

Julio - Diciembre 2024 - N°20

# OBSERVATORIO

GERENCIA DE RIESGOS

## La gestión de riesgos digitales y la IA



ager̄s

ACTUALIDAD - ENTREVISTAS - ESPECIAL FERMA FORUM 2024 - LA ASOCIACIÓN

# SUMARIO

La revista Observatorio de Gerencia de Riesgos de AGERS respeta las opiniones expuestas en los artículos por sus autores, pero no se hace responsable de los contenidos de los mismos. Cualquier forma de reproducción, distribución o transformación de la revista, sólo podrá realizarse bajo la autorización previa de sus autores

## PRESIDENTE:

JUAN CARLOS LÓPEZ PORCEL

## DIRECTOR:

GONZALO ITURMENDI

## REDACCIÓN Y COORDINACIÓN:

ALICIA SOLER

## CONSEJO DE REDACCIÓN:

ALFREDO ZORZO, MARIO RAMÍREZ, ALFONSO GARRIDO, ANDRÉS BARCELÓ Y FERNANDO REDONDO

## DISEÑO Y REALIZACIÓN EDITORIAL:

LUCIA ALMAGRO, MARÍA SAAVEDRA, MARÍA DEL MAR YÁGUEZ Y DANIEL HERRERA

## EDITA:

AGERS

## LUGAR DE EDICIÓN:

MADRID

## DOMICILIO SOCIAL:

C/ PRÍNCIPE DE VERGARA,  
86, 28006 MADRID

## CORREO:

COMUNICACIONES@AGERS.ES

## DEPÓSITO LEGAL:

M-2025-2020

## ISSNL:

2695-6802

# 04

"2024: CONSTRU-  
YENDO UN FUTURO  
MEJOR A TRAVÉS DE  
LA UNIÓN Y LA INNO-  
VACIÓN",  
POR ALICIA SOLER

# 06

MARSH

Riesgos cyber en  
el horizonte,  
por Nelia Argaz

# 10

GENERALI

La IA en el  
Sector Marítimo,  
por Manuel Luzena

# 12

AXA XL

Un espectro anda  
suelto: se llama IA, por  
Patrick Lee-Warner

# 16

BHSI

Balance de un año car-  
gado de retos y emo-  
ciones para el mercado  
de Cyber,  
por Sanae Blanco

# 18

MAPFRE

IA en los Seguros de  
Riesgos Globales,  
por Carlos Villanueva  
Afán de Ribera

# 20

HOWDEN

El auge del ciberseguro  
en un panorama de  
amenazas intensificadas

# 24

AON

Inteligencia Artificial:  
Nuevos Desafíos y  
Oportunidades en el  
Sector Asegurador,  
por Juan Carlos Martínez  
Rodríguez y Belén Vílchez  
Morales





## 28 ENTREVISTA CYBER

“El seguro ciber es la clave en un entorno de riesgos crecientes”, responde Agustín de la Cuerda y entrevista Juan Gayá

## 34 RISKONNECT

Esfuézate por tener el mismo marco para todos tus riesgos “Risk under one roof”, por Jorge Nadel

## 38 INTERNATIONAL SOS

Beneficios de la IA para la Gestión de Riesgos, por Santiago Álvarez de Toledo

## 40 INNOVAIBÉRICA

Una Mirada al Futuro de la Gestión de Riesgos, por Sergio Gómez Rodríguez

## 43 ESPECIAL FERMA

- Madrid FERMA FORUM 2024
- FERMA FORUM en días
- Paneles de los españoles en el FERMA FORUM 2024
- Hablando con AGERS
- FERMA FORUM en imágenes
- FERMA NIGHT 2024 y clausura



## 76 LA MENTORIZACIÓN Y EL INTERCAMBIO DE EXPERIENCIAS ESENCIALES

## 90 EVENTOS DE LA ASOCIACIÓN:

- «Programas de Seguros Internacionales»
- Desayuno «DE TÚ A TÚ» con Alejandra Galdos de HSF y Marta Vega de Exolum
- Foro sobre Litigiosidad en USA con BHSI
- la Coyuntura del Seguro de Crime y los Retos Cibernéticos
- Envejecimiento como Riesgo Empresarial
- Nuevas Guías sobre Ciberseguridad e Inteligencia Artificial

## 104 Nuevos asociados AGERS 2024 PATROCINADORES

# “2024: Construyendo un futuro mejor a través de la **unión** y la **innovación**”

2024 ha sido un año de grandes momentos y aprendizajes, lleno de desafíos, pero también de oportunidades para avanzar juntos hacia un futuro más seguro, unido y esperanzador. Este año, más que nunca, hemos sentido la importancia de colaborar, de cuidarnos unos a otros y de apostar por soluciones innovadoras en un mundo tan convulso y cambiante.

Comenzamos el año con un paso firme hacia la prevención de riesgos en un contexto de crecientes desafíos climáticos. En enero, viajamos a Asturias, a la planta de ArcelorMittal en La Granda, para reunirnos con la Dirección General del Agua. Allí, discutimos la necesidad de prevenir los riesgos derivados de las inundaciones, un tema crucial cuando el cambio climático sigue golpeando con fuerza. Fue una jornada de reflexión y trabajo conjunto, donde analizamos las zonas más vulnerables y las soluciones más efectivas para mitigar estos riesgos. Con el apoyo de Mapfre y del CCS, que nos brindaron su visión experta sobre el riesgo y el seguro, sentamos las bases para un futuro más resiliente.

En abril, celebramos un hito muy especial para AGERS: nuestro 40 aniversario. Cuatro décadas trabajando para proteger lo que más importa, y lo hicimos rodeados de amigos, colegas y aliados. Fue una jornada llena de energía positiva, celebrando los logros del pasado y mirando hacia el futuro. Un momento de reencuentro, de compartir historias, reír y fortalecer los lazos con todos aquellos que han sido parte de este camino.

El otoño trajo consigo uno de los eventos más grandes y esperados del año: el FERMA Fórum en Madrid. Durante tres días, más de 3.000 profesionales de toda Europa se dieron cita en la capital española para intercambiar ideas, compartir experiencias y aprender unos de otros. Fue un espacio de reflexión, colaboración, amistad y convivencia. Un recordatorio de la importancia de la unión en un sector que, aunque diverso, tiene un objetivo común: avanzar hacia un mundo más seguro y resiliente.

Casi en el inicio del Adviento, presentamos dos guías fundamentales: una sobre riesgos cibernéticos y otra sobre inteligencia artificial. En un mundo cada vez más digital, estas herramientas se han convertido en esenciales para enfrentar los nuevos riesgos que surgen en cada rincón de la red.

Y así llegamos a diciembre, con la publicación de El legado de un perito de Elías Rodríguez. Esta obra se suma a nuestra creciente biblioteca de conocimiento, con más de 30 libros especializados que buscan formar y educar a los profesionales del futuro. El legado de un perito es un homenaje a aquellos que han dedicado su vida a fortalecer el sector y un recordatorio de cómo el conocimiento y la experiencia pueden iluminar el camino en tiempos inciertos.

A lo largo de todo este 2024, también nos hemos mantenido cerca de aquellos que más lo necesitaban. Frente a la tragedia de la DANA, hemos ofrecido asesoramiento y apoyo, ayudando a mitigar los efectos de las inundaciones y las catástrofes. Como comunidad, debemos estar siempre dispuestos a ayudar, a brindar soluciones y a ser solidarios en los momentos de mayor necesidad.

En un mundo lleno de turbulencias y cambios constantes, 2024 nos ha recordado algo fundamental: solo juntos, unidos en paz y en el amor por lo que hacemos, podemos avanzar hacia un futuro mejor. Hemos aprendido que la colaboración es la clave, que el conocimiento nos da poder, y que siempre hay espacio para la esperanza, incluso cuando los desafíos parecen insuperables.

Así, con ilusión y optimismo, cerramos un año de crecimiento y unión, con la certeza de que el camino hacia un futuro más justo y seguro es posible. Y seguiremos caminando, paso a paso, hacia un 2025 lleno de más logros, más trabajo conjunto y, sobre todo, más amor por lo que hacemos.

Que seáis felices.



**Alicia Soler**  
Executive Manager - AGERS



8ª EDICIÓN - 2025/2026

# PROGRAMA DE FORMACIÓN AVANZADA EN GESTIÓN DE RIESGOS Y SEGUROS

*Riesgos y Seguros: una nueva perspectiva*

# Riesgos cyber en el horizonte



*Cada avance en inteligencia artificial, los conflictos geopolíticos, la expansión del Internet de las Cosas (IoT) y el desarrollo de la computación cuántica redefinen el panorama de ciberamenazas, y revelan una necesidad: enfocar la estrategia de ciberseguridad y resiliencia como ventaja estratégica. Al anticipar, cuantificar y gestionar adecuadamente estos riesgos, las organizaciones pueden posicionar la seguridad de la información como un motor de confianza y crecimiento. El desafío radica en equilibrar innovación, eficiencia y resiliencia en un entorno donde las amenazas no solo se multiplican, sino que diversifican y amplifican su impacto.*

En este artículo, exploraremos ejemplos prácticos y potenciales derivados de riesgos emergentes, y cómo un enfoque estratégico en ciberriesgo puede generar un valor tangible, impulsando la sostenibilidad y el éxito a largo plazo de las organizaciones.

## **RIESGOS EMERGENTES DE CIBERSEGURIDAD**

### **1. INTELIGENCIA ARTIFICIAL Y CIBERATAQUES DIRIGIDOS A SISTEMAS IA**

La inteligencia artificial (IA) está transformando sectores de manera transversal, con aplicaciones que abarcan desde la creación de nuevos procesos y funciones de negocio hasta la detección avanzada de fraudes en industrias como finanzas, salud, manufactura y servicios ITC.

Esta tecnología introduce diferentes tipologías de riesgos, entre los que destacamos los derivados de ataques dirigidos a sistemas de ciberseguridad basados en IA que pueden comprometer la integridad de decisiones automáticas, generando consecuencias operativas graves con impacto financiero y reputacional.

Por otro lado, la introducción de la IA durante los procesos de negocio por parte de actores malintencionados, por ejemplo, el proceso de contratación supone una nueva vía de entrada para cibercriminales, donde la mayoría de las organizaciones no disponen de controles de detección óptimos.

