunos gaps por cubrir, cada vez son menos y más pequeños, y un día habrán desaparecido. Ése es el horizonte al que nos dirigimos, no podemos olvidarlo.

Espero que disfrutéis del resto de artículos y temas que incluye este número, desde ciberseguridad, a fraude, resiliencia operativa o la influencia de China, además de una interesante entrevista con el escritor y periodista Alex Grijelmo.

Disfrutar también -y mucho- de sus merecidas vacaciones.

# Sostenibilidad: De los cuentos a las cuentas

**La información no financiera se está equiparando progresivamente a la información financiera porque la experiencia empírica demuestra que los aspectos ESG generan riesgos e impactos financieros relevantes, positivos y negativos, que influyen en la viabilidad de la compañía.**

Una de las frases que más veces se ha oído en el mundo de la gestión empresarial es la que dice que *"lo que no son cuentas, son cuentos"*. Sin embargo, desde que, en 1997, se crease el *Global Reporting Iniciative* (GRI) con el objetivo sistematizar una batería de indicadores para medir los impactos ambientales y sociales de las empresas, hasta hoy, cuando tanto desde Europa como desde Estados Unidos se han lanzado procesos de *hard law* y de *soft law* sobre el reporte de sostenibilidad, hemos vivido un proceso de casi 25 años con un objetivo claro: equiparar la información no financiera (o de sostenibilidad, o de ESG, o como se quiera denominar) a la financiera. Es decir: los cuentos se querían parecer a las cuentas.

**Alberto Castilla Vida.** *EMEIA ESG Solution Lead & Spanish Country Leader de la práctica de Sostenibilidad y ESG.* alberto.castillavida@es.ey.com
**Alberto Andreu Pinillos.** *Senior Advisor, EY España.* Alberto.AndreuPinillos@es.ey.com

Pero… ¿por qué se está produciendo esta equiparación? La respuesta, en nuestra opinión, es sencilla: los aspectos anteriormente llamados *"No Financieros" (*hoy llamados ESG) generan importantes impactos financieros en el mercado, positivos… pero también negativos. No hay más que echar la vista atrás para darse cuenta de que muchos escándalos corporativos que tuvieron su origen en factores ESG, generaron enormes quebrantos patrimoniales. Por eso es necesario dotar de mecanismos de transparencia que permitan que, cualquiera que financie una empresa (inversores, financiadores, bonistas, etc.), tenga claro el nivel de riesgo que asume al realizar operaciones con ella… en todos sus ámbitos (financieros y no financieros).

Pero este argumento puede llevarse incluso más allá. ¿Cuánto empleo destruyeron estos casos? ¿Cuántos proveedores dejaron de ingresar el importe de sus facturas o perdieron negocios futuros? ¿Qué impacto tuvieron en las cuentas públicas? Definitivamente, los aspectos de sostenibilidad tienen impactos financieros muy importantes para todos los *stakeholders*, no solo para los *stakeholders* (accionistas). Por tanto, para conocer hoy la viabilidad de cualquier compañía es necesario analizar toda la información de la empresa en su conjunto: la financiera y la de sostenibilidad.

## Una equiparación global

Este proceso de equiparación de información se está produciendo a nivel global, porque el capital y las relaciones comerciales son globales. Europa, que quiere liderar este proceso desde 2014 con la Directiva (UE) 2014/95, de 22 de octubre, sobre información no financiera y diversidad, ha aprobado recientemente la Directiva (UE) 2022/2464, de 14 diciembre, conocida popularmente como Directiva Información Corporativa en Materia de Sostenibilidad (CSRD por sus siglas en inglés), que se desplegará a través de los *"European Sustainability Reporting Standards"*, preparados por el EFRAG y publicados en junio por la Comisión para ronda alegaciones. Estados Unidos, también está en ese camino,

después de que la SEC publicase en marzo de 2022 el documento *"The Enhancement and Standardization of Climate-Related Disclosures for Investors".*

Junto a estas iniciativas, hay otras lanzadas por instituciones globales que están avanzando en esta misma dirección con su propio modelo de estándares: la *Task Force on Climate related Financial Disclosures* (TCFD), el *think tank* creado en 2017 para trabajar sobre riesgos climáticos; el *International Sustainability Standards Board* (ISSB), creado en noviembre de 2021 por la Fundación IFRS, que ya ha sacado dos documentos para comentarios, que se apoya en TCFD y en los parámetros de las normas del Sustainability Accounting Standards Board (SASB); o las iniciativas lideradas por *Value Reporting Foundation*, y por el WEF *(WEF IBC's stakeholder capitalism metrics),* que tienen también como objetivo la creación de estándares en sostenibilidad y con las que IFRS está alcanzado también acuerdos para alcanzar un modelo coherente de métricas.

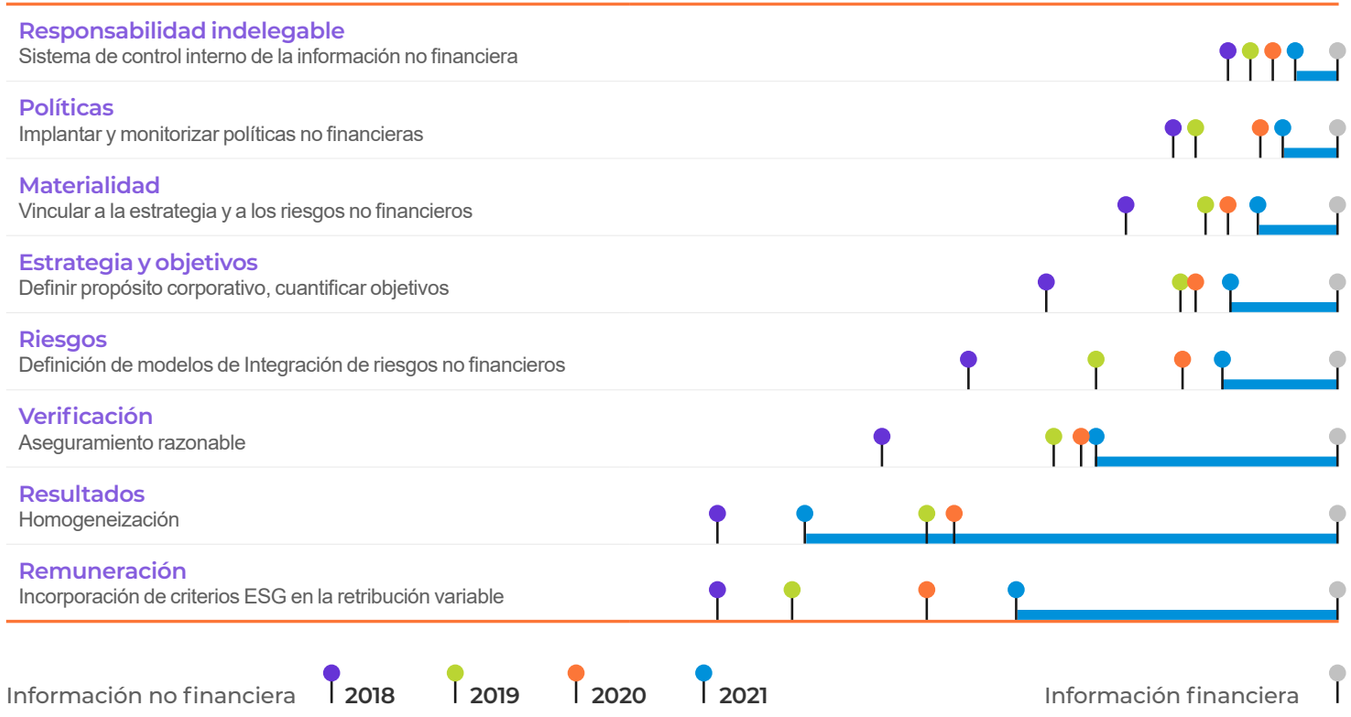
## Retos del consejo de administración

Este proceso, equiparación de las informaciones financiera y de sostenibilidad, tiene un impacto muy destacado para los consejos de administración. La razón es sencilla: aun cuando la legislación actual le confiere al consejo responsabilidades equivalentes en ambas informaciones (tiene que firmar las cuentas, el EINF y que éste forme parte de las cuentas anuales) lo cierto es que los mecanismos de control y supervisión que tiene sobre ambas no están igualmente desarrollados.

En el gráfico adjunto, que se incluye en el *"V Estudio comparativo de los Estados de Información No Financiera (EINF) del Ibex 35"*, hemos analizado cómo ha evolucionado, desde 2018 hasta hoy, la madurez de los principales instrumentos de control y supervisión de la información de sostenibilidad respecto de los de la información financiera, que cuentan con un nivel de madurez muy alto (círculo blanco del gráfico). En el gráfico se aprecia el gap aún existente de la madurez de los principales instrumentos de control y supervisión, como son la existencia de políticas, análisis de materialidad, estrategias y objetivos, gestión de riegos, verificación, homogeneidad de los resultados y criterios de remuneración. La razón de este gap es muy clara. Mientras que, en el caso de la información financiera, los mecanismos de control y supervisión se llevan construyendo desde la aprobación del Plan General de Contabilidad de 1990 en el Real Decreto 1643/1990 de 20 de diciembre, en materia de sostenibilidad esos mecanismos se han empezado a desarrollar desde apenas cuatro años, desde la entrada en vigor de la Ley 11/2018 de Información no Financiera y Diversidad, que obligaba el consejo a firmar el Estado de Información No Financiera (EINF) como parte integrante de las cuentas anuales y del informe de gestión de la compañía, una de las responsabilidades indelegables del consejo.

## MECANISMOS DE CONTROL Y SUPERVISIÓN DE LA INFORMACIÓN FINANCIERA VS INFORMACIÓN DE SOSTENIBILIDAD

### Gap del nivel de madurez entre los mecanismos de ambas informaciones




***Fuente:*** *EY, V Informe Comparativo de los Estados de Información no Financiera (EINF) del IBEX 35.*

## Mecanismos para acelerar el cierre del gap

Por tanto, el reto de la empresa europea, si la UE quiere liderar este movimiento, va a ser cerrar el gap de madurez entre los mecanismos de control y supervisión de ambas informaciones, la financiera y la de sostenibilidad. Y parece claro que la directiva CSRD y los estándares ESRS van a suponer un paso definitivo para cerrar ese gap, porque, entre otros instrumentos, introducen dos palancas que, en nuestra opinión son definitivas.

La primera palanca tiene que ver con el Punto de Acceso Único Europeo (PAUE), una plataforma tecnológica en el que, las empresas afectadas por la Directiva, deberán depositar sus informes de sostenibilidad a través de los formatos de archivo más comunes (XBRL, PDF, XML, HTML, CSV, TXT y XLS), lo que permitirá definitivamente disponer de datos ciertos, homogéneos y la comparables.

La segunda está relacionada con el nivel de aseguramiento requerido para la información de sostenibilidad. En el caso español, después de la Ley 11/2018, se obligaba a las compañías afectadas por ella a realizar una verificación limitada a través de un tercero. Pero la nueva CSRD va un paso más allá y deja abierta la puerta a que la información

de sostenibilidad se someta, a partir de 2028, a los mismos criterios de aseguramiento razonable que la información financiera. Si esto es así, los consejos de administración tendrán que acelerar todos los mecanismos de control y supervisión de la información de sostenibilidad que mencionamos en este artículo, acelerando, sobre todo, la implantación de un Sistema de Control Interno (el SCIINF). Para entender la altura de este desafío, conviene recordar que, en 2021, solo un 9% del Ibex35 contaba con algunos indicadores particulares verificados con aseguramiento razonable.