- Ejemplo potencial de impacto en el sector financiero: En el ámbito bancario, un ciberataque dirigido a sistemas de detección de fraude basado en IA podría habilitar la manipulación de transacciones o la aprobación de operaciones fraudulentas, afectando directamente la integridad del sistema. Según el último Global Financial Stability Report del Fondo Monetario Internacional (FMI), aunque la IA mejora la eficiencia, también puede incrementar la exposición a ciberataques y a intentos de manipulación del mercado mediante algoritmos maliciosos.
- Ejemplo de impacto en el sector tecnológico: empresa estadounidense de formación y concienciación en ciberseguridad detectó que había contratado a un ingeniero del software, supuesto ciudadano de Estados Unidos, para un puesto de tecnología





**Nelia Argaz**

*Líder en Cyber Security & Business Resilience Leader  
for Continental Europe de Marsh*

desarrollado en trabajo remoto. El trabajador contratado era en realidad una persona controlada por un actor de amenazas norcoreano. Pese a que el proceso de contratación incluyó verificaciones de antecedentes, referencias y cuatro entrevistas basadas en videoconferencia, el trabajador evitó ser atrapado al usar una identidad válida robada a un individuo con sede en EE. UU, incluyendo su imagen. Así, el plan fue mejorado con uso de tecnología deepfake, mediante el cual sus rasgos asiáticos fueron modificados por una fisonomía caucásica.

## **2. VULNERABILIDADES EN EL INTERNET DE LAS COSAS (IOT)**

El Internet de las Cosas (IoT) ha impulsado la innovación y eficiencia en múltiples sectores, permitiendo la conexión de dispositivos y sistemas que antaño funcionaban de manera aislada. Sin embargo, la adopción masiva de dispositivos IoT ha incrementado considerablemente la superficie de ataque, exponiendo a las organizaciones a una mayor variedad de amenazas con impactos relevantes no únicamente en el ámbito tecnológico o económico, sino también en el físico. Pese a no ser un riesgo emergente por sí solo, la combinación de riesgos emergentes en el uso de dispositivos IoT, que suelen tener limitaciones en cuanto a medidas de seguridad, representan puntos de entrada vulnerables que los atacantes pueden explotar para comprometer redes o manipular sistemas críticos, y en algunos casos, causar daños físicos. No en vano, la Presidencia del Consejo y los negociadores del Parlamento Europeo han alcanzado un acuerdo provisional sobre la legislación propuesta relativa a los requisitos de ciberseguridad para los productos con elementos digitales, cuyo objetivo es garantizar que productos IoT, incluyendo los domésticos como frigoríficos, televisores y juguetes conectados sean seguros antes de que se introduzcan en el mercado (Ley de Ciberresiliencia o EU Cyber resilience Act).

- Ejemplo de impacto en seguridad y telecomunicaciones: En 2024, un ataque dirigido contra miembros de Hezbolá en el Líbano explotó dispositivos de comunicación, como buscapersonas y walkie-talkies, en lo que se presume fue una operación de la agencia de inteligencia israelí. Este incidente combinó un ciberataque con una modificación física en la cadena de suministro: los dispositivos fueron manipulados para incorporar material explosivo que podían detonarse de forma remota. Este ataque demuestra cómo un vector combinado (ciber y físico) puede tener consecuencias devastadoras, resaltando la vulnerabilidad de los dispositivos IoT en escenarios de conflicto y la necesidad de controles robustos en la cadena de suministro.

## **3. COMPUTACIÓN CUÁNTICA Y AMENAZAS A LA CRIPTOGRAFÍA**

La tecnología cuántica tiene la capacidad de romper el método de cifrado, exponiendo los datos de cualquier empresa que no utilice criptografía post cuántica, como email, VPN; e incluso bases de datos que han sido robados, quedando a la espera de disponer dicha tecnología post cuántica para descifrarlos. A diferencia de los ordenadores tradicionales, los cuánticos pueden realizar cálculos complejos de manera exponencialmente más rápida, lo que amenaza directamente los algoritmos de cifrado asimétrico ampliamente utilizados en la actualidad, como RSA y ECC (Elliptic Curve Cryptography), que dependen de la factorización de números primos u otros problemas matemáticos complejos de difícil resolución en sistemas clásicos.

- Ejemplo de impacto potencial transversal: En cualquier empresa que gestione datos y sistemas online, la capacidad de un ordenador cuántico para romper el método de cifrado, podría exponer dichos datos. Según el Global Financial Stability Report de abril



de 2024 “la llegada de la computación cuántica y su capacidad para romper rápidamente los algoritmos de cifrado utilizados en los sistemas financieros también podrían magnificar las pérdidas por ciberataques”.

En este sentido, el Instituto Nacional de Estándares y Tecnología (NIST) ha desarrollado estándares de algoritmos resistentes a la computación cuántica, recomendando a las organizaciones la implementación progresiva de soluciones de cifrado post-cuántico para mitigar esta amenaza inminente.

#### 4. RIESGOS EN LA CADENA DE SUMINISTRO DIGITAL

El mundo digital interconectado define hoy en día los ecosistemas organizativos que conectan con una red mundial de fabricantes, desarrolladores de software y otros proveedores de servicios. Por ejemplo, un dispositivo puede haber sido diseñado en un país y construido en otro utilizando múltiples componentes de varias partes del mundo que, a su vez, han sido ensamblados con piezas de distintos fabricantes. Así, a los riesgos clásicos de la cadena de suministro digital, se añaden ciberataques y vulnerabilidades potenciados por los riesgos emergentes ya descritos.

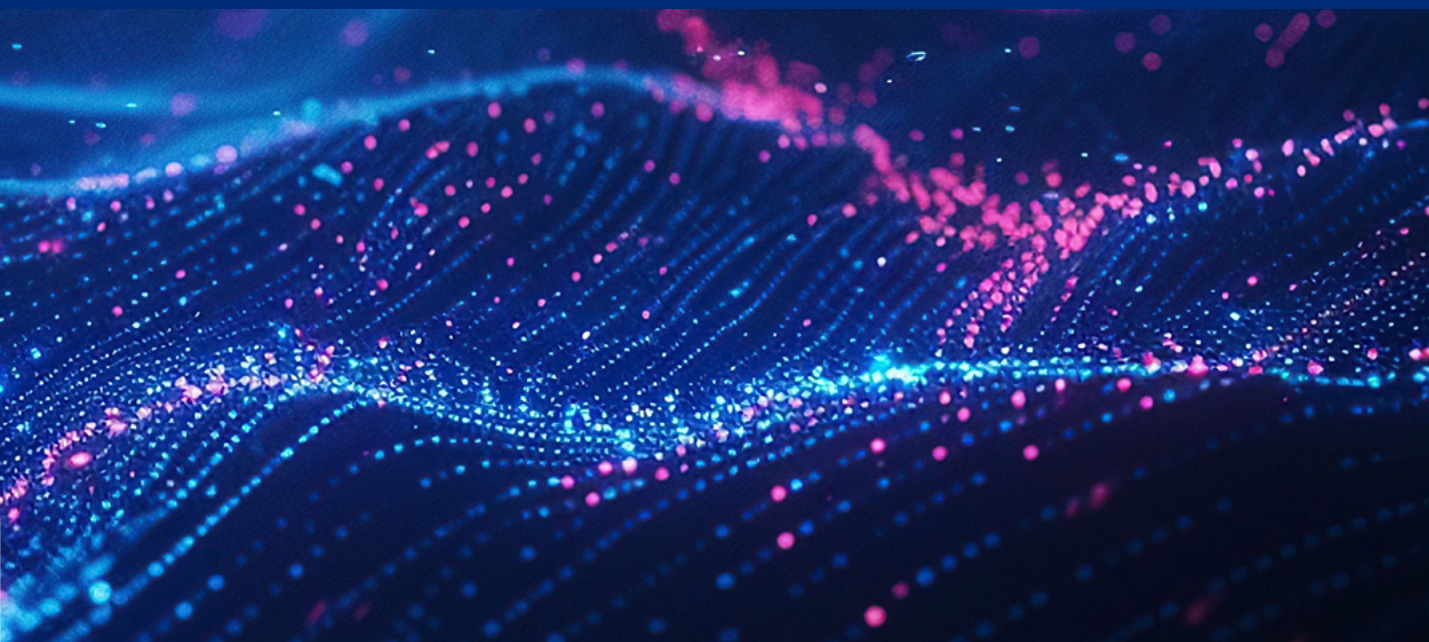
El último Informe de Riesgos Globales 2024 de Marsh McLennan subraya una creciente dependencia de proveedores externos y servicios digitales y enfatiza la necesidad de fortalecer la resiliencia de las cadenas de suministro digitales mediante la implementación de prácticas de seguridad robustas y la colaboración estrecha con proveedores para mitigar los riesgos asociados.

- Ejemplo de ciberataque en la cadena de suministro: En junio de 2023, la vulnerabilidad en el software MOVEit Transfer, desarrollado por Progress Software, fue explotada por el grupo de ransomware Clop. Este ataque afectó a más de 100 organizaciones a nivel mundial, incluyendo entidades gubernamentales y empresas privadas, comprometiendo datos sensibles y causando interrupciones significativas en las operaciones. El incidente evidenció cómo una brecha en un proveedor de software puede tener un efecto dominó en múltiples sectores, resaltando la necesidad de una gestión rigurosa de la seguridad en la cadena de suministro digital.
- Ejemplo de fallo IT en la cadena de suministro digital: En julio de 2024, una actualización defectuosa del software de seguridad de CrowdStrike provocó una interrupción masiva que afectó a millones de dispositivos a nivel mundial. Este incidente, aunque no fue un ciberataque, evidenció cómo una falla en un proveedor de servicios críticos puede tener un impacto significativo en la cadena de suministro digital. Según un informe de Marsh, las interrupciones en la cadena de suministro digital pueden resultar en pérdidas financieras sustanciales y afectar gravemente la reputación de las empresas involucradas.

#### 5. ESTRATEGIAS PARA LA GESTIÓN DE RIESGOS EMERGENTES

Defino los procesos a llevar a cabo para la gestión de riesgos emergentes de ciberseguridad integral. No pretendo basarme en soluciones técnicas, sino en sentar las bases propias de la gestión avanzada de riesgos, con





un enfoque conjunto y alineado de análisis, mitigación y transferencia.