## Conclusión

**Por tanto, si ya empezamos a ver cuál es la meta final, parece claro que habrá que ir preparándose para llegar en condiciones. Algunas empresas, como los buenos maratonianos, ya han empezado el entrenamiento; otras aún están en proceso de reflexión, quizá pensando que queda tiempo. Cada uno sabrá cuál es la mejor estrategia a seguir, pero los tiempos son claros. ¡A por ello!**

## El nuevo informe de sostenibilidad*

**Calendario de implantación de la Directiva (UE) 2022/2464 de Información Corporativa en Materia de Sostenibilidad** (CSRD por sus siglas en inglés)

AÑO DE REPORTE

### 2025

Para los ejercicios económicos que comiencen a partir del 1 de enero de 2024 **aplica a las grandes empresas ya sujetas a la directiva sobre información no financiera. (NFRD)****

### 2026

Para los ejercicios económicos que comiencen a partir del 1 de enero de 2025 aplica a las **grandes empresas no sujetas a la directiva sobre información no financiera (que cumplan durante dos ejercicios consecutivos dos de tres condiciones:** más de 250 de media de trabajadores empleados, una facturación de 40 millones de euro, 20 millones en activos totales).

### 2027

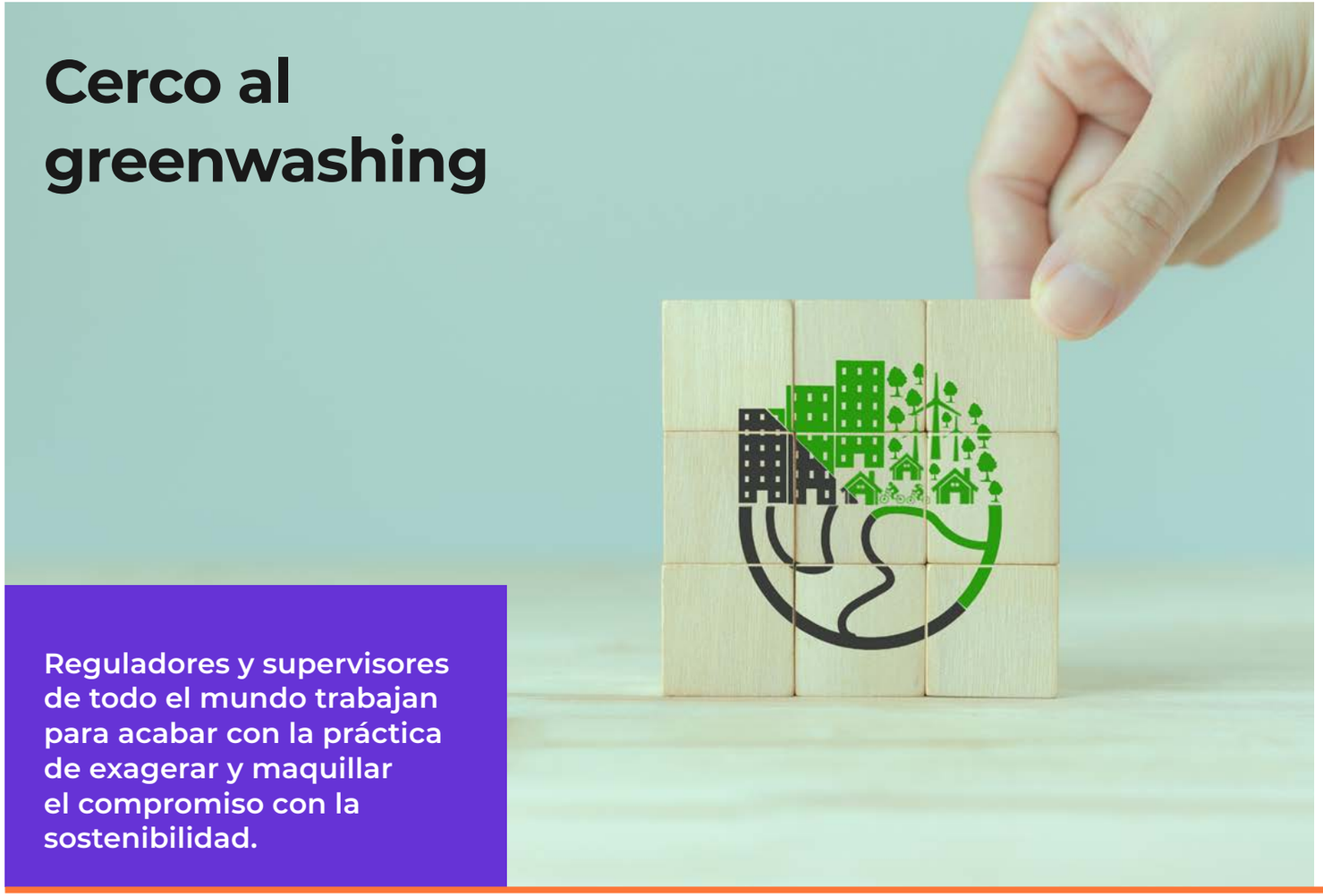
Para los ejercicios económicos que comiencen a partir del 1 de enero de 2026 aplica a **las pymes cotizadas (que no sean microempresas) y otras empresas.**

### 2029

Para los ejercicios económicos que comiencen a partir del 1 de enero de 2028 **aplica a empresas fuera de la UE con sucursales o dependientes.**

** La información recogida en este gráfico puede estar sujeta a cambios en virtud de la Transposición de la Directiva a la legislación española.*
*** NFRD aplica a las grandes empresas de interés público (que superen a fecha de cierre los 500 empleados).*
***Fuente:** EY, basado en Directiva UE 2022/2464 (2023).*

# Cerco al greenwashing



**Reguladores y supervisores de todo el mundo trabajan para acabar con la práctica de exagerar y maquillar el compromiso con la sostenibilidad.**

Grandes reguladores y supervisores internacionales se han puesto todos manos a la obra para acabar con el *greenwashing* (literalmente lavado verde). Europa está siendo muy activa para acabar con una práctica que se ha cuadriplicado en cinco años, cebándose en los aspectos medioambientales -impacto climático, entorno y biodiversidad- y sociales, según datos de RepRisk recogidos en los estudios lanzados hace unos días por los tres supervisores financieros europeos, los ESAs. (2023 Junio).

Antes de repasar algunas iniciativas, convendría distinguir dos tipos de greenwashing: el clásico, exagerar el carácter sostenible o medioambiental de ciertos productos o servicios en las comunicaciones

**Consuelo Calle.** *Instituto de Auditores Internos.*
*ccalle@iai.es*

públicas, equivalente a la publicidad engañosa. Y el greenwashing financiero, que consiste en catalogar incorrectamente, en un tramo superior al que le corresponde, la categoría sostenible de un fondo de inversión u activo financiero (ver los artículos 8 y 9 del Reglamento SFDR[1]. Este segundo tipo de greenwashing fue el caso de la gestora del Deutsche Bank (agosto 2021). Repasamos los hitos.

| | |
|---|---|
| **2023 Junio** | Los **tres principales supervisores financieros europeos, los ESAs -integrados por EBA** (entidades financieras), **EIOPA** (seguros y fondos de pensiones) y **ESMA** (mercados de capitales)- hacen público un informe preliminar sobre el greenwashing tras recabar y analizar evidencias sobre los drivers, claves y riesgos asociados al **greenwashing**. El trabajo, denominado *Call For Evidence* y ordenado por la Comisión Europea, será presentado en un informe definitivo en mayo de 2024. |
| **2023 Marzo** | La **Comisión Europea** presenta la propuesta de *Directiva Green Claims (GCD)* para atajar el *greenwashing* regulando la forma en que las empresas deben comunicar y fundamentar sus compromisos y afirmaciones ecológicos... Las empresas deben aportar pruebas que refrenden sus declaraciones sostenibles o medioambientales. |
| **2023** | El regulador publicitario en ***Reino Unido, Advertising Standards Authority*** (ASA) ha prohibido una veintena de campañas publicitarias al considerarlas prácticas de lavado verde. Afecta a múltiples sectores. Las campañas, que deben cambiarse o dejar de emitirse, utilizaban palabras y frases confusas, vagas o engañosas o comparaciones poco claras. |

[1] *Reglamento 2019/2088 sobre la divulgación de información relativa a la sostenibilidad en el sector de los servicios financiero.*

| | |
|---|---|
| **2023 Abril** | El **regulador de la publicidad en Francia** publica una guía *anti-greenwashing*. El *lavado verde* o *écoblanchiment* ha sido objeto de advertencias y sanciones desde 2007 en las leyes de protección del consumidor. |
| **2022 Octubre** | El regulador financiero británico, FCA, propone un paquete de medidas que incluyen etiquetas de sostenibilidad de productos de inversión y restricciones sobre cómo se pueden usar términos como *'ESG'*, *'verde'* o *'sostenible'*. Busca mejorar la transparencia y confianza de los inversores en los productos de inversión sostenible. |
| **2022 Abril** | La inquietud por el *greenwashing* se eleva a la **ONU**, que anuncia la creación de un grupo de trabajo integrado por 17 expertos internacionales encargado de fijar criterios claros para impedir que multinacionales, ciudades y regiones hagan un lavado verde de su imagen con las promesas contra el calentamiento global. |
| **2022 Febrero** | *ESMA*, el supervisor europeo de los mercados de capitales, incluye acabar con el *greenwashing como una de las prioridades de su plan de trabajo* para el trienio 2022-2024 en el campo de las finanzas sostenible. |
| **2022 Agosto** | El supervisor australiano de los mercados financieros (FSC) regula la difusión de aspectos ligados al clima por parte de gestores de inversión para establecer objetivos y categorías sostenibles claras. La FSC seguía así los pasos de lo que poco tiempo antes había hecho el regulador financiero, ASIC. Singapur adopta medidas similares. |
| **2021 Marzo** | El supervisor y regulador bursátil estadounidense, la ***Securities and Exchange Commission (SEC)***, propone reglas para mejorar el reporting de los riesgos no financieros con indicaciones específicas para evitar nombres de fondos engañosos, a la par que ponía en marcha un grupo de trabajo para identificar y penalizar las prácticas de *greenwashing* en el mundo de las inversiones de ESG. |

## Una práctica extendida

**53%** de los casos analizados, las **empresas no proporcionan información suficiente** para que los **consumidores puedan valorar** si sus **afirmaciones** sobre la **sostenibilidad de sus actividades** y **productos** son **exactas**

**37%** de las afirmaciones incluyen **términos vagos** y **generales** como **"consciente", "ecológico"** o **"sostenible"**

**59%** de los casos, **no aportan pruebas** de fácil **verificación** para respaldar sus **afirmaciones**

**42%** de los casos, **la información** sobre sostenibilidad proporcionada por las empresas **incluían "afirmaciones exageradas, falsas o engañosas** y podrían considerarse prácticas comerciales desleales en virtud de la Directiva sobre prácticas comerciales desleales (UCPD).

***Fuente:*** *Análisis de 2021 de la Comisión Europea Screening of websites for 'greenwashing': Se analizando 344 declaraciones empresariales de sostenibilidad*

**https://ec.europa.eu/commission/presscorner/detail/en/ip_21_269**

| | |
|---|---|
| **2021 Agosto** | La ***SEC*** abre una investigación sobre la DWS, la gestora de fondos del grupo Deutsche Bank, para investigar las acusaciones de que el grupo habría estado remitiendo información incorrecta, al exagerar los criterios de sostenibilidad de una cartera de fondos que se comercializa bajo la categoría ESG. |
| **2021 Agosto** | El **supervisor alemán, BaFin,** abre su propia investigación sobre el engaño verde de DWS. El caso fue denunciado por la responsable de sostenibilidad de la gestora, que fue despedida tras ello. El escándalo forzó la dimisión del CEO de la gestora, Asoka Woehrmann. |
| **2021 Agosto** | La Ley del Clima y Resiliencia en Francia prohíbe expresamente mencionar en ningún producto, servicio o mensaje publicitario expresiones como *"neutro en carbono", "biodegradable"* o *"respetuoso con el medio ambiente"* salvo que esa afirmación esté seriamente fundamentada con información pública y disponible para todos en algún tipo de informe o trayectoria comprobable. La regulación contempla sanciones y con multas proporcionales a la facturación que ese producto o campaña haya generado. |
| **2021 Enero** | La Comisión Europea toma las riendas para acabar con el *greenwashing* tras realizar un análisis de 344 declaraciones medioambientales de empresas y desvelar grave deficiencias: *Screening of websites for 'greenwashing': half of green claims lack evidence.* |

Parece que ahora sí, el *greenwashing* puede tener los días contados.

Amplio análisis del informe de los ESAS en este artículo: **La UE mapea el Greenwashing para erradicarlo.**

(Solo para suscriptores de Esfera. Consejeros. Aun no lo eres? **Solicítanos el alta**)

Miguel Ángel Serrano

***Escritor, CEO y Asesor principal en Landguage Consulting***

***www.landguage.consulting***

Ejércitos de influencers chinos, armados de un código de comportamiento, a la conquista de un mundo plano.

## Fábricas chinas de influencers

El mundo se está convirtiendo en algo más ancho y líquido. Veloz y con poca capacidad de dejar impronta. El conocimiento se deposita como huella de pájaro en la playa: la siguiente ola de saber técnico borrará lo anterior. Lo sólido y profundo parece ir perdiendo el sitio: cada nueva red social insiste en esto. Recortar la duración y confiar en el entretenimiento. Es la fórmula perfecta para que nada permanezca.

Seguro que el lector ha oído hablar acerca de los jóvenes chinos, especialmente mujeres, que intentan abrirse camino como influencers en redes. Es una muestra impresionante de cómo las diferencias culturales determinan el camino que toman las personas. Google publicó un mapa, basado en las búsquedas por país que comenzaban preguntando "Como ser…+ una profesión", que interesa ver.

**En 2022 el estado chino ha publicado un código de cumplimiento, moral y estético.**

**Influencers chinos: La banalidad**

Haz Click en el video de Miguel Ángel Serrano

Los que preguntan desde países hispanohablantes prefieren ser *youtubers* o *influencers*, este último es el caso de España. Y si están tratando de adivinar la profesión preferida según este poco científico método en China…es la de dietista. No tengo una explicación para eso, la verdad, pero tampoco para la preferencia de los españoles y parte de los americanos.

Los *influencers* chinos, en gran número, deben encontrar un tema, hacerlo monetizable, mantener viva una corriente estable de comunicación, buscar su público y marcas que puedan pagarles… es una profesión, que en muy pocos casos produce

ingresos muy cuantiosos. Lo mismo que un *influencer* español, excepto porque el estado chino está planeando limitar sus posibles ganancias. Ser su socio, quieran o no. Y al estar en un sistema de capitalismo de estado, tienen que cumplir con algunas reglas que ni de lejos se nos ocurrirían a los occidentales. Por ejemplo, en 2022 el estado chino ha publicado un código de cumplimiento, moral y estético, que ahorma el resultado de los videos resultantes. Muchos *influencers* impactan en la forma de pensar de personas en etapa de formación, y ya hemos visto cómo consejos de belleza acaban en catástrofe u otros sobre dietética provocan trastornos en los adolescentes. El código chino exige al comunicador un nivel de conocimientos suficiente en temas de alto impacto, como la medicina o el derecho, pero también establece prohibiciones, como hablar mal del sistema comunista, evidentemente, o fomentar, por ejemplo, el desperdicio de comida. Da verdadero miedo.

Miles de jóvenes se lanzan a la aventura en condiciones precarias: es sencillo encontrar imágenes o videos descriptivos de estas fábricas de *influencers*. Se puede ver a decenas de jóvenes, especialmente chicas, en fila, con su anillo de iluminación, produciendo sus pequeñas historias: no solo buscan la protección del número ante posibles agresiones, sino que se sitúan en barrios ricos porque las donaciones que pueden conseguir son mejores cuanto mejor es la zona, y el algoritmo de geolocalización ayuda en eso.

Al reflexionar sobre esto, que es extraño, pavoroso y entristecedor, lo que me asombra es cómo hemos permitido que lo falso, lo artificioso, lo inane, se hayan hecho dueños de nuestro ocio. Llevamos ya mucho tiempo permitiendo que personas sin preparación den consejos de salud, dermatología o empresa, en formatos que nos parecerían intolerables no hace tanto tiempo. Y, además, impulsados de forma opaca por misteriosos algoritmos. Recuerdo mis tiempos de estudiante, cuando la publicidad, por ley, debía estar claramente separada de la información. Y cuando el medio difusor era responsable del contenido.

**Las donaciones que pueden conseguir son mejores cuanto mejor es la zona.**

Contenidos sin interés y uniformados, que ahora, además, pueden ser compuestos por máquinas. La verdadera revolución es desintoxicarse de esto y volver a las aulas, los libros, los expertos y el pensamiento libre y liberador, sin códigos chinos de por medio.

**La verdadera revolución es desintoxicarse de esto**

> **La credibilidad se rompe cuando uno se equivoca y no lo reconoce**

# Alex Grijelmo

*Escritor y periodista. Creador de la Fundéu.*

**Por Ignacio Bazarra**
*Fotos: Ángel Navarrete*

*Les Luthiers, que le conocen bien, le bautizarían como el compositor de palabras. Y la definición no puede ser más acertada para Alex Grijelmo, escritor y periodista, que ama el lenguaje y ha buceado por todos sus entresijos, desde la teoría y la práctica. Doctor en Periodismo, ha sido directivo del grupo PRISA, presidente de la Agencia EFE y creador de la Fundación del Español Urgente (Fundéu), esa plataforma que nos ayuda a saldar dudas para hablar siempre con propiedad. Entre sus libros de lectura obligada para aquellos que quieran hablar y comunicar de forma correcta están "El genio del idioma", "La seducción de las palabras", y, más recientemente, "Propuesta de acuerdo sobre el lenguaje inclusivo". Sus fieles seguidores le disfrutan todos los domingos en la columna "La punta de la lengua" en El País, un periódico en el que trabajó entre 1983 y 2002 en diferentes puestos de responsabilidad.*

**La complejidad no se puede transmitir con simpleza, pero sí con sencillez**

Haz Click en el video de Alex Grijelmo

**Las empresas hoy no solo hacen negocios. Tienen una voz propia, conversan con la sociedad e incluso se convierten en plataformas de comunicación. ¿Cree que comunican bien o tienen aún camino por recorrer?**

En la comunicación entre una empresa y un cliente lo fundamental es elegir el registro en el que nos vamos a entender. Y muchísimas empresas, sin darse cuenta, eligen su propio registro. No el del público, sino el suyo. Si soy un banco, voy a utilizar las palabras de la banca. Si soy una aseguradora, el de las empresas de seguros, y así con muchos sectores que utilizan su registro en lugar de utilizar el vocabulario de tu público. Puede ser por desconocimiento –*"elijo el lenguaje en el que me siento cómodo"*-, porque las palabras significan precisamente lo que yo sé, o bien porque de ese modo transmito la imagen de que soy muy competente en la materia y, así, el que recibe el mensaje se siente empequeñecido.

**¿Cree que debería existir un *"libro de estilo"* de las empresas?**

Hacer un libro de estilo es muy fácil: lo encargas a un experto y ya está. Lo difícil es cumplirlo y poner a alguien que lo asuma como propio y promueva esa cultura en toda la empresa. Que todos se relacionen con él de manera amigable. No es un corsé ni una nueva gramática, debe ser una herramienta para relacionarte mejor con los clientes. Conozco muchos casos de manuales de relación con el usuario que se incumplen. Cuando llegan los auditores dicen: sí, cuentan con un manual de atención al usuario, pero ¿quién vela por el cumplimiento? ¿Dónde está el canal para recoger las quejas de los usuarios? ¿Le ha facilitado el manual al usuario para saber qué derecho tiene y a qué se obliga usted?

**"El auditor interno también tiene cierto sesgo al pensar siempre que debe encontrar algo**

**¿Qué claves le daría para construir ese relato a las empresas? ¿Y a quien redacta un informe de auditoría, por ejemplo?**

En primer lugar, imaginarse al destinario, verlo físicamente, incluso concretarse en una persona que reúna las características del público al que te diriges. En segundo lugar, encontrar el registro adecuado para esa persona. Si usamos tecnicismos propios de nuestro ámbito, que no dicen nada al destinatario, no estamos comunicando. Lo primero para hablar con otra persona es elegir el idioma. Si hablas con un inglés que no sabe español, tienes que utilizar el inglés. Si pretendes obtener algo de esa comunicación, tienes que hablar en el idioma del destinatario.

Finalmente, explicar todo lo que es complejo de una manera sencilla. No simple, porque no se puede simplificar lo complejo. ¿Cómo se consigue eso? Con metáforas. Y no han dado muchísimas muestras en este sentido los científicos durante la pandemia. Oyes hablar al paleontólogo Juan Luis Arsuaga, a la directora del CNIO, María Blasco, o al físico Manuel Toharia y te das cuenta de que utilizan muchísimas metáforas y alegorías para explicar algo que sucede en una probeta, por ejemplo, y logran que les entiendas perfectamente: *“A esta célula le hemos dotado de una espada para que combata a…”*.

*Álex Grijelmo defiende que los altos directivos consulten con sus expertos en comunicación antes de tomar decisiones importantes porque, si no lo hacen, luego son muy difíciles de explicar interna y externamente. “Igual que le consultas al abogado de la empresa. No haces las cosas y luego las consultas a la asesoría jurídica”, explica. Cualquier profesional de la compañía debería recibir formación en comunicación. Todo comunica y construye el relato, desde un informe de auditoría a un anuncio de empleo o una junta de accionistas.*

**Las empresas han asumido que tienen una misión y unos valores hacia la sociedad y, cada vez más, hacia el planeta. Estos aparecen en el frontispicio de su web y sus publicaciones. Luego alguien tiene que vigilar si se están cumpliendo.**

Son palabras grandes, huecas, de un significado muy amplio, como justicia, equidad, democracia, donde caben valores mucho más pequeños. Un tipo de declaraciones tan etéreas que no comprometen a nada, muy al estilo de algunos artículos de la Constitución Española, que son aspiraciones comunes pero que inducen muy poco a exigir su cumplimiento.