### **1- CUANTIFICACIÓN DEL RIESGO CIBERNÉTICO Y PRIORIZACIÓN ESTRATÉGICA**

Cuantificar el ciberriesgo es fundamental para definir una estrategia de ciberseguridad efectiva y priorizar inversiones. En lugar de ver la seguridad como un simple coste más, se debe optar por una metodología que permita identificar el retorno a la reducción del riesgo. Una buena práctica es asignar un valor monetario y trazable a cada escenario de ciberriesgo, basado en las partidas de pérdidas y extra costes generados tras su potencial materialización, y evaluando la probabilidad de que ocurra un incidente en base a controles internos y contexto externo.

### **2- ESTRUCTURAS DE TRANSFERENCIA DEL RIESGO**

La transferencia del riesgo es una opción válida para minimizar el impacto financiero de un ciberincidente materializado, como pérdidas y extra-costes derivadas de violaciones de seguridad, interrupciones de servicio, servicios de gestión y respuesta o ciberfraudes.

Debemos seguir trabajando con el mercado asegurador para identificar potenciales coberturas y defi-

nir posibles necesidades surgidas de riesgos emergentes.

Dicha transferencia se puede realizar apoyándose en un bróker de seguros para definir la estructura de transferencia óptima combinando, si así fuera necesario, transferencia al mercado asegurador con estructuras de financiación como, por ejemplo, cautivas o estructuras de transferencia alternativas (ATLs).

### **3- LA SEGURIDAD ES COSA DE TODOS**

El uso de nuevas tecnologías y una superficie de ataque ampliada (por ejemplo, la variabilidad, heterogeneidad y dependencia de la cadena de suministro digital), sumado a los actores ciberdelincuentes surgidos de tensiones geopolíticas, acelera y amplifica, no sólo el radio de acción de las ciberamenazas, sino las vías de acceso y las tipologías de impacto de éstas.

La amplificación y tipología de amenazas amenaza la necesidad de resolver las acciones de ciberseguridad no únicamente desde la perspectiva tecnológica, sino considerando el ecosistema de riesgo global de la organización. Esto implica desarrollar una estrategia de ciberriesgo sólida enfocada a gestionar los equilibrios entre resiliencia y eficiencia, protección y funcionalidad y, mitigación y transferencia de riesgos, con un enfoque claramente alineado con la estrategia de la organización.

10



*Manuel Luzena  
Head of Marine & Aviation  
Underwriting Generali GC&C  
Mediterranean-Latam*

# La IA en el Sector Marítimo

LA INTELIGENCIA ARTIFICIAL (IA) ESTÁ TRANSFORMANDO LA INDUSTRIA MARÍTIMA AL OFRECER NUEVAS FORMAS DE OPTIMIZAR OPERACIONES Y MEJORAR LA SEGURIDAD. MEDIANTE SISTEMAS AVANZADOS DE APOYO A LA TOMA DE DECISIONES, LA IA PERMITE AUTOMATIZAR TAREAS CLAVE COMO LA NAVEGACIÓN Y LA OPTIMIZACIÓN DE RUTAS, ASÍ COMO REALIZAR PREDICCIONES EN BASE A LOS DATOS RECOPIADOS. ESTOS AVANCES PROMETEN UNA NAVEGACIÓN MÁS EFICIENTE Y SEGURA, AUNQUE PARA DECISIONES CRÍTICAS AÚN SE REQUIERE LA SUPERVISIÓN DE PERSONAS.



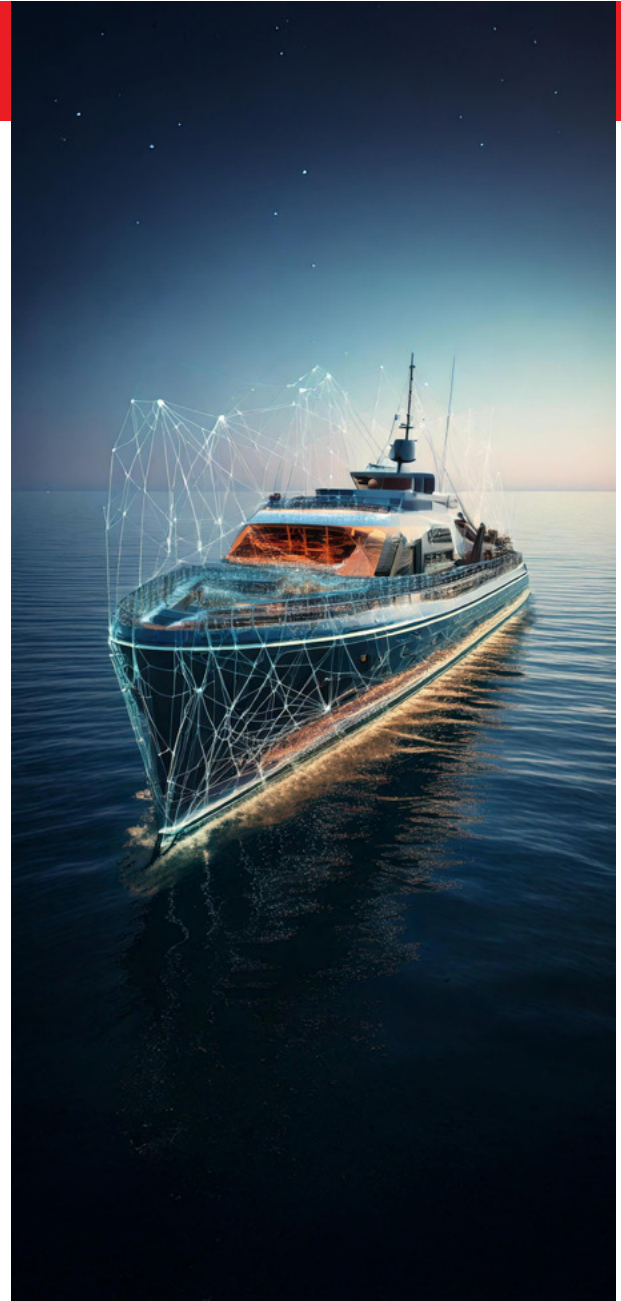
Ya hoy, se están desarrollando prototipos de barcos autónomos, especialmente de pequeño tamaño y propulsados eléctricamente, que dependen en gran medida de la IA para gestionar la navegación. Estas embarcaciones buscan aliviar la escasez de marineros y mejorar la eficiencia del transporte marítimo. Sin embargo, aunque estos avances son prometedores, para su aplicación a gran escala tendremos que esperar un tiempo.

En relación con la navegación marítima, el uso de esta tecnología supone la optimización de rutas, lo que no solo ahorra tiempo y reduce el consumo de combustible, sino que también mejora significativamente la gestión de riesgos. Al analizar datos históricos de tráfico y condiciones marítimas, la IA puede identificar áreas de riesgo y planificar rutas más seguras, lo que es importante para prevenir siniestros. Esto reduce la frecuencia y el impacto de los accidentes, y también optimiza la transferencia de riesgos, beneficiando tanto a las empresas de transporte como a las aseguradoras.

En cuanto al transporte de mercancías, también tiene aspectos positivos, como maximizar el uso del espacio de carga y calcular la mejor distribución para garantizar la estabilidad del buque, lo que reduce los costes y minimiza el riesgo de daños a la carga. Con el monitoreo en tiempo real, se pueden supervisar las condiciones de las mercancías (como temperatura y humedad), lo que impacta positivamente las reclamaciones relacionadas con daños o pérdidas.

Aunque todos estos avances tendrán un impacto positivo, existen aún ciertos desafíos e incertidumbres que enfrentar. La eficacia de estos sistemas en la toma de decisiones críticas depende en gran medida de la calidad y disponibilidad de los datos. En situaciones imprevistas o con datos insuficientes, puede encontrarse limitada, lo que subraya la necesidad de intervención de personas para garantizar la seguridad.

Además, con el avance de la automatización y los sistemas autónomos, el sector asegurador deberá adaptarse a nuevas exigencias de cobertura, especialmente



en casos de negligencia que involucren a pilotos autónomos o sistemas automatizados. Dentro de las cláusulas inglesas "Additional Perils", se incluye la cobertura por pérdida o daño a la embarcación debido a accidentes o por negligencia, incompetencia o error de juicio de cualquier persona, independientemente de quién sea. Será interesante observar cómo esta cláusula evolucionará en el futuro para reflejar los nuevos desafíos que traerá la automatización y la IA en la navegación.

# Un espectro anda suelto: se llama IA

*La inteligencia artificial (IA) ha penetrado tan rápidamente en nuestra vida cotidiana que apenas pasa un día sin que oigamos o leamos algo sobre ella, o incluso la utilicemos nosotros mismos. Esto abarca desde artulugios privados para editar las fotos de las vacaciones hasta aplicaciones altamente profesionales y complejas que podrían tener un impacto relevante en el futuro de nuestro planeta.*

Pero ¿qué hay de los riesgos asociados al uso de la IA? ¿A qué retos se enfrentan las empresas y qué necesidades de protección surgen como consecuencia? Según el Informe de Riesgos Futuros de AXA, los ciberriesgos y los riesgos relacionados con la IA y el big data son una de las principales preocupaciones de los expertos en riesgos encuestados de 50 países.

Como responsable del negocio cibernético de AXA XL en España y Portugal, a menudo me preguntan si ampliar la cartera es una buena idea, dado que las amenazas de ransomware, ataques a las cadenas de suministro y similares son cada vez más sofisticadas y eficientes, y ahora los desarrollos en torno a la IA están exacerbando el riesgo de incidentes cibernéticos.

Mi respuesta es sí, si lo enfocas en la colaboración con clientes y corredores, en lugar de limitarte únicamente a proporcionar capacidad. Debemos encontrar soluciones viables que mitiguen el riesgo, para que los clientes sigan desarrollándose en este mundo digital.

## NECESIDAD DE PROTECCIÓN DE LOS CLIENTES

Los riesgos cibernéticos siguen siendo uno de los mayores retos para las empresas, ya que los ataques son cada vez más sofisticados y organizados. En mis conversaciones con los clientes queda claro una y otra vez que muchos de ellos piensan inicialmente en la mayor cobertura de seguro posible al menor precio posible, por razones comprensibles. Sin embargo, enseguida se hace evidente que la necesidad de protección va mucho más allá de la mera seguridad financiera.