**Estamos asistiendo a un profundo debate sobre el Greenwashing. ¿Cuándo se rompe la línea de la credibilidad?**

La credibilidad se puede romper por muchos motivos, arrancando por la mentira. Las mentiras tienen las patas muy cortas y se terminan descubriendo. Además, el público detecta enseguida la incoherencia entre el hacer y el decir. Pero la credibilidad también se rompe cuando alguien se equivoca y no lo reconoce. El error está permitido, pero hay que saber gestionar los errores. Lo que nos diferencia es cómo gestionamos la equivocación: pidiendo perdón, diciendo que nos hemos equivocado, aunque luego no puedes estar equivocándote de forma reiterada. El problema es cuando te obstinas en el error.

> **El error está permitido, pero hay que saber gestionar los errores y no obstinarse ni equivocarse de forma reiterada**

**Los periodistas decimos que no existe la objetividad absoluta porque todos tenemos sesgos y no los podemos ocultar. El auditor aspira también a esa objetividad cuando redacta un informe. ¿Qué herramientas ha utilizado en su vida profesional para evitar esos sesgos?**

Seguramente sean inevitables, pero debemos combatir contra nuestros propios sesgos. ¿Cómo? Con datos y la indicación de la fuente de donde salen los datos. Hay un cierto sesgo del auditor que yo he visto y es el de que siempre ha de encontrar algo. Como si, al no haber encontrado nada, hubiera hecho mal su trabajo. Recuerdo una auditoría del Tribunal de Cuentas que recriminaba en la Agencia

EFE ¡un apunte contable que nos había empeorado el resultado! Yo pensaba: esta gente necesita encontrar algo. Nos pasa como editores: cuando corriges un texto y llegas a la última línea y no has corregido nada, dices, *"yo no aporto nada a este texto, tengo que encontrar algo"*. Hay que tener cuidado con eso.

**Los informes de auditoría y en general los textos jurídicos y contables son muy técnicos. Usted los analizó hace unos años en la Comisión sobre el Lenguaje Jurídico. ¿Cree que habría que meterles cierta narrativa, storytelling, sin perjudicar ese anhelo de independencia y objetividad?**

Es lo más difícil: la interpretación de los datos. Estamos hoy abrumados por la cantidad de información. ¿Pero cómo los interpretamos? Interpretar no es opinar, es encontrar ese contexto que explica los números: averiguar de dónde viene algo, por qué ha sucedido algo y qué consecuencias puede tener. Pero no es juzgar. Cada vez necesitamos más interpretación en este sentido de contexto. En el periodismo y en la auditoría. Anotar una cifra detrás de otra no conduce a nada, hay que ver la evolución. Hay elementos externos que no están en los datos y sin embargo son importantes para explicar eso que ha sucedido. Puedes equivocarte, pero ahí está el valor que aporta el periodista y el auditor.

**Nunca en la historia de la humanidad ha habido tantos datos, nunca se ha escrito y leído tanto. Se impone la lectura en diagonal por falta de tiempo, no pasas de la primera o la última página. ¿Es esto un problema?**

El problema es que no nos enseñan a hacer un resumen ejecutivo. Aprendemos por pura intuición a destacar los puntos fundamentales, como el DAFO que hace una empresa. El cerebro humano funciona así: la atención decae a los pocos minutos. Tiene sentido elegir las 2 o 3 frases que los demás, tu público, van a recordar. Yo no creo que leer en diagonal esté mal. Lo haces cuando lees una sentencia, por ejemplo, pero también un informe de auditoría. Asumes el riesgo porque quien lo ha elaborado ha puesto todos los datos y es su credibilidad la que te da la confianza de poder leerlo en diagonal.

**El valor añadido de una auditoría es encontrar el contexto, la interpretación**

Enrique Sueiro

***Asesor de comunicación directiva***
***www.enriquesueiro.com***

Los avances tecnológicos son tan deseables y necesarios como una comunicación que no pierda su condición de humana.

## Inteligencia humana, comunicación y negligencia artificial

Inteligencia como sustantivo rima con adjetivos como emocional, creativa y contextual, pero no con artificial. Del latín *intus legere* (leer dentro), la persona inteligente es capaz de penetrar en dimensiones profundas de la realidad. Esta mirada interior se complementa con otra exterior magistralmente descrita por Chesterton cuando decía que *"thinking means connecting things".* Si pensar consiste en relacionar (bien) cosas (relevantes), qué difícil imaginar semejante pericia en una máquina, entre otras razones, porque las cosas importantes no son cosas.

En el caso de las realidades entrañablemente humanas, poliédricas por definición, menudo desafío calibrar el impacto del miedo, la compasión, el resentimiento, la vanidad, el cariño, la incertidumbre, el amor, la ambición, el honor, la dignidad… ¿Cómo medir todo lo mucho omitido que incluyen los puntos suspensivos anteriores a esta frase?, ¿qué algoritmo es fiable para valorar el compromiso?

El fascinante mundo de la comunicación personal y directiva tiene mucho de ciencia y, aún más, de arte. Desde luego, no es una ciencia exacta porque, gracias a Dios, los seres humanos no somos exactos. ¿Qué métrica mide con precisión el grado de libertad personal y sus consecuencias ejecutivas?, ¿cómo se gestionan las percepciones, necesariamente subjetivas y cambiantes?

Recordemos, porque ya las hemos vivido, situaciones de crisis múltiple (económica, emocional, social…) como una pandemia o un atentado terrorista de gran impacto, como el 11-S. ¿Qué inteligencia no humana es capaz de

**¿Cómo se gestionan las percepciones, necesariamente subjetivas y cambiantes?**

responder con más tino que el entonces alcalde de Nueva York cuando le formularon una pregunta tan concreta como imposible de contestar a las pocas horas de aquel día tan triste de 2001.

- ¿Sabe el número de bajas *(casualties)*?

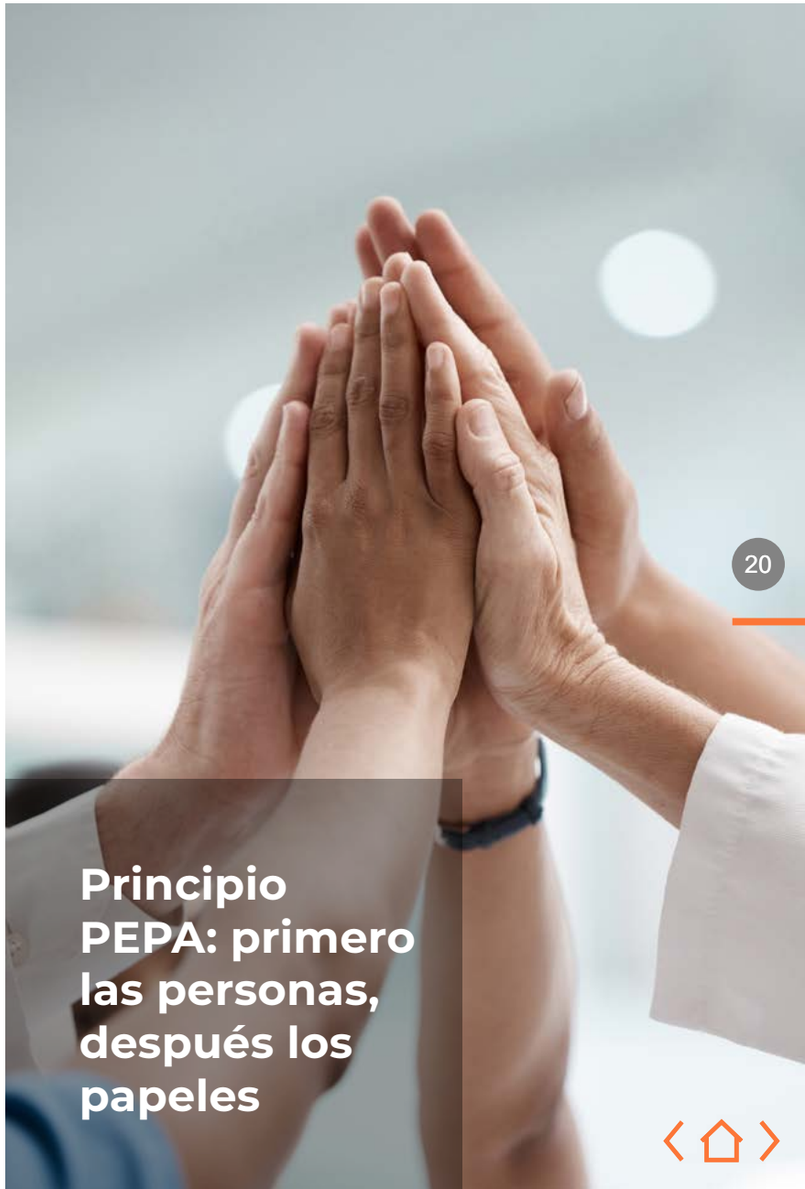
- Ahora nuestra prioridad son las víctimas y sus familias. No debemos especular con la cifra que, cuando la conozcamos, será muy superior de lo que podemos soportar.

## El resultado de no pensar podría ser un fallo por negligencia artificial.

Dudo que el entonces lúcido Rudolph Giuliani pudiera verse superado hoy en comunicación efectiva por el más sofisticado sistema artificial. Quienes hemos padecido atentados terroristas y vivimos para contarlo somos, quizá, más conscientes de lo difícil que resulta comunicar cuando es necesario hacerlo, aunque no dispongas de datos. Es la hora de la prudencia y de gestionar emociones. También es el momento TV (temple y visión) para dar la cara y poner voz con serenidad, elegancia y claridad. Es insensato hacer predicciones categóricas, pero sí es prudente extremar la cautela si alguien elude la responsabilidad de pensar y delega la sensibilidad de comunicar. El resultado bien podría ser un gran fallo multiorgánico por negligencia artificial.

Nadie sensato discute la bondad de los avances tecnológicos, como tampoco la necesidad de las normas de tráfico y la legislación en la sociedad. Pero las leyes no están, en su sentido más profundo, para la formalidad de cumplirse, sino para ayudar a las personas. Adelantar en una curva no está mal porque lo prohíba la DGT, sino porque ponemos en peligro nuestra vida y la de otros (y por fortuna, además, la DGT lo sanciona).

Un falso progreso ciega a muchos con el señuelo de estar a la última a costa de dejar de estar a la primera. No perdamos el norte ni olvidemos que es más importante la brújula que el cronómetro. Para ello puede orientar el Principio PEPA: primero las personas, después los papeles.



# Una actualización necesaria para abordar el riesgo de fraude

**La reciente actualización de la "Fraud Risk Management Guide" trae novedades importantes y enfatiza la necesidad de adoptar programas integrales para combatir el fraude.**

La *Fraud Risk Management Guide* publicada por COSO y ACFE en 2016 fue un hito de especial relevancia en la lucha contra el fraude corporativo y sentó las bases de un enfoque holístico, basado en programas consistentes con el COSO 2013 *IC Framework.*

De esta forma, el enfoque integral que plantearon COSO y ACFE puso de manifiesto la necesidad de crear funciones especializadas en las organizaciones para impulsar el conjunto actividades destinadas a combatir el fraude: la evaluación de riesgos, el diseño de políticas, procedimientos y controles (preventivos y detectivos), las investigaciones, las acciones de remediación y la monitorización continua de los programas.

**Marisa Yepes Martínez.** *Socia, KPMG Forensic.* *myepes@kpmg.es*
**Juan Arenas González.** *Director, KPMG Forensic.* *jarenas@kpmg.es*

Con carácter general, el enfoque de gestión integral del riesgo de fraude que propusieron COSO y ACFE en 2016 continúa siendo una asignatura pendiente en las organizaciones españolas. Es difícil encontrar empresas que cuenten con una función específica encargada de gestionar de manera integral el riesgo de fraude.

No obstante, a diferencia de lo que ocurría en 2016, hoy encontramos bases sólidas en los equipos de auditoría interna para promover la implantación de funciones antifraude. La reciente actualización de la *Fraud Risk Management Guide* supone una estupenda *"excusa"* para ponernos manos a la obra y adoptar el enfoque holístico que precisamos para combatir el fraude con eficacia.

## El coste del fraude

**3.600 $ millones de dólares fueron las pérdidas por fraude en 2022**

**5% de los ingresos anuales es lo que se lleva el fraude**

**1,7 $ millones de dólares fue la pérdida media**

**21% de los casos de fraude perdieron más de un millón de dólares**

***Fuente:*** *Report to Nations 2022 de la Asociación de Examinadores en Certificados de Fraude Certificados (ACFE).*

## La necesidad de actualizar la guía

La actualización de la *Fraud Risk Management Guide* era necesaria y viene a dar respuesta a importantes cambios acaecidos desde 2016.

Además de las novedades regulatorias, se han producido acontecimientos que han afectado al entorno en el que operan las empresas. La pandemia global ha propiciado nuevas formas de relacionarnos y un uso intensivo del trabajo en remoto, la irrupción de los cripto-activos, el incremento de las transacciones digitales, los nuevos modelos de negocio desarrollados exclusivamente a través de la red, etc. dibujan un escenario cambiante que favorece la aparición de nuevos tipos de fraude basados en mecanismos cada vez más sofisticados.

En este contexto, nos gustaría destacar los siguientes tres elementos de la actualización de la guía:

1

### La disuasión como elemento clave en la lucha contra el fraude

La implementación de un sistema de gestión de riesgos integral que se comunique a toda la organización y que cuente con el compromiso del Consejo de Administración y la Alta Dirección es esencial para que la “oportunidad percibida” se vea mitigada, dificultando de esta manera que el fraude llegue a producirse.

Por tanto, la generación del efecto disuasorio incide en gran medida en la efectividad global del sistema de gestión de riesgo de fraude, incluso cuando otros elementos del programa no alcancen los mismos niveles de efectividad.

2

### La necesidad de reforzar los elementos del programa utilizando Data Analytics

La inclusión de Data Analytics como uno de los puntos transversales a todos los principios de la guía resulta clave. El incremento de las transacciones digitales y el consiguiente aumento de la disponibilidad de datos estructurados facilita su uso para mejorar la gestión de los riesgos de fraude. Según un estudio conjunto realizado por ACFE y SAS la tecnología juega un papel clave en la lucha contra el fraude. Más de la mitad de las organizaciones utilizan sistemas de detección de fraude basados en la tecnología y se espera que el uso de estas técnicas crezca de forma notable en los próximos años.

En esta línea, el diseño, implementación y sofisticación de controles y alertas de fraude de las organizaciones debe ser más dinámico y eficiente. Por ello, disponer de recursos dedicados con capacidades de análisis de datos en la función de gestión de riesgos de fraude permitirá a las organizaciones una mejora en la monitorización, adaptación de controles, evaluación de la efectividad y retroalimentación del sistema.

3

### Una función especializada

Por último, creemos importante señalar que las funciones de control interno y gestión de riesgo de fraude están relacionadas y se apoyan mutuamente, pero tienen sustanciales diferencias. Como apunta la guía, buena parte de los procedimientos de control interno pueden ser adecuados para garantizar la exactitud de la información financiera, pero no por ello van a ser suficientes para mitigar el riesgo de fraude.

Es por este motivo que, para que sean eficaces, las funciones antifraude deben incorporar profesionales especializados, que conozcan las tendencias y estén al tanto de las principales novedades regulatorias y las mejores prácticas en la materia.

## Fraude: datos a tener en cuenta

**12-18 meses** de media es lo que se tarda en ser detectado

Operaciones, contabilidad y ventas concentran el **38%** de los casos de fraude

**42%** se detecta a través de denuncias por parte de los empleados

**8%** de los fraudes implican el uso de criptomonedas

**16%** de los casos fue detectado por Auditoría Interna

**40%** de los fraudes se llevan a cabo a través del email

***Fuente:*** *Report to Nations 2022 de la Asociación de Examinadores en Certificados de Fraude Certificados (ACFE) .*

En definitiva, esta actualización de *Fraud Risk Mangement Guide* era necesaria porque viene a plantear soluciones ante los nuevos retos que afrontamos, en entornos cambiantes y cada vez más complejos. No se trata únicamente de la ética empresarial que a raíz de las nuevas regulaciones en materia de ESG y Compliance está promoviendo grandes cambios en las empresas. También es una cuestión de responsabilidad con los resultados y, en este sentido, es importante que la alta dirección conozca que combatir el fraude de manera sistematizada va a generar importantes ahorros a la organización.

# Puntos clave de la nueva guía

El fraude no es estático. En los últimos años, ha experimentado un salto cuantitativo, pero sobre todo cualitativo, en formas, procedimientos, herramientas y tecnologías utilizadas tanto para la comisión del delito como para la detección del fraude. Era necesaria una puesta al día de los marcos de referencia para atajar esta importante lacra empresarial. Y sin duda, una de las referencias más relevantes es la Guía COSO de gestión del riesgo de fraude, lanzada por primera vez en 2016 y revisada y actualizada el pasado 2 de mayo de 2023.

**Consuelo Calle.** *Instituto de Auditores Internos.*
*ccalle@iai.es*

## Mecanismos de control

La **PRESENCIA DE MECANISMOS DE CONTROL** se asocia con:

**MENOS** pérdidas por fraude

**MÁS RÁPIDA** detección

Casi **LA MITAD** de los casos de fraude mostraron:

**Ausencia** de controles internos — 29%

**No funcionaron** los controles existentes — 20%

**81%** de las compañías que sufrieron fraude **modificaron** posteriormente sus controles

**75%** reforzó los procedemientos de control

**64%** aumentó la monitorización proactiva con analítica de datos

***Fuente:*** *Report to Nations 2022 de la Asociación de Examinadores en Certificados de Fraude Certificados (ACFE)*

**El fraude es un riesgo latente que impacta muy negativamente en la imagen y reputación corporativa**

A continuación, resumimos los principales puntos que recoge la guía, elaborada por COSO junto a la principal organización que certifica a los expertos en fraude, la *Association of Certified Fraud Examiners* (ACFE).

El documento proporciona un marco integral para que las organizaciones fortalezcan sus prácticas de gestión del riesgo de fraude, un problema que afecta (o puede afectar) a organizaciones de todos los sectores -caso del fraude en los estados financieros-, aunque, por su naturaleza, algunos sean más proclives que otros a ciertos tipos de fraude, caso de apropiación indebida de activos o corrupción. La guía pone énfasis en que una gestión efectiva del fraude requiere de un enfoque integral y que incluya estrategias proactivas de prevención, detección y respuesta al fraude.

## Cinco principios

COSO presenta cinco principios fundamentales que deben sustentar los esfuerzos de gestión del riesgo de fraude de una organización y que son consistentes con los componentes del marco COSO de Control Interno.

**Establecer una estructura de gobierno del riesgo de fraude**

### 1 ENTORNO DE CONTROL

Las organizaciones deben demostrar su compromiso con la gestión del riesgo de fraude asignando responsabilidades, estableciendo líneas claras de comunicación e integrando la gestión del riesgo de fraude en el marco más amplio de gestión del riesgo empresarial.

**Evaluar el riesgo de fraude**

### 2 EVALUACIÓN DEL RIESGO

Es esencial identificar y evaluar los posibles riesgos de fraude para determinar su probabilidad y el impacto potencial. Este proceso implica evaluar tanto factores internos como externos, así como comprender las vulnerabilidades únicas de la organización.

**Diseño e implementación**

### 3 ACTIVIDADES DE CONTROL

Las organizaciones deben desarrollar e implementar un conjunto sólido de sistemas de control adaptados para abordar los riesgos de fraude identificados. Estos controles deben actualizarse, monitorearse y probarse regularmente para evaluar su efectividad.

**Realizar investigaciones y acciones correctivas**

### 4 INFORMACIÓN Y COMUNICACIÓN

Cuando se sospeche o se detecte fraude, las organizaciones deben responder de manera rápida y adecuada. Esto implica realizar investigaciones exhaustivas, tomar las acciones correctivas necesarias y considerar las consecuencias legales y de reputación.

**Monitorear el riesgo de fraude y el cumplimiento**

### 5 MONITORIZACIÓN

Monitorización continua es fundamental para garantizar la efectividad del programa de gestión del riesgo de fraude de una organización. Revisar regularmente las actividades de control, evaluar los indicadores de fraude y estar al tanto de los riesgos de fraude emergentes contribuyen a reducir el riesgo de sufrir algún caso de fraude.

# Ciberseguridad: atención a NIS2 y a la cadena de suministro

**La red de proveedores y partners se ha convertido en el principal objetivo de los ciberdelincuentes. La Directiva NIS2 exige un control más estrecho.**

Un total de 188.820 incidentes gestionados por el Incibe en 2022, un 8,8% más que en 2021. De ellos, un 38% fueron clasificados con un grado "alto" de peligrosidad y un 1,8%, con grado *"muy alto"*. La mayor parte de estos incidentes (52%) tuvieron como destino a empresas y tenían como objetivo principal la captura de datos. Los llamados operadores esenciales o infraestructuras críticas, es decir, todo aquello que tiene que ver con los servicios esenciales como luz, agua… sufrieron 546 incidentes, concentrados especialmente en el sector de energía (37%) y de transporte (22%). En estos casos, por su sensibilidad, el nivel de peligrosidad era más elevado: 31% "alto" y 21% "muy alto".

**Consuelo Calle.** *Instituto de Auditores Internos.*
*ccalle@iai.es*

Todos estos datos[1] reflejan la creciente amenaza que suponen los ciberataques para la sociedad, las empresas y los estados en general, como comentó en su intervención en el **Foro de Expertos** de junio **Marina Rodríguez Díaz**, Jefa de la Unidad de Ciberseguridad y Desinformación del **Departamento de Seguridad Nacional** de Presidencia del Gobierno. *"La ciberseguridad está más allá de quien gobierna y es algo que nos involucra a todos, al gobierno central, a las comunidades autónomas y a las administraciones locales"*, dijo tras explicar la estructura y la estrategia de Seguridad Nacional, para a continuación adentrarse en algunos aspectos relevantes de la nueva regulación de ciberseguridad que llegará en 2024, con la transposición a la normativa española de la **Directiva NIS2**[2].