Las grandes empresas, en particular, suelen tener infraestructuras informáticas muy complejas, con múltiples sistemas que se utilizan para controlar procesos y procesar datos. Tienen un gran número de interfaces con proveedores de servicios y otros colaboradores comerciales que utilizan el acceso remoto para el mantenimiento o suministran regularmente a la empresa nuevas actualizaciones. No hay que descuidar tampoco las normas del "home office", en virtud de las cuales los empleados acceden a los sistemas de la empresa desde su



XL Insurance

*Patrick Lee-Warner*  
IFL & Cyber Underwriter Manager, AXA XL Iberia

entorno informático doméstico. Éstas son sólo algunas de las posibles puertas de entrada que pueden conducir a incidentes cibernéticos.

Como aseguradora, nuestro objetivo debe ser contribuir de forma importante a la seguridad de nuestros clientes más allá de la propia póliza, para que puedan concentrarse en su actividad real. Las aseguradoras especializadas pueden ayudar a las empresas a analizar detalladamente su situación de riesgo, controlar los riesgos y sugerir medidas para minimizarlos, de modo que la probabilidad de que se produzcan pueda reducirse, en algunos casos considerablemente. Al mismo tiempo, muchos clientes disponen de recursos muy limitados o inexistentes que pueden actuar con rapidez y precisión en caso de incidente cibernético, por ejemplo, para detener la salida de datos y las interrupciones de la actividad, cumplir las obligaciones de información y, si es posible, evitar daños a la reputación. Las aseguradoras especializadas también pueden prestar una ayuda importante en este sentido.

### **¿LA IA CAMBIA LAS REGLAS DEL JUEGO DE LOS CIBERATAQUES?**

Para los ciberdelincuentes, la IA es una herramienta nueva y eficaz que puede utilizarse de diversas formas e incluso engañar a los ojos y oídos de la otra parte en una conversación digital. En estos intentos de fraude mediante falsificaciones complejas, la IA imita acústica y a veces incluso visualmente a una persona que induce a los empleados de una empresa a realizar pagos ilegales, por ejemplo, porque un responsable de la empresa les está dando supuestamente las instrucciones pertinentes mientras les mira a los ojos digitalizados en la pantalla. Estos métodos llevan los conocidos ataques del «falso presidente» a un nuevo nivel.

Para minimizar estos riesgos, pueden ser útiles instrucciones sencillas, como una llamada telefónica obligatoria a una línea de la empresa. Tales instrucciones específicas de seguridad deben estar definitivamente ancladas en una política interna. Sin embargo, las falsificaciones sólo representan una fracción de los intentos de ataque contra los que las empresas deben protegerse. Hoy en día, ya no es necesario tener conocimientos avanzados de programación para lanzar ataques de hac-

kers, ya que las herramientas correspondientes se ofrecen en la “darknet” como un servicio («ciberdelincuencia como servicio»). A menudo se proporcionan al mismo tiempo instrucciones sobre cómo utilizar las herramientas. Estas aplicaciones utilizan la IA, por ejemplo, para escanear Internet en busca de empresas menos protegidas o para identificar puntos débiles específicos en una empresa concreta antes de que se produzca el ataque propiamente dicho.

Sin embargo, no sólo los delincuentes utilizan la IA para sus propios fines. Varias aseguradoras ya están utilizando diversas herramientas de IA para el análisis y la supervisión en directo, con el fin de evaluar la situación de riesgo de los clientes y sugerir medidas preventivas contra las brechas de seguridad existentes.

En AXA XL, ya estamos trabajando en la evaluación automatizada de los documentos de riesgo presentados y llevamos algún tiempo realizando nuestras evaluaciones de seguridad a través de “Security Scorecard” con ayuda de la IA. “Security Scorecard” busca en Internet información sobre la situación de seguridad del cliente con el objetivo de encontrar posibles vulnerabilidades antes de que lo hagan los ciberdelincuentes y eliminarlas cuando sea posible. Esto incluye, por ejemplo, puertos expuestos, software obsoleto y vulnerabilidades conocidas. También analiza datos de otras fuentes diversas, como investigadores de seguridad, fuentes de inteligencia sobre amenazas y bases de datos de vulnerabilidades.

Al igual que la IA generativa de los delincuentes, la IA de las aseguradoras también es capaz de aprender y adaptarse. Por tanto, en mi opinión, la IA cambia más las reglas del juego en cuanto a la velocidad de la carrera entre el ataque a los activos de una empresa y las medidas de protección. Esta carrera siempre ha existido y, por desgracia, no tiene fin a la vista.

### **¿QUÉ PASA CON LA IA DEL PROPIO CLIENTE?**

Debido a los enormes beneficios que las organizaciones esperan obtener del uso de la IA para mejorar los procesos y diseñar productos y servicios, también se está convirtiendo en una parte importante de la cadena de valor de muchas empresas e industrias. Como los procesos respaldados por la IA dependen





en gran medida de los datos, pueden ser fundamentalmente susceptibles de sufrir daños cibernéticos, como el envenenamiento de datos y las violaciones de datos, que pueden provocar daños, multas y pérdida de reputación. En este contexto, también debe mencionarse el riesgo de sesgo, es decir, la desventaja causada por los algoritmos de IA utilizados. Además, las novedades regulatorias que inevitablemente surgen pueden suponer un riesgo para las empresas si, por ejemplo, un conocimiento o cumplimiento insuficientes de las nuevas normativas da lugar a reclamaciones por responsabilidad.

### **ASEGURABILIDAD**

En el debate sobre el creciente número y variedad de incidentes cibernéticos, surge una y otra vez la cuestión de si los riesgos concretos a los que se enfrentan las empresas a lo largo de sus cadenas de valor y suministro siguen siendo asegurables a largo plazo, sobre todo en vista del avance triunfal de la IA. Los riesgos incluyen la violación de datos, los fallos de seguridad de la red y la extorsión cibernética, como los ataques de “ransomware”. También puede haber costes de investigación y respuesta a incidentes, costes legales, costes de notificación, seguimiento del crédito de las personas afectadas y posiblemente incluso pérdidas por interrupción de la actividad, que pueden asegurarse.

Al igual que con los riesgos de catástrofes naturales, en rápido crecimiento, creo que en los próximos años será esencial una cooperación aún más estrecha entre clientes, corredores y aseguradoras. También en este caso, la transparencia y la prevención serán aún más importantes en el futuro, ya que la comunicación temprana y regular es la clave para optimizar significativamente la capacidad de recuperación.

La IA también desempeña un papel importante en la mejora de la transparencia, ya que puede analizar grandes cantidades de datos no estructurados, como texto, voz, vídeo e imágenes, a veces en tiempo real, acelerar los conocimientos y permitir decisiones más informadas en la gestión de riesgos y la suscripción.

La prevención eficaz contra los riesgos globales en rápida evolución, como el cibernético, no puede lograrse sin inversiones con visión de futuro y un criterio planificado. Además de las herramientas pertinentes ya mencionadas varias veces, las aseguradoras necesitan una red mundial de expertos, deben establecer colaboraciones firmes y, por último, pero no por

ello menos importante, promover la formación y el perfeccionamiento de los talentos. Por parte de los clientes, es necesario adoptar medidas de seguridad estructuradas basadas en los datos y conocimientos adquiridos sobre su propia situación de amenaza, para lo cual pueden contar con el apoyo de sus corredores y aseguradoras. Por ejemplo, les ayudamos a adaptar las mejores prácticas a su propia empresa cuando se trata de optimizar su infraestructura informática, las actualizaciones de seguridad informática, los requisitos para los proveedores y otros prestadores de servicios. También es especialmente importante la formación periódica de todos los grupos de personas relevantes, para que puedan reconocer e informar de los intentos de “phishing” en una fase temprana. La lista de posibilidades es muy larga, por eso es tan importante mantener un diálogo estrecho.

### **FALTA DE JÓVENES TALENTOS**

Una cuestión cada vez más importante en relación con la ciberresiliencia y el uso responsable de la IA es la escasez de jóvenes talentos. En el sector de los seguros llevamos varios años experimentando esta escasez por parte de los gerentes de riesgos, los corredores y las aseguradoras. Este punto también se debatió en el simposio de la GVNW. Esto es especialmente notable en líneas de negocio de rápido crecimiento, como la cibernética.

Las aseguradoras que quieran satisfacer la creciente demanda de soluciones cibernéticas y adelantarse a las amenazas deben asegurarse de que más jóvenes se interesen por una carrera en el sector de los seguros. Debemos captar y desarrollar talento. Por tanto, en relación con el tema de este artículo, la formación y el perfeccionamiento deben tener como objetivo dotar a los compañeros de la capacidad que necesitan para un futuro más influenciado por la IA. Debemos permitirles utilizar las nuevas posibilidades tecnológicas de forma que puedan centrarse en las áreas de su trabajo en las que sus habilidades humanas son cruciales.

Los riesgos asociados a la IA evolucionan tan rápido como los avances tecnológicos y las aplicaciones. Los gerentes de riesgos, los corredores y las aseguradoras tienen que estar siempre atentos a los avances, pensar en el futuro y trabajar juntos para encontrar soluciones a estos retos.

El espectro metafórico del título de este artículo no se desvanecerá en el aire.

9ª EDICIÓN - 2025/2026



# POSTGRADO EXPERTO EN GERENCIA DE RIESGOS

*Expertos en riesgos, líderes en soluciones*



UNIVERSITAT DE  
BARCELONA



16



*Sanae Blanco*  
Senior Underwriter  
Executive & Professional BHSI

## **Balance de un año cargado de retos y emociones para**

# **El mercado de Cyber**

*Durante este último año caracterizado por la inestabilidad geopolítica y por el auge de la inteligencia artificial generativa, han resurgido ataques de Ransomware significativos (más de un 18% de incremento comparado con los niveles de 2023, según informes como el Global Cyber Report publicado por Howden para 2024), a pesar de la mejora en la concienciación y en los controles de riesgos por parte de cada vez más empresas. Las amenazas siguen intensificándose y poniendo en jaque nuestros activos. Los ciberataques continúan siendo un motor económico muy rentable para los delincuentes.*



Esta siniestralidad experimentada en 2024 ha afectado a todo tipo de organizaciones y actividades. Desde grandes compañías del Ibex35, instituciones financieras y compañías de seguros, hasta infraestructuras críticas como; energéticas, entidades del sector sanitario y aerolíneas. También se han visto afectadas grandes compañías de retail (supermercados y textil), así como, organismos públicos; desde RTVE hasta ayuntamientos como el de Málaga, entre otros, pasando por universidades como la Complutense y hasta la propia DGT. Se espera que los sectores directamente relacionados con la situación geopolítica sigan siendo el foco de los atacantes debido a su capacidad para alterar la estabilidad de un país, con lo cual y como consecuencia de todo esto estaremos atentos a los posibles cambios en los tratados de reaseguro para 2025.