**El riesgo de la cadena de suministro crece con la integración de componentes y servicios en nuevos productos**

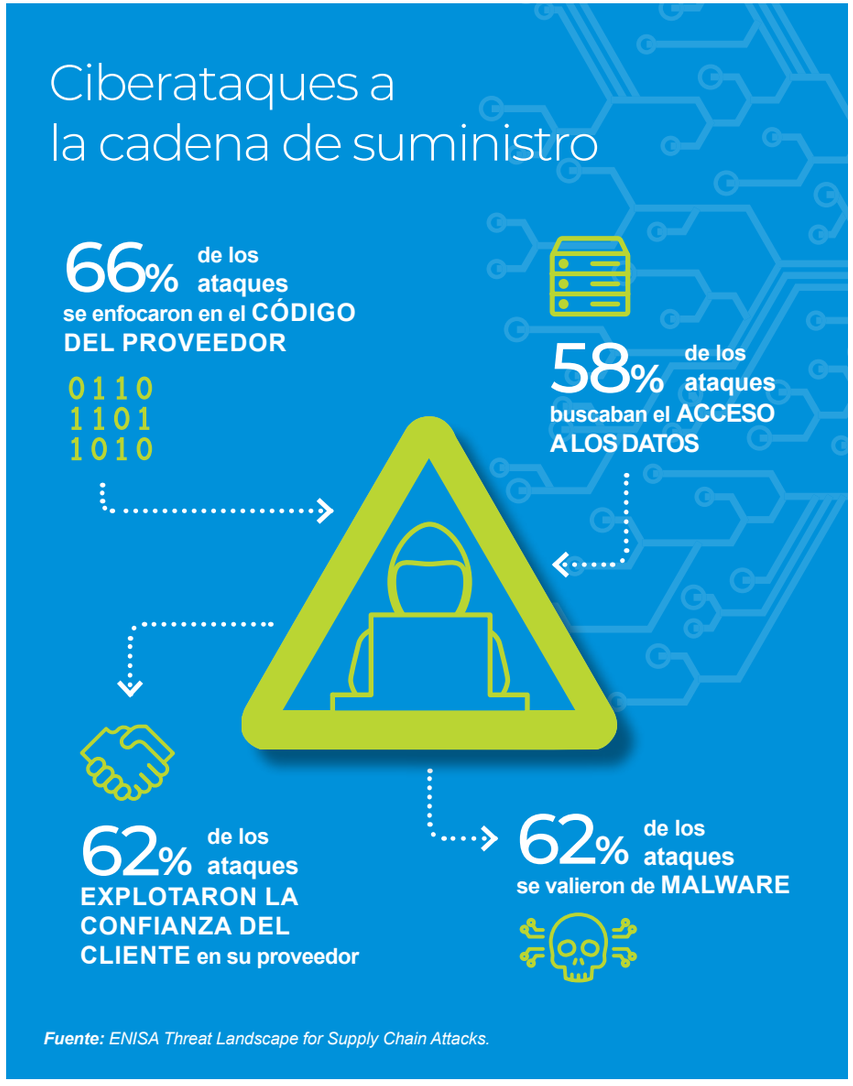
Y una de las novedades más importantes que introduce la directiva es la obligación de vigilar de cerca los riesgos de ciberseguridad de la cadena de suministro, que se ha convertido en el principal objetivo[3] para los ciberdelincuentes lo que amplía en enormemente el perímetro de vigilancia en términos de ciberseguridad. Ya no solo es la empresa sino todo su ecosistema de *partners* y proveedores. *"Con frecuencia son el eslabón más vulnerable, además de conformar un perímetro casi infinito por el creciente volumen de interacciones que tienen las empresas con sus ecosistemas"*, explicaba Marina.

La ciberseguridad de la cadena de suministro, especialmente la derivada de la dependencia de software, ocupa el primer puesto en el ranking de las top 10 ciber amenazas para 2030 apuntadas por la Agencia Europea de Ciberseguridad (Enisa)[4]. Las identifica como *"ciber amenazas que pueden afectar a los servicios e infraestructuras de la Unión Europea (UE) y a la capacidad de la*

## 10 principales ciberamenazas para 2030


***Fuente:*** *ENISA Foresight Cybersecurity Threats for 2030*

[1] ***Incibe.*** *Informe Balance de Ciberseguridad en 2022. (Abril 2023).*
[2] ***Unión Europea.*** *Directiva (UE) 2022/2555, conocida como NIS2. (Diciembre 2022).*
[3] ***Red Seguridad.*** *La cadena de suministro se ha convertido en el principal objetivo para los ciberdelincuentes (Junio 2023).*
[4] ***Enisa.*** *Identifying emerging cyber security threats and challenges for 2030. (Marzo 2023).*




*sociedad europea y a la seguridad de sus ciudadanos"*. Uno de los casos más recientes y conocidos de este tipo es el que sufrió en 2021 la energética Solarwind, que comprometió al Departamento del Tesoro de Estados Unidos[5].

Respecto a la cadena de suministro, la agencia europea destaca que este es riesgo seguirá creciendo por la *"mayor integración de componentes y servicios en nuevos productos"* y los cada día más rápidos *"ciclos de lanzamiento de productos"*. Todo ello conduce a un *"aumento considerable de la programación basada en componentes, que llevará a una reutilización del código y el uso de programas y bibliotecas de código abierto"*. En otras palabras, que los ciberataques podrían fluir rápidamente a través de las cadenas de suministro replicando modelos y códigos. *"Y aunque algunos de estos componentes serán escaneados regularmente para detectar posibles vulnerabilidades, la combinación de software, hardware y código basado en componentes creará interacciones e interfaces no supervisadas"* por donde se pueden colar fácilmente los *hackers*, continúa Enisa en su informe. Esta alerta de riesgos para la cadena de suministro global puede tener motivaciones económicas, pero también políticas o de espionaje y causar una gran disrupción en toda la compañía, tanto mayor cuando más grande, compleja y mayores interconexiones tiene esa cadena de suministro, tal y como expone Enisa[6] en un informe específico sobre esta cadena de valor.

Los datos recopilados por la Agencia Europea de Ciberseguridad, tras analizar múltiples de estos ataques, apuntan pistas sobre dónde y cómo actuar de forma prioritaria. Seis de cada diez los ataques se aprovecharon de la confianza del cliente con el proveedor; casi siete de cada diez se enfocaron en el código del proveedor; seis de cada diez buscaban el acceso a los datos y se valieron de malware para llevar a cabo el ciberataque.

[5] ***El País.*** *Anatomía del gran ciberataque que ha comprometido el corazón de la Administración de EEUU (Diciembre 2020).*
[6] ***Enisa.*** *Threat Landscape for Supply Chain Attacks (Julio 2021).*

La Directiva NIS2 aborda esta necesidad de vigilar y supervisar *"la seguridad de la cadena de suministro y las relaciones con proveedores"* para evitar que se convierta en un coladero de ciberataques.

La norma, que revisa y amplía la anterior Directiva NIS, amplía el ámbito de aplicación para abarcar *"organizaciones medianas y grandes de más sectores críticos para la economía y la sociedad, incluyendo proveedores de servicios públicos de comunicaciones electrónicas, servicios digitales, gestión de aguas residuales y residuos, fabricación de productos críticos, servicios postales y de mensajería, así como a las Administraciones Públicas"*. Como nos recordó en el Foro de Expertos Marina Rodríguez Díaz, esto atañe en España a la Administración General del Estado, las Comunidades Autónomas y la administración pública a nivel local. Estas últimas cuentan con sistemas de control menos robustos que las grandes empresas y tiene una mayor tendencia a externalizar los servicios de ciberseguridad con expertos externos. Además, la administración, al igual que las empresas, ha pisado a fondo el acelerador de la digitalización en los últimos años y ahora permite a los ciudadanos realizar múltiples gestiones -si no casi todas- a través de Internet.

*"El objetivo de NIS 2 no es reaccionar sino prevenir, adelantarse para estar preparado"*, insistió la Jefa de la Unidad de Ciberseguridad y Desinformación, tras recordar que la directiva persigue armonizar la normativa entre los estados miembros y establecer una mayor cooperación entre las autoridades europeas y promoción de la colaboración público-privada en cuestiones de ciberseguridad.

La transposición de la Directiva NIS 2 a la normativa española, que está previsto se lleve a cabo en 2024, fecha tope que establece Bruselas, exigirá modificar el **Real Decreto Ley 12/2018**[7] **y el RD 43/2021**. Además de las novedades ya citadas, la nueva directiva incluye los *"sectores críticos"*, un nuevo concepto que aglutina los sectores de gestión de residuos, aeroespacial, proveedores y fabricantes de servicios digitales, sector alimentario (producción, transformación y distribución), servicios postales y los dedicados a la generación y distribución de sustancias y productos químicos. Se introducen más requisitos de seguridad en las organizaciones -privacidad desde el diseño, obligación de cifrado, respuesta a incidentes, certificación de servicios, sistemas y/o productos, etc.



Accede a más información sobre la Directiva NIS en el Lunes del IAI: **Ciberseguridad: regulación europea y el papel de Auditoría Interna**

[7] ***BOE.*** *Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. (2018)*

## Ciberseguridad: tendencias clave

1. ATRIBUCIÓN DE RESPONSABILIDAD AL CONSEJO DE ADMINISTRACIÓN
2. LA IMPORTANCIA DE LA CADENA DE SUMINISTRO
3. LA GOBERNANZA INTERNA DE LA CIBERSEGURIDAD COMO ELEMENTO CLAVE
4. PLANES DE CONTINUIDAD
5. EL CONTROL DE LAS AUTORIDADES SE INCREMENTA: SANCIONES,COSTE REPUTACIONAL
6. CENTRALIZACIÓN DE PROCESOS Y PERSONAS
7. CERTIFICACIÓN COMO ELEMENTO CENTRAL
8. CUMPLIMIENTO NORMATIVO: FUNCIÓN LEGAL DE CIBERSEGURIDAD
9. COMUNICACIÓN INTERNA (CONCIENCIACIÓN) Y EXTERNA
10. AUTOREGULACIÓN COMO SOLUCIÓN ANTE LA FALTA DE RESPUESTAS

***Fuente:*** *Presentación de los Lunes del IAI, Mayo 2021. Vicente Moret Millás: letrado de las Cortes Generales*

# DORA y la función de Auditoría Interna

**La normativa de resiliencia operativa digital es un reto complejo para el sector financiero, que debe prepararse con antelación para reforzar sus capacidades ante potenciales eventos disruptivos.**

Vivimos en una sociedad de constante cambio e incertidumbre. Los usuarios cada vez demandan mejores servicios (innovación), que sean ágiles y rápidos (inmediatez) y que permitan su uso desde cualquier lugar (movilidad).

Si particularizamos en el ecosistema financiero, cada día aparecen nuevos actores y modelos de negocio que han acelerado la transformación digital e incrementando el uso de la tecnología por parte de las entidades. La tecnología actúa como palanca y acelerador en los procesos de transformación digital, y su uso da lugar a un nuevo escenario de mayor exposición a riesgos que las compañías deben gestionar en su día a día.

**Micael Gesto.** *Socio de Risk Advisory de Deloitte en España*
*mgesto@deloitte.es*

El incremento del riesgo tecnológico y el incremento de los incidentes graves ha generado preocupación en el sector y en los organismos reguladores y supervisores durante los últimos años[1].

La Ley de resiliencia operativa digital (DORA)[2] es parte de un paquete normativo mucho más amplio que abarca múltiples campos de las finanzas digitales y que ha sido desarrollada por la Comisión Europea con el fin de reforzar la resiliencia del ecosistema financiero. El objetivo es robustecer las capacidades de las entidades para hacer frente ante un potencial ataque o cualquier evento que pueda derivar en una disrupción en los servicios prestados a los usuarios.

DORA constituye un conjunto de medidas uniformes que permiten establecer un marco de actuación común en todo el ecosistema financiero y su ámbito de aplicación se estructura en 5 grandes bloques:

- Gestión de los Riesgos TIC.
- Gestión de incidentes TIC.
- Testeo de la resiliencia operativa.
- Gestión de riesgos de externalización.
- Información e inteligencia sobre amenazas.

## Visión global de los requerimientos de DORA

**Cinco ámbitos de gestión del Riesgo TIC**


***Fuente:*** *Deloitte*

Adicionalmente, la normativa incluye un régimen sancionador y mayores atribuciones a los supervisores, lo que supone un componente importante de riesgo regulatorio y potencial impacto financiero en caso de incumplimiento que también se debe considerar en el modelo de gestión de riesgos de las entidades.

[1] ***Deloitte.*** *El estado de la ciberseguridad en España.*
[2] *Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero.*

Cumplir con DORA es un reto para las entidades y supone la involucración de muchas áreas dentro de la organización. Auditoría Interna, como actor ubicado en la tercera línea de defensa de la entidad, debe jugar un papel relevante ofreciendo una visión independiente del estado de cumplimiento de la norma por parte de la entidad y ofreciendo una visión independiente de la exposición a los riesgos en términos de resiliencia.

**El 93,75% de las empresas tuvieron al menos 1 incidente crítico de seguridad en el 2022[3].**

La mayor involucración de la alta dirección es un aspecto clave de la norma, por ello, es fundamental promover un cambio de cultura en la organización y ofrecer en tiempo y forma información clara y objetiva de la situación de la entidad para el proceso de toma de decisión considerando aquellos aspectos que impactan en la resiliencia de la entidad. Auditoría Interna reporta directamente a los principales órganos de gobierno de las entidades y deberá ayudarles a entender si los principales riesgos asociados están siendo gestionados adecuadamente por la organización, así como, levantar cualquier aspecto que pueda suponer un riesgo.

Si se profundiza en la norma, hay múltiples requisitos donde la función de Auditoría Interna podría tener un rol relevante. Se establece la necesidad de realizar auditorías periódicas TIC y revisiones cuando se produzcan modificaciones significativas en la infraestructura TIC tecnológica y realizar una auditoría periódica del Marco de Control TIC por un auditor preparado.

Un elemento clave para conocer las capacidades de resiliencia de la entidad es el *testing:* probar y evolucionar nuestros procesos a medida que identificamos aspectos que no funcionan como se espera. DORA refuerza los requerimientos de *testing* y exige disponer de planes de pruebas adaptados a cada entidad en función de su tamaño, negocio y perfil de riesgo. La norma especifica que las pruebas deben realizase de forma independiente, por tanto, los nuevos requerimientos pueden impulsar y reforzar la función de Auditoría Interna.

Aunque DORA entró en vigor el pasado enero, actualmente, falta más de un año y medio para su aplicabilidad. Los dos años que el regulador ofrece a las entidades para su adaptación muestran la complejidad y el gran impacto que esta supone para las entidades. Es fundamental empezar a trabajar en identificar cuales son los potenciales gaps actualmente y desarrollar planes que permitan adaptarse y llegar a tiempo a enero de 2025.

## Implicaciones estratégicas para la Alta Dirección de las entidades financieras

### **ESTRATEGIA** EN TORNO A LA RESILIENCIA

Las nuevas obligaciones requerirán un **cambio de mentalidad de la alta dirección**, que tendrán la tarea de fortalecer la resiliencia de su empresa frente a interrupciones digitales inesperadas de una manera dinámica que responda constantemente a la evolución de las amenazas y vulnerabilidades.

1. **El cambio de enfoque** que trae consigo el concepto **de "resiliencia operativa"**
2. **Refuerzo de la rendición de cuentas de los Comités Ejecutivos** en torno a la resiliencia operacional
3. Impacto sobre las **estrategias de externalización**
4. **Influencia de la resiliencia operacional en la toma de decisiones de inversión** a nivel ejecutivo
5. **Obligaciones recurrentes que impulsarán la evolución de la gestión de la resiliencia** a lo largo del tiempo

***Fuente:*** *Deloitte. El estado de la ciberseguridad en España[3].*

# Repensar el mundo

Lejos de americanizarse, el mundo se *"achina"* cada vez más. Tenga o no relaciones con China, ninguna empresa debe perder de vista lo que ocurre en el gigante asiático porque, de una forma u otra, acabará impactándole.

El fin de la pandemia nos ha despertado en un mundo que no se parece demasiado al remanso de paz, bienestar barato, consumo creciente, abundancia material, energía fácil y dominación occidental en el que creíamos vivir. El reciente ascenso y renovada pujanza de China nos obliga a tomar conciencia de que entramos en la fase final de un ciclo histórico – 150 años – de dominación mundial occidental y nos empuja a prestar más atención a lo que está ocurriendo en el otro lado del mundo. Comprender China es crucial para comprender el futuro.

Asia, con China a la cabeza, está a punto de tomar la delantera a un orden geopolítico en el que han predominado los atributos occidentales durante los dos últimos siglos. En 2030, Asia concentrará dos tercios de la clase media mundial. Más allá del afán de conocimiento, empatía cultural o la sana curiosidad, es una cuestión de competitividad: para

**Julio Ceballos.** *Especialista en internacionalización, estrategia de mercado y negociación comercial en China. Autor del del bestseller "Observar el arroz crecer. Cómo habitar un mundo liderado por China"*
*www.julioceballos.com*

# El poder de China en cifras

**1.400** millones de habitantes

**2º país** más poblado del mundo

**PIB: 17,1 €** billones €

**2º** mayor país del mundo

**39** años de edad media

Solo un 26% tiene + de 55 años


de la población vive ya en áreas urbanas


de la población tiene acceso a Internet y utilizan el navegador chino Baidu


de la población tiene un móvil


Produce el 20% de los vehículos de todo el mundo

**13,2 €** billones de deuda pública (77% del PIB)

**12.169 €** de renta per cápita (puesto 63 de 196 países)

**Principal socio comercial** +150 países (exporta el 19% del PIB e importa el 15%)

**Estrategia** para ser en 2030 líder mundial en Inteligencia Artificial

***Fuente:*** *Banco Mundial y Datosmacro para datos macroeconómicos y We Are Social para datos de la economía digital.*


**En 2030, Asia concentrará dos tercios de la clase media mundial**

mantener parte de nuestro actual bienestar y calidad de vida, importancia, peso geopolítico, capacidad de negociación e influencia, debemos aprender a convivir con la realidad asiática y a desentrañar la lógica que emplea la mayoría del mundo (60% de la población global vive en Asia) para diseñar su futuro.

Si algo nos ha enseñado la pandemia es que el mundo es un lugar altamente interconectado, que la exportación representa un sólido pilar de crecimiento y que, para bien o para mal, lo que sucede en China tiene un gran impacto en las empresas y en la economía mundial: el mundo entero se quedó sin microchips debido al cuello de botella que sufrió China con la pandemia y a la distorsión en la cadena de suministro global.

## China lidera gran parte de los desarrollos en la economía digital y aspira a ser líder en Inteligencia Artificial

China no va a desaparecer, va para largo y tiene aún mucho potencial sin aprovechar. Las apuestas sobre el año en que China superará a EEUU como primer PIB mundial bailan entre el 2028 y el 2033. Ya le ha superado en gasto en I+D sobre PIB y sus universidades destacan en los ranking mundiales. China es financiador neto de la economía global y se encuentra en el centro de la región económica más grande y dinámica de un mundo que, lejos de americanizarse, se *"achina"* a pasos agigantados. Además, con el programa **Nueva Ruta de la Seda** para financiar infraestructuras, China está ampliando su área de influencia a otras partes del mundo, léase África, América Latina o Eurasia. Actualmente, ya es el principal socio comercial de más de 150 países, tiene una balanza comercial con un enorme superávit (571.937 millones de euros), lo que le permite atesorar el mayor volumen reservas de divisas del mundo (2,75 billones de euros).

Sin duda, China es vector de crecimiento futuro, un polo de atracción de inversión y un centro del consumo global. Un lugar que no hay que perder de vista y que presenta una inmensa oportunidad de negocio.

China sigue siendo la gran fábrica del mundo, y poco a poco va dejando atrás viejas prácticas de copiar o imitar. Ahora lidera gran parte de los nuevos desarrollos en la economía digital y aspira a ser, en 2030, líder en Inteligencia Artificial. China tiene una de las mayores y más rápidas redes fijas y móviles de conexión a Internet, es líder mundial en economía digital y comercio electrónico -Aliexpress, Shein y WeChat son mundialmente conocidas- y en el desarrollo de Inteligencia Artificial aplicada tanto a la industria como a la medicina, la agricultura y los propios consumidoresy los propios consumidores están habituados al pago por móvil, los asistentes de voz y los traductores en tiempo real. El gigante Baidu acaba de lanzar su propio GPTChat (Ernie Bot).