Cómo olvidar el mediático incidente CrowdStrike que provocó una alarma mundial en Julio, volviendo a planear sobre el mercado la incertidumbre del riesgo sistémico, cuestionando la agregación, debido a la vulnerabilidad como característica intrínseca de la tecnología.

Un año, además, en el que la continua intensificación de la regulación ha sido protagonista. El sector financiero y proveedores de servicios externos de TIC poniéndose a punto para dar cumplimiento al reglamento europeo DORA, que entrará en vigor el próximo 17 de enero de 2025 y que ha establecido el foco, en la resiliencia operativa de estos servicios y en la gestión de los riesgos inherentes de los proveedores. Mantener la disponibilidad e integridad de estas actividades frente a un ciberataque es clave para aportar seguridad y certidumbre a la economía de un país.

La Directiva de la UE, NIS 2, por su parte, ha sido recientemente incorporada a nuestras leyes nacionales el pasado octubre y está centrada en elevar el nivel general de ciberseguridad en “Entidades Esenciales” como las dedicadas a la energía, la salud, los transportes y las infraestructuras digitales. Así como, en “Entidades Importantes”, como empresas productoras de alimentos y servicios postales, abordando también y al igual que DORA, la

seguridad de la cadena de suministro, pero dentro de un contexto sectorial más amplio. Previendo sanciones estrictas por su incumplimiento (incluyendo multas de hasta el 2% de la facturación global anual para EE).

Todo lo anterior, unido a una cuestión que continúa siendo compleja y un reto: la todavía falta de una adecuada cuantificación del riesgo cibernético y el reconocimiento real de su exposición, especialmente en algunos sectores como el sanitario, el sector industrial, el sector hotelero o el sector de la construcción. Esto deja en ocasiones a ciertas empresas expuestas financieramente, tras un ataque, y a la vez puede generar ineficiencias en una parte del sector asegurador dedicado a asumir ese riesgo.

Esta falta de cuantificación eficaz del riesgo tiene implicaciones directas en la forma en la que las empresas asignan sus recursos de ciberseguridad a las áreas más críticas y, por lo tanto, en la continuidad de su operación, en sus cuentas de resultados y en su reputación dentro de la sociedad.

El reto continúa siendo encontrar un equilibrio, entre cada perfil de riesgo, el diseño de productos completos que cubran las demandas globales de los diferentes clientes y la adecuación técnica de las primas. Tratando de garantizar, entre todos, la sostenibilidad a largo plazo de un producto que ha demostrado ser clave para la supervivencia y para la continuidad de las operaciones de nuestro tejido empresarial, pero que, en el último año se ha visto comprometido, por un entorno altamente competitivo, que fomenta ajustes de primas en ocasiones muy difíciles de justificar desde un punto de vista de suscripción.

Todo esto, teniendo en cuenta el incremento en la frecuencia y en la sofisticación de la siniestralidad, puede llevarnos de nuevo a la reducción de capacidades por parte de algunas aseguradoras con estrategias menos largoplacistas, quedando sin margen alguno para la rentabilidad y generando líneas deficitarias. Desencadenando esto en la confusión por parte de los compradores, que asisten, a la gran volatilidad de los términos cada cierto tiempo.

18



AI

# IA en los Seguros de Riesgos Globales

*La inteligencia artificial (IA) está transformando la manera de gestionar los seguros de grandes riesgos. La mayoría de las líderes en seguros valora la IA como clave para el crecimiento, siendo evidente que las aseguradoras que la adopten tendrán ventajas frente a sus competidores.*

*Para poder capturar realmente el beneficio de la IA como elemento diferenciador es necesario poner foco en la calidad de los datos, que permitan un análisis adecuado de la información. El dato es un activo estratégico y un elemento diferencial de negocio. Dato es negocio, y sin dato no hay IA.*



*Carlos Villanueva Afán de Ribera*  
*Chief Operations & Data Officer – MAPFRE Global Risks*

Gracias a las técnicas de Big Data combinada a su capacidad para predecir, detectar distintos patrones y recomendar acciones, la IA se ha convertido en una **herramienta esencial para la rápida identificación, prevención y mitigación de riesgos**. La IA puede ser un “copiloto” perfecto en diferentes procesos críticos, tales como, verificación, automatización de procesos, suscripción, prevención, seguridad, modelización, simulaciones, etc.

La **verificación de datos** es un proceso crítico en la industria aseguradora. La IA puede automatizar y mejorar significativamente este proceso, reduciendo errores y acelerando el tiempo de respuesta. Por ejemplo, los algoritmos de aprendizaje automático pueden analizar documentos y registros para verificar la autenticidad de la información proporcionada por los clientes, detectando inconsistencias, reestructurando datos y reduciendo mucho los tiempos de análisis y procesamiento de la información.

La **automatización de procesos** mediante IA también está revolucionando la eficiencia operativa en el sector asegurador, optimizando gran parte de las tareas operativas y permitiendo concentrar esfuerzos en actividades de mayor valor añadido. Esto no sólo mejora la eficiencia, sino que también aumenta la satisfacción del cliente al reducir los tiempos de espera y mejorar la calidad del servicio.

La Suscripción es otra área donde la IA es un complemento perfecto. Los **modelos predictivos basados en IA** pueden evaluar el riesgo de manera más precisa, considerando una amplia gama de factores que los métodos tradicionales podrían pasar por alto. Igualmente, es de gran ayuda para el análisis de datos complejos y/o modelizaciones de escenarios catastróficos. Esto no sólo mejora la precisión de la Suscripción, sino que también permite a las aseguradoras ofrecer soluciones más personalizadas y competitivas.

Otra área crítica donde la IA está demostrando su valor es la prevención de incendios. Un claro ejemplo son los

**termosensores equipados con IA**, ya que pueden detectar cambios de temperatura y patrones de calor que podrían indicar un incendio inminente. Estos sistemas pueden alertar a los equipos de emergencia en tiempo real, permitiendo una respuesta rápida y efectiva que puede salvar vidas y reducir daños materiales.

Por su parte, la **verificación mediante grabaciones de vídeo** es otra aplicación innovadora de la IA en la gestión de grandes riesgos. Los algoritmos de visión artificial pueden analizar imágenes y vídeos para verificar la autenticidad de eventos y condiciones, eliminando la necesidad de desplazamientos físicos para inspecciones. Esto no sólo ahorra tiempo y recursos en los traslados, disminuye la huella de carbono de las compañías y reduce la exposición a riesgos laborales mediante la monitorización continua de las condiciones del entorno y el comportamiento de los trabajadores, sino que también permite detectar situaciones peligrosas y alertar en tiempo real a los supervisores antes de que ocurra un accidente. De este modo, se reducen las incidencias de lesiones.

Otro aporte relevante de la IA en la gestión de grandes riesgos lo encontramos en los **gemelos digitales**. Estas representaciones virtuales de sistemas físicos permiten la simulación y el análisis de diferentes escenarios. En el contexto de la gestión de grandes riesgos, una fábrica gemela, creada digitalmente, puede simular siniestros y evaluar el impacto de diferentes estrategias de mitigación. Esto permite a las empresas prepararse mejor para eventos adversos y optimizar sus planes de respuesta.

Para concluir, la inteligencia artificial está transformando la gestión de grandes riesgos en el sector asegurador: desde la verificación de datos y la suscripción de pólizas hasta la prevención de incendios y la seguridad en las actividades de nuestros clientes. La IA ayuda en la búsqueda de soluciones innovadoras que mejoran la eficiencia, reducen los riesgos y aumentan la seguridad. En MAPFRE Global Risks estamos trabajando en diferentes casos de uso que nos permiten la adopción progresiva de estas tecnologías, para continuar ofreciendo un servicio de calidad a nuestros clientes y mantenernos a la vanguardia de la industria.



# El auge del ciberseguro en un panorama de amenazas intensificadas

- *Según el cuarto informe anual de Howden sobre el mercado de los seguros cibernéticos, no hay indicios de que el panorama de riesgos de ciberdelincuencia vaya a disminuir.*
- *El análisis de Howden de los ataques registrados por el CSIS descubrió que cerca del 90% de los ataques tenían motivaciones políticas.*
- *Desde Howden Iberia, se ha observado un incremento de ataques como el ransomware.*

En ningún otro momento ha experimentado el mercado de los ciberseguros la actual combinación de condiciones: un panorama de amenazas intensificadas combinado con un mercado de seguros estable respaldado por sólidos controles de riesgo. Según el cuarto informe anual de Howden sobre el mercado de los seguros cibernéticos, no hay indicios de que el panorama de riesgos de ciberdelincuencia vaya a disminuir; así lo evidencian los índices de ransomware, la inestabilidad geopolítica y la proliferación de IA generativa.

El ciberseguro ha sido una de las áreas de seguros de más rápido crecimiento durante la última década. Por lo que ir un paso delante de los atacantes no solo hace que las organizaciones sean más resistentes a los ciberataques por motivación financiera, sino que también estén mejor preparadas para afrontar incidencias de mayor escala. Inestabilidad política

El entorno geopolítico cada vez más febril se suma a la sensación de incertidumbre. La ciberdelincuencia sigue cons-



tituyendo una enorme amenaza para las empresas de todo el mundo y hay pocos indicios de que su actividad vaya a remitir pronto, siendo su profesionalización una de las tendencias más marcadas e importantes de los últimos años.

Aunque muchos grupos de ciberdelincentes operan con independencia del respaldo estatal, ambos están a menudo interrelacionados. Prueba de ello son los crecientes niveles de ciberdelincuencia procedente de Rusia, así como los ataques a empresas e infraestructuras críticas por parte de grupos delictivos por motivos políticos.

Un análisis de Howden de los ataques registrados por el CSIS descubrió que cerca del 90% de los ataques (de abril de 2023 a marzo de 2024) tenían motivaciones políticas. Las potencias cibernéticas mundiales parecen haber aceptado que las cibercampañas concertadas patrocinadas por Estados, y a menudo agresivas, se han convertido en una norma.

Es probable que el alcance y la duración de las guerras en curso en Ucrania y Oriente Medio, junto con actividades de menor nivel dirigidas a socavar el proceso democrático en un año de elecciones importantes, tengan profundos efectos en la ciberseguridad mundial.

## **RIESGO Y RESILENCIA: RESURGIMIENTO DEL RANSOMWARE**

El ransomware sigue dominando el entorno de las ciberpérdidas. Un número cada vez mayor de ataques de ransomware implican ahora el robo de datos personales o comerciales sensibles con fines de extorsión, es decir, amenazando con filtrar datos al dominio público. Esto no sólo aumenta la complejidad de los incidentes, sino que también conlleva un mayor riesgo de daños a la reputación.

En los últimos 12 meses se ha observado la fragmentación de los grupos de ransomware, una mayor colaboración entre los piratas informáticos y un apoyo tácito de gobiernos hostiles.

Por su parte, las empresas que han invertido en controles de riesgo y gestión de crisis son ahora menos susceptibles de sufrir impactos materiales, lo que reequilibra las consideraciones de coste-beneficio para algunas empresas.

A medida que la cibernética hace honor a su dinámica reputación, el valor de los seguros se pone aún más de relieve, ya que incentivan y ayudan a aplicar una mejor higiene cibernética, refuerzan la resistencia e indemnizan las pérdidas.

## **LA IA GENERATIVA DENTRO DEL PANORAMA DE LAS CIBERAMENZAS**

A pesar del amplio consenso entre la comunidad de ciberseguridad y el mercado de seguros sobre el potencial transformador de esta nueva tecnología, tanto para las capacidades ofensivas como defensivas, hay mucha menos claridad sobre qué casos de uso demostrarán ser los más importantes y cuándo es probable que ganen tracción. No obstante, cada vez están más claras dos conclusiones emergentes sobre cómo la IA generativa remodelará el panorama de las amenazas en los próximos años.

En primer lugar, dados los incentivos geopolíticos y financieros, los agentes de amenazas sofisticados y respaldados por el Estado utilizarán la IA Generativa para perfeccionar sus tácticas, técnicas y procedimientos (TTP) con una eficacia y escala cada vez mayores. En febrero de 2024, Microsoft y Open AI revelaron que los actores de amenazas de los estados nación han estado utilizando ChatGPT para

facilitar las actividades de piratería establecidas, con una banda rusa, por ejemplo, llevando a cabo el reconocimiento de satélites. En segundo lugar, y lo que es más importante para el mercado de los seguros, la IA Generativa aumentará la agregación potencial, la gravedad y la frecuencia de las reclamaciones en áreas predecibles mediante la mejora de las capacidades de los hackers comerciales.

Los tecnólogos, los expertos en ciberseguridad y el mercado de seguros coinciden en general en que esta nueva tecnología transformará las capacidades ofensivas y defensivas, consideran que la IA generativa tiene más probabilidad de aumentar la frecuencia, la gravedad y la acumulación de las reclamaciones, pero también gracias a esta tecnología pueden implementarla a los controles de riesgo existentes, para repeler a los actores de amenazas.

Según el estudio de ciberseguridad de Howden, la IA generativa mejorará las capacidades de los actores de amenazas entre 2024 y 2026 en cinco dimensiones clave. Todos los tipos de atacantes, desde los agentes estatales altamente capacitados hasta los grupos de delincuencia organizada y los hackers menos cualificados, verán cómo la IA mejora sus capacidades. Más allá de esto, el impacto será muy matizado.

- **Hackers menos cualificados:** Este grupo es el que verá un mayor aumento de sus capacidades. Lo más importante es que muchos actores de amenazas novatos obtendrán acceso a herramientas, código e inteligencia que les permitirán empezar a piratear.
- **Grupos de delincuencia organizada:** Los grupos de ciberdelincuentes organizados y tecnológicamente avanzados se centrarán cada vez más en el pirateo más lucrativo, es decir, en atacar a las empresas más propensas a pagar grandes rescates con ataques sofisticados. Además, la IA generativa mejorará las capacidades de exfiltración al aumentar la velocidad y la precisión con la que se pueden identificar y robar datos de gran valor.
- **Actores estatales altamente capacitados:** Los hackers más sofisticados cuentan con el respaldo de Estados nación y siguen muy centrados en conflictos y objetivos geopolíticos más que en ganar dinero. No obstante,

estos actores podrían utilizar la IA Generativa para mejorar las capacidades de los programas maliciosos en caso de que cambien las prioridades, lo que a su vez supondría un mayor riesgo de propagación y agregación de pérdidas.

Para Howden, la IA generacional ofrece oportunidades tanto a los ciberatacantes como a los defensores y parece que tendrá un impacto significativo en el panorama de las amenazas al permitir ataques más avanzados por parte de actores sofisticados y reducir las barreras de entrada para los hackers novatos. La buena noticia es que las nuevas defensas impulsadas por la IA se están desarrollando a buen ritmo y que el uso eficaz de los controles de riesgo más tradicionales puede reforzar la resistencia.

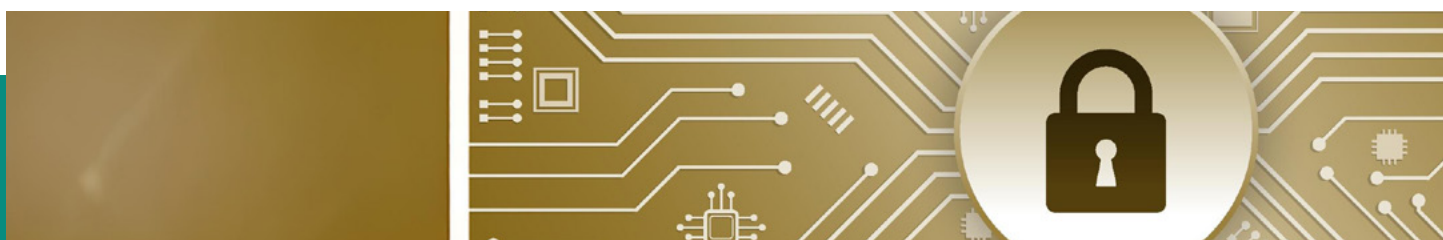
### IMPACTO ECONÓMICO DE LOS CIBERATAQUES

El impacto económico de los ciberataques varía, incluyendo costes directos como la recuperación de sistemas y pérdida de ingresos, y costes indirectos como daños a la reputación y posibles sanciones legales. La reputación de las compañías se ve gravemente afectada, lo que puede resultar en una fuga de clientes y una disminución de la confianza de los inversores, subrayando la importancia de una estrategia de ciberseguridad robusta.

### INCREMENTO DE LOS CIBERATAQUES POR TEMPORADAS

Durante la temporada de verano, las amenazas de ciberataques se intensifican significativamente, aprovechando la reducción de personal y las vulnerabilidades estacionales (la reducción de personal es en sí una vulnerabilidad). Así lo han identificado Howden Iberia, prueba de estos ataques se han evidenciado este verano con el incidente de CrowdStrike, que afectó a sistemas de Microsoft.

En años anteriores, se ha registrado un aumento de hasta el 30% en los incidentes de ciberseguridad durante la temporada de verano en comparación con el resto del año. Específicamente, durante el primer trimestre de 2024, se reportaron 841 incidentes de brechas de datos, un incremento del 90% respecto a los 442 incidentes del mismo período en 2023.





Patricia Fernández, directora de Cyber en Howden Iberia, declara: “Durante el verano, vemos un incremento notable en los ciberataques debido a la reducción de personal y las vacaciones. Es crucial que las empresas mantengan una vigilancia constante y refuercen sus estrategias de ciberseguridad para mitigar estos riesgos.”

Asimismo, el mes de noviembre de 2023 se destacó como el de mayor actividad de ciberdelincuencia en todo el año, impulsado por el aumento de la actividad durante el Black Friday y la proximidad de las festividades navideñas, lo cual evidencia la creciente sofisticación y volumen de los ataques dirigidos a las empresas que venden digitalmente. Las previsiones indican que estos ataques podrían seguir creciendo un 20% adicional en noviembre de 2024, lo cual genera inquietud sobre la seguridad de las plataformas de ecommerce, en un escenario donde los ciberdelincuentes se aprovechan del aumento en las transacciones digitales, especialmente durante eventos de alta actividad como el Black Friday.

### VULNERABILIDAD DE LOS NEGOCIOS ANTE LOS CIBERATAQUES

La vulnerabilidad de los negocios ante los ciberataques es una realidad que requiere atención y acción inmediata. Por ejemplo, la caída de los sistemas de Microsoft, causada por un fallo en una actualización de CrowdStrike, afectó a usuarios y empresas globalmente, provocando así la cancelación de más de 2.000 vuelos y problemas en bancos y servicios, lo que generó pérdidas millonarias. Este incidente destaca la vulnerabilidad de los sistemas tecnológicos, la ausencia de un control exhaustivo en procesos de actualización de software y la importancia de estrategias de ciberseguridad robustas.

Adrián Feliú, responsable de Ingeniería Cyber en Howden Iberia, comenta: “El incidente con Microsoft y CrowdStrike es un claro recordatorio de lo vulnerable que es nuestro ecosistema digital y lo conectado que está con nuestra vida diaria. Como respuesta a este incidente muchas compañías tomaron la mala decisión de desactivar la protección activa de CrowdStrike para continuar con su operativa de negocio sin interrupciones, sin darse cuen-

ta de que pudieron dejar la ventana abierta a atacantes, que, una vez dentro, habrían iniciado la fase de reconocimiento de red para acabar con un ataque masivo en los próximos meses.”

### CÓMO SE PREPARA EL SECTOR DE LOS CIBERSEGUROS FRENTE A ESTE PANORAMA EN AUMENTO

Para enfrentar estos riesgos, el sector de los ciberseguros se prepara meticulosamente. Se realizan evaluaciones de riesgos estacionales y se refuerzan los equipos de respuesta a emergencias cibernéticas, aumentando los recursos para asegurar una vigilancia continua. Además, se intensifican las iniciativas de educación y capacitación para los clientes, proporcionando herramientas esenciales para proteger sus sistemas y datos durante el verano.

Los sectores más vulnerables incluyen el público, financiero, industrial, retail y sanitario. Estos sectores son particularmente atractivos para los ciberdelincuentes debido a la naturaleza crítica de los datos que gestionan y las complejidades de sus sistemas tecnológicos. La gran cantidad de datos personales, los sistemas de TI frecuentemente desactualizados y la convergencia de tecnologías operativas incrementan la susceptibilidad de estos sectores.