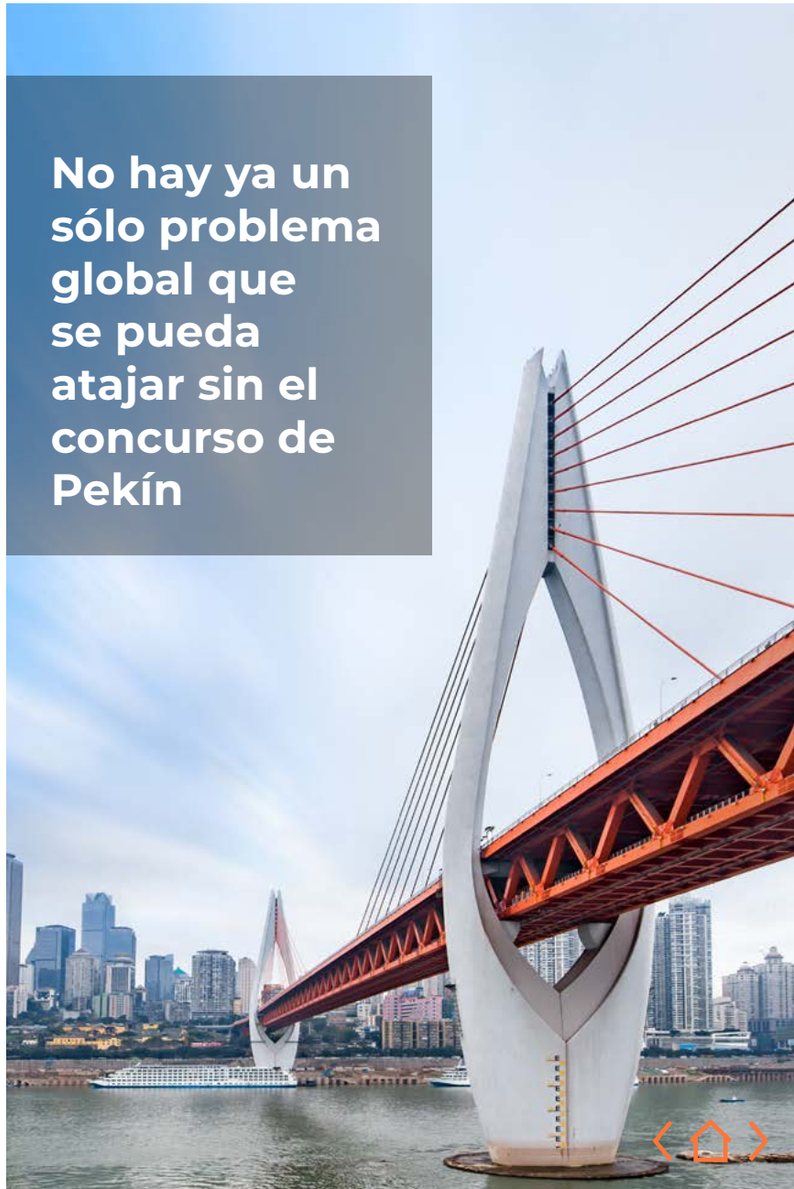
Pese a la creciente rivalidad transpacífica, Asia y China componen una realidad irreplicable, sin la cual no podemos vivir. Tanto es el peso geopolítico que tiene hoy este *"Estado-civilización"* -China-, que no hay ya un sólo problema global que se pueda atajar sin el concurso de Pekín. El ascenso de China no va a cambiar el tablero ni las fichas, pero sí las reglas del juego internacional. Dicho cambio supone el mayor acontecimiento histórico y desafío geopolítico de los próximos 50 años y nuestra mayor oportunidad (o amenaza) profesional y empresarial futura. La magnitud del reto contrasta con el desconocimiento imperante sobre este país. Convivir y comprender China será, para quienes habitamos en Occidente, uno de los grandes desafíos del siglo XXI.

## China presenta una gran oportunidad comercial: desaprovecharlo tiene un alto coste de oportunidad

La oportunidad de mercado en China para las empresas occidentales no deja de crecer. Con 400 millones de personas disponiendo de una capacidad adquisitiva equivalente a la media europea, China es el primer mercado mundial en múltiples segmentos de bienes de consumo físicos (especialmente en el medioambiental, salud y cuidado personal, moda, alimentación, bienestar, ocio y educación) y es líder en comercio electrónico. Desaprovechar el acceso a esa enorme bolsa de consumidores tiene un coste de oportunidad muy alto, pero saber aprovecharlo exige salvar adecuadamente la distancia cultural existente y generar estrategias a largo plazo que permitan adaptar el modelo de negocio a la competitividad y el dinamismo que le son propios al mercado chino. Además, China es nuestro primer socio comercial (no europeo) y, también, el primer inversor en España (fuera del perímetro OCDE).

La inflación, el control antimonopolio sobre sus grandes consorcios empresariales privados, la trampa de rentas medias, la crisis inmobiliaria, las normativas medioambientales para el cumplimiento de su agenda de descarbonización o la tensa rivalidad geoestratégica con EEUU, pueden animar a pensar que China es un gigante con pies de barro, pero China tiene sus propios planes. Pekín ha apostado, con éxito, por su propia estrategia de desarrollo económico: un modelo basado en el control del mercado, el crecimiento sostenible, la innovación tecnológica y el consumo interno.

La presencia de marcas y multinacionales españolas en China es destacada y no siempre se pone adecuadamente en valor, pues es modesta



**Tanto hacer negocios en China como competir con sus empresas exige aprender a habitar un mundo con atributos cada vez más chinos**



en comparación con la de empresas francesas (el doble) o alemanas (9 veces más). Muchas obtienen en China buena parte de sus ventas. Esto se acentuó con la pandemia. China es el mayor mercado de consumo a futuro, el único con potencial de crecimiento sólido y sostenido en las próximas décadas y, para muchos, la única posibilidad de multiplicar su negocio. Quienes ya están operando en China, quieren reposicionarse para aprovechar todo el potencial; quienes lo intentaron y fracasaron, buscan otra oportunidad; y quienes aún no están, no quieren seguir renunciando a este enorme mercado.

Pese al proceso de **reglobalización post-pandémico**, a la llamada a un -inviable- ***decoupling*** y a la **regionalización** de ciertas dinámicas comerciales, de aquí al 2030, tanto en términos de exportación, como de distribución, inversión o producción, las empresas españolas se juegan mucho en China. Tanto aprovechar esa oportunidad como competir con China exige aprender a habitar un mundo con atributos cada vez más chinos.

Comprender el futuro que construye China -se mantengan o no relaciones comerciales allí- exige de una mirada *"desde dentro"* al país, pues su múltiple potencial disruptivo (económico, financiero, tecnológico, geopolítico, etc.) nos obliga a repensar el mundo de mañana. En definitiva, un imperativo para mantener la competitividad en el siglo XXI.

# Asamblea

## Sonsoles Rubio reelegida presidenta del Instituto

### ASAMBLEA DEL INSTITUTO

**Sonsoles Rubio, Directora de Auditoría Interna de Iberdrola**, ha sido reelegida presidenta el Instituto de Auditores Internos de España en la asamblea del pasado 29 de junio. Rubio accedió al cargo en junio de 2020 convirtiéndose en la primera mujer al frente del Instituto en toda su historia.

La asamblea también aprobó la renovación de mandatos 2023-2025 de los consejeros: Manuel de Alzúa (Amadeus IT Group), Vicepresidente; Sonia Vicente (MMT Seguros), Secretaria y los Consejeros: María Luisa Gordillo (Mapfre); Francisco Martínez (Bankinter) y Paula Mouzo (Inditex).

La presidenta agradeció a los socios su confianza y repasó los hitos más significativos del año, empezando por los detalles y la evolución del **Plan Estratégico 2022-2024** que tiene como ejes de actuación mejorar la influencia de los auditores internos e **impulsar el servicio** para que el auditor interno tenga las capacidades y competencias para asegurar su relevancia en las organizaciones.


Accede a la memoria de 2022


Accede a la información de la asamblea a general (solo para socios)

**3.725** socios

**4,31** sobre 5 nota media de formación en la encuesta de calidad

**4.573** asistentes a cursos y eventos

**176** consejeros en Esfera

**219** certificaciones profesionales

**1.720** asistentes a los Lunes del IAI

# Foros

## La CNMV enfatiza el papel de la Comisión de Auditoría

### ENCUENTRO CONSEJEROS

El 9 de mayo celebramos nuestro Encuentro Consejeros de 2023. Contamos con **Montserrat Martínez Parera**, vicepresidenta de la CNMV, quien enfatizó el papel de la Comisión de Auditoría. Analizados la Inteligencia Artificial de la mano de **Rita Estévez**, consejera de **Línea Directa**. Repasamos las previsiones macro y geopolíticas con **Federico Steinberg**, investigador principal del **Real Instituto Elcano**. Y asistimos a un interesante diálogo entre la presidenta de la Comisión de Auditoría de **Inditex**, **Pilar López**, y la directora de Auditoría Interna de la misma compañía, **Paula Mouzo.**

Leer más.



Haz Click aquí para ver vídeo

Ver las sesiones completas esfera consejeros

(solo para suscriptores de Esfera. ¿Eres consejero o Director de Auditoría Interna y no tienes acceso? Solicítanos el alta)

## Ciberseguridad, tendencias y colaboración con Auditoría Interna

### FORO DE EXPERTOS


La ciberseguridad centró el Foro de Expertos de junio. Contamos con **Marina Rodríguez Díaz,** jefa de la Unidad de Ciberseguridad y Desinformación del Departamento de **Seguridad Nacional** de Presidencia del Gobierno; una mesa redonda con los siguientes directores de Auditoría Interna: **Rosa Sánchez (Enagás)**; **Raquel Pilares (AEDAS Homes)** y **Francisco Martínez García (Bankinter)**. Y asistimos a una charla entre dos profesionales de **Iberdrola, José Manuel Alonso (CISO) y Daniel Ponz Lillo**, responsable de auditoría de sistemas y ciberseguridad.

Leer más.

# Foros

## Herramientas para el razonamiento ético

**LUNES DEL INSTITUTO**

**Pablo Villar,** responsable del ámbito asegurador del departamento de Auditoría Interna de **Mutua Madrileña**, nos ofreció una visión general de las principales teorías éticas que articulan los debates sociales y políticos actuales.

Leer más.

Haz Click aquí para ver vídeo


## Taxonomía UE: Haciendo Camino al andar

**LUNES DEL INSTITUTO**

Realizamos un profundo análisis de la taxonomía europea de actividades sostenibles de la mano de **Helena Redondo**, experta en **Sostenibilidad y Gobierno Corporativo.**

Leer más.

Haz Click aquí para ver vídeo


## Revisión de las Normas globalesde Auditoría Interna

**LUNES DEL INSTITUTO**

El **Director Técnico del Instituto, Jesús Lafita**, nos pone al día en las novedades y pasos realizados y pendientes del proceso de revisión de las Normas Internacionales para el ejercicio profesional de la Auditoría Interna (IPPF) que está llevando a cabo el Instituto global, IIA.

Leer más.

Haz Click aquí para ver vídeo

# Conocimiento

## El rol de la Comisión de Auditoría en asuntos ESG

### ESFERA CONSEJEROS

Informe elaborado por el Centro de Gobierno Corporativo de **Esade, PwC España y el Instituto de Auditores Internos de España.** Encuesta que analiza el papel de la Comisión de Auditoría en los riesgos ESG.

Leer más.


Accede al documento

## Auditoría Interna de la Cultura Corporativa

### LA FÁBRICA DE PENSAMIENTO

Una guía que tiene dos objetivos principales: impulsar el entendimiento de la Cultura Corporativa como un elemento más del universo auditable, y servir como punto de partida para abordar este tema por primera vez, o para contrastar.

Leer más.

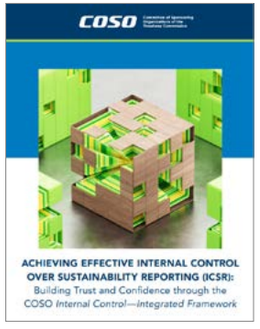

Accede al documento (solo registrados)

## Control interno de la información sobre sostenibilidad

### GUÍA COSO

COSO ha elaborado la guía *Cómo alcanzar un control interno efectivo en la información sobre sostenibilidad* para mejorar el reporting de la información no financiera aplicando 17 principios del marco COSO control interno.

Leer más.



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 - Fax: 91 593 29 32



www.auditoresinternos.es