Las empresas adoptan varias medidas clave de seguridad, como el uso de herramientas avanzadas de detección y respuesta a amenazas, programas regulares de corrección de vulnerabilidades y métodos de autenticación seguros. Además, educan a sus empleados, mantienen copias de seguridad y gestionan cuidadosamente el acceso a cuentas sensibles, segmentan redes y actualizan sistemas. Con estos esfuerzos, las empresas buscan no solo prevenir ataques, sino también minimizar el daño en caso de que ocurran, facilitando una recuperación rápida y efectiva.

En conclusión, el mercado de los ciberseguros se enfrenta a un entorno de riesgos sin precedentes que exige respuestas innovadoras y dinámicas. La creciente amenaza de la ciberdelincuencia impulsada por los factores mencionados ha convertido al ciberseguro en un sector de crecimiento acelerado, con una función clave en la resiliencia de las organizaciones frente a ciberataques.

DESCARGA  
EL INFORME COMPLETO  
PINCHANDO AQUÍ

24

AI



*Juan Carlos  
Martínez Rodríguez  
Chief Data and AI Officer*

# Inteligencia Artificial: Nuevos Desafíos y Oportunidades en el Sector Asegurador

EN LA ACTUALIDAD, LA INTELIGENCIA ARTIFICIAL (IA) E INTELIGENCIA ARTIFICIAL GENERATIVA (IA GEN) HA REVOLUCIONADO DIVERSOS SECTORES ECONÓMICOS, ENTRE ELLOS, EL SECTOR ASEGURADOR. LA VELOCIDAD DE ADOPCIÓN DE ESTA TECNOLOGÍA HA PLANTEADO PREGUNTAS CRUCIALES: ¿CÓMO GARANTIZAR UN RETORNO DE LAS INVERSIONES EN IA?, ¿CUÁLES SON LOS RIESGOS ASOCIADOS A SU IMPLEMENTACIÓN Y CÓMO GESTIONARLOS DE MANERA EFECTIVA? ¿QUÉ MEDIDAS DEBO APLICAR PARA CUMPLIR CON LA LEGISLACIÓN (LEY EUROPEA SOBRE IA)? ESTAS PREOCUPACIONES NO SON EXCLUSIVAS DEL SECTOR ASEGURADOR, SINO QUE SE EXTIENDEN A TODOS LOS ÁMBITOS EMPRESARIALES.



# AON

**Belén Vílchez Morales**

Director | Specialty Financial Lines & Intellectual Property

## RIESGOS DE LA IA

Las empresas están cada vez más preocupadas en cómo mitigar los riesgos relacionados con la IA. Entre las inquietudes más comunes destacan: la seguridad de los datos para que las IAs no revelen información confidencial, el impacto en la privacidad por el uso de datos personales o privados empleados para entrenar modelos, la infracción de derechos de autor y propiedad intelectual, la ética por la utilización de cierta información para entrenar modelos, uso de sistemas transparentes y sostenibles, los daños que pueden originar la toma de decisiones o comunicaciones automatizadas, y el riesgo de que las soluciones de IA no alcancen los resultados esperados.

## REGULACIÓN

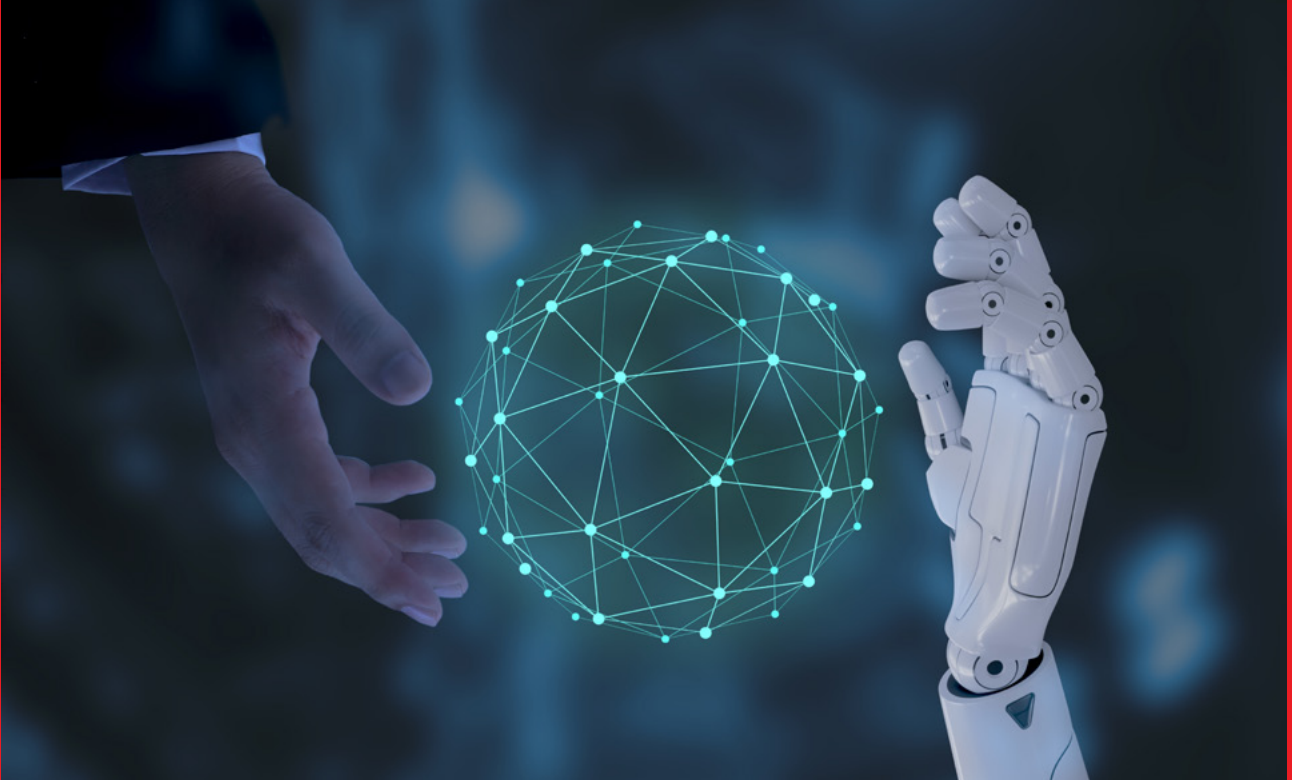
Europa ha querido ser pionero en la regulación de la IA aprobando el Reglamento (UE) 2024/1689 que entró en

vigor el 1 de Agosto de 2024 (y que será aplicable en su mayoría desde el 2 de Agosto de 2026), por el que se establecen normas armonizadas en materia de inteligencia artificial.

Esta innovadora norma ha generado cierto desconcierto en las obligaciones de las empresas y consecuencias de su implementación, ya que el Reglamento quiere establecer obligaciones a proveedores y usuarios de la IA en función del nivel de riesgo que la misma presente. Por lo que surge una primera obligación que es la evaluación de la IA, catalogando los riesgos en inaceptables si suponen un riesgo para las personas, o de alto riesgo si afectan negativamente a la seguridad o derechos fundamentales.

Los Estados miembros tendrán que establecer sanciones efectivas, proporcionadas y disuasorias, aunque el Reglamento avanza como umbrales (En su rango menor para PYME 's) las siguientes cuantías:

| ASUNTO  | SANCIÓN   |
|---|---|
| Infracciones de prácticas prohibidas o incumplimientos relacionados con los requisitos sobre datos;   | Hasta 35 millones de euros, o el 7 % del volumen de negocios anual    |
| Incumplimiento de cualquiera de los demás requisitos u obligaciones del Reglamento;   | Hasta 15 millones de euros o el 3% del volumen de negocios anual      |
| Suministro de información incorrecta, incompleta o engañosa a los organismos notificados y a las autoridades nacionales competentes en respuesta a una solicitud; | Hasta 7,5 millones de euros, o el 1,5 % del volumen de negocios anual |



### **APLICACIONES PRÁCTICAS DE LA IA**

Se habla de la cuarta revolución industrial refiriéndose a la tripla IA, Blockchain y computación acelerada. La IA ya está transformando múltiples áreas de negocio: Desde el desarrollo de productos personalizables (hiperpersonalización), hasta la capacidad de ofrecer precios dinámicos basados en el comportamiento del cliente. Asimismo, el uso de IA para realizar evaluaciones predictivas, simulación de escenarios y mejorar la gestión de riesgos operacionales está permitiendo a las empresas ser más ágiles, flexibles, y precisas en sus estrategias, obteniendo además optimización de costes.

Las aplicaciones de la IA son inmensas, aunque podemos destacar que, ciertos sectores como son el sector financiero, industrial, educación o salud tienen mayor implementación de la IA; destacando algunos usos clave:

- En el sector asegurador y financiero, una de las principales preocupaciones es la detección de fraude mediante IA. Además, la IA está desempeñando un papel clave en la detección y gestión de riesgos emergentes, lo que permite a las aseguradoras adelantarse a posibles catástrofes medioambientales, ciberataques, situaciones geopolíticas extraordinarias, o crisis financieras.

- En el sector industrial/energía/construcción destaca la mejora en la cadena de suministro al poder analizar datos de producción y demanda en tiempo real, así como la mejora de la seguridad al poder incorporar IA en detección de movimientos y evitar accidentes laborales o analizar patrones de fallo en máquinas.
- En el ámbito de la salud, la IA se puede usar para optimizar la eficacia de los tratamientos, acelerar el diagnóstico médico y mejorar la toma de decisiones clínicas.

### **¿CÓMO MITIGAR Y TRANSFERIR ESTOS RIESGOS?**

Para concluir, la Inteligencia Artificial se está convirtiendo en un activo crucial para la competitividad y flexibilidad empresarial. Sin embargo, con grandes oportunidades vienen también grandes riesgos, y productos aseguradores pueden ser clave para ofrecer la seguridad que las empresas necesitan en este nuevo entorno tecnológico. En esta labor es clave que consulte con su asesor de seguros/broker de confianza para analizar herramientas y servicios de mitigación o determinación de estos riesgos, analizando cuáles pueden ser transferibles al mercado asegurador, y qué nuevos productos aseguradores pueden ayudarse en su estrategia de riesgos.





# 35

# CONGRESO AGERS

Madrid

SAVE THE DATE

26.06.2025

PINCHA AQUÍ



agers



## ENTREVISTA

**“El seguro ciber es la clave en un entorno de riesgos crecientes”**

**RESPONDE**  
**AGUSTÍN DE LA CUERDA,**  
DIRECTOR GENERAL DE ALLIANZ  
COMMERCIAL PARA IBERIA

**ENTREVISTA**  
**JUAN GAYÁ,** VICESECRETARIO  
DE AGERS Y GERENTE DE RIESGOS Y  
SEGUROS GRUPO EL CORTE INGLÉS



agers







**JUAN GAYÁ:** Hace unos pocos años en determinados foros se llegaba a plantear si el seguro ciber acabaría desapareciendo. Las condiciones para contratar exigían superar los cuestionarios con sobresaliente, las primas eran elevadísimas y las capacidades muy limitadas. ¿Cómo vivisteis esa época en Allianz Commercial?

**AGUSTÍN DE LA CUERDA:** Una parte de nuestro valor añadido para el cliente es invertir en conocimiento técnico y aplicarlo para dar las mejores condiciones posibles con un enfoque estable en el largo plazo. Más que en cuestionarios, en Allianz Commercial creemos en la colaboración permanente con el cliente en todos los ámbitos, intercambiando conocimiento, gestionando juntos el riesgo y con condiciones estables.

En este caso, el punto crítico en el mercado fue la gestión del cúmulo. En Allianz Commercial apostamos por la estabilidad, gestionando la capacidad con prudencia pero manteniendo la colaboración y el apoyo al cliente.

**JUAN GAYÁ:** Los requisitos que solicitáis las aseguradoras a grandes empresas para aceptar este riesgo son muy exigentes y probablemente difíciles de alcanzar por PYMES. ¿Existen diferencias en estos en función de la dimensión de la empresa? ¿Cuáles son estas? ¿Cómo puede ayudar un asegurador a una PYME en el proceso de adecuación del riesgo para que sea asegurable?

**AGUSTÍN DE LA CUERDA:** Es cierto que las PYMES requieren un planteamiento específico. La exposición es menor por su volumen, pero el nivel de asesoramiento y los servicios por parte de su asegurador son muy importantes. En definitiva, requieren de servicios de prevención y gestión de siniestros adaptados a sus necesidades.

Algunas veces vemos que son conscientes del daño posible, pero no tanto de las responsabilidades. Apoyarles en el conocimiento integral del riesgo, medidas de prevención y cómo mitigar las consecuencias de un siniestro son un valor indispensable.

Cada vez más nuestras PYMEs son conscientes, y esto supone un extraordinario potencial de crecimiento en este segmento, que tiene un nivel de aseguramiento con margen de mejora.

**JUAN GAYÁ:** Podemos considerar como seguros básicos que debería tener contratada cualquier empresa el de responsabilidad civil, el de daños e incluso el de D&O. ¿El de ciber debería formar parte de este programa básico de seguros? ¿Va camino de serlo?

**AGUSTÍN DE LA CUERDA:** Sin duda. En el Barómetro de Riesgos de Allianz de 2024, el 38% de la empresas resaltaron los incidentes ciber como una de sus principales preocupaciones. El número va al alza, estaremos atentos al Barómetro de 2025. Asimismo, en el informe "Cyber Security Resilience 2024" de Allianz Commercial se menciona que en tan solo un año la frecuencia de siniestros superiores a 1 millón de euros aumentaba un 14%, y el coste medio lo hacía un 17%.

Hablamos de un riesgo que evoluciona, con escenarios cada vez más sofisticados. Por ejemplo, tenemos escenarios de ransomware que evolucionan hacia amenazas de data privacy. Es un ejemplo claro de colaboración necesaria entre cliente-intermediario-asegurador, por ello hay que ir adaptando nuestros productos a riesgos que evolucionan de forma extraordinariamente rápida.

Sí vemos esta tendencia en el mercado, en todos los segmentos. Otras líneas de negocio son maduras y las necesidades evolucionan más lentamente, sobre todo si no requieren una gestión multinacional o utilizan nuevas tecnologías. Cuando hablamos de ciber, queda mucho por hacer. Se trata de una necesidad del cliente que los aseguradores y mediadores debemos trabajar para cubrir en el corto plazo.

**JUAN GAYÁ:** Estamos de acuerdo que este seguro debería considerarse básico, al tratarse de un riesgo generalizado y que afecta de forma importante a cualquier empresa, pero ¿existen determinadas tipologías de negocio de las que vosotros o el mercado en general tenga poco apetito? ¿Qué podría hacer una empresa que no consiga colocar su riesgo en el mercado teniendo buenas medidas de protección/recuperación?

**AGUSTÍN DE LA CUERDA:** Una empresa que tenga un buen conocimiento del riesgo, con medidas adecuadas de protección y recuperación, tendrá en general una buena respuesta del mercado. Durante el diálogo cliente-media-





dor-asegurador, es muy importante llegar a un entendimiento profundo de la exposición y explicar cómo estamos gestionando el riesgo.

En casos excepcionales, especialmente sensibles, tal vez los productos habituales no sean la solución. En ese caso, a través de la transferencia alternativa de riesgos (ART) se pueden diseñar soluciones plurianuales, a veces multilínea, que llegan a cubrir una amplia gama de riesgos incluyendo casos excepcionales de ciber. No es lo frecuente, pero en casos complejos puede ser la solución. En ese caso la experiencia y solidez técnica del asegurador es clave. La experiencia evita sorpresas.

**JUAN GAYÁ:** Pasemos ahora a un bloque de preguntas relacionadas con los siniestros, ¿cuáles son las coberturas que consumen más capital? ¿Y cuáles las más frecuentes?

**AGUSTÍN DE LA CUERDA:** Ransomware continúa ocupando el 58% de la siniestralidad, considerando solo los siniestros de más de 1 millón de euros, aunque el problema no es solo financiero. Tiene un enorme coste reputacional, como hemos visto en casos recientes en diferentes países.

El problema cada vez se vuelve más sofisticado, utilizando inteligencia artificial para los ataques. También utilizan

extorsiones de segundo y tercer nivel, aprovechando los datos para atacar a clientes y proveedores. Aquí es interesante recalcar que, cuando existe un programa de prevención con la colaboración del asegurador y el mediador, la respuesta es mucho mejor.

Una tendencia interesante son las reclamaciones por violación de datos, que no son consecuencia de un ataque. Asimismo, una tendencia a monitorizar por parte de las aseguradoras y los clientes es la recopilación de datos y su procesamiento, o la utilización de datos biométricos (todas ellas sin cumplir completamente con la regulación). En Estados Unidos ya son tendencia las Class Actions, y en Europa debemos prestar atención para prevenir estos escenarios.

**JUAN GAYÁ:** Con aquellos siniestros de importancia en los que se han activado vuestras pólizas, ¿qué partidas del daño que ha sufrido el asegurado ha quedado sin cubrir? En general, ¿los límites contratados han sido suficientes?

**AGUSTÍN DE LA CUERDA:** Normalmente los límites contratados son suficientes y las coberturas son correctas en el mercado actual. Sin embargo, debemos tener en cuenta la evolución extraordinariamente rápida de estos riesgos y



su impacto creciente. Por ello, desde Allianz Commercial recomendamos revisar coberturas y límites en cada renovación.

El coste medio de una violación de datos alcanzó un récord de \$4.9mn en 2024, con cifras más altas en mercados como Estados Unidos (\$9.36mn), lo que sugiere la necesidad de revisar límites y coberturas periódicamente.

También es importante tener en cuenta lo que no es asegurable. El daño reputacional o la pérdida de mercado que puede conllevar un incidente como ransomware o de pri-

vacidad de datos, puede ser extraordinariamente importante. Por ello, reitero una vez más que la prevención es más importante que nunca en esta línea de negocio.

**JUAN GAYÁ:** Muchos de los siniestros se producen no por un ataque directo al asegurado, sino a través de alguno de sus proveedores. ¿Qué peso tienen estos siniestros frente a los ataques directos? ¿Se consigue recuperar una parte significativa de la indemnización al repetir contra estos?

**AGUSTÍN DE LA CUERDA:** Cada compañía es un ecosistema, con una conectividad creciente y sistemas cada vez más sofisticados de gestión de datos. ¡En 2025 se esperan 200 zettabytes, 50% en la nube! Si bien algunos gastos pueden ser recuperados, esto depende de las circunstancias específicas y de la capacidad de las empresas para implementar acuerdos sólidos con proveedores. En este contexto, la falta de controles básicos en la cadena de suministro ha sido un factor clave en siniestros recientes.

Tal y como mencionaba, el ransomware evoluciona hacia la extorsión de segundo y tercer nivel, y podemos ser perfectamente una víctima más de un incidente en un proveedor. En definitiva, la vulnerabilidad de la compañía viene del eslabón más débil de ese ecosistema, donde la gestión de proveedores es un punto crítico. Un dato relevante es que el 40% de las violaciones de datos afectaron a diferentes entornos, como almacenamientos de datos en la nube privados y públicos. Sin embargo, la responsabilidad se mantiene con la compañía, por este motivo la gestión de proveedores se convierte en un factor indispensable.

**JUAN GAYÁ:** La gestión de un siniestro ciber se diferencia de siniestros que podamos considerar más tradicionales, ¿cuáles serían algunas de estas diferencias?

**AGUSTÍN DE LA CUERDA:** Hablamos de siniestros muy diferentes. En este punto, la experiencia con un equipo sólido de Siniestros es fundamental. Los siniestros de ciber requieren una respuesta rápida y coordinada, que incluye aspectos técnicos, legales, regulatorios y de comunicación. A diferencia de los siniestros tradicionales, éstos afectan no solo a la empresa, sino también a terceros, y a menudo involucran sanciones regulatorias y riesgos reputacionales.





Una de las principales diferencias entre ambos es la rapidez en la atención y la importancia de una coordinación compleja. Involucrar a los técnicos de Seguridad de la Información es clave, pero requiere también la participación de asesores legales y forenses, notificaciones a la Agencia Española de Protección de Datos, autoridades y un plan de comunicación.

En definitiva, son escenarios complejos con múltiples roles, una comunicación difícil y múltiples perspectivas, que en ocasiones cuenta con un lenguaje muy especializado. Un equipo de siniestros del asegurador con experiencia que pueda colaborar tiene un valor extraordinario.

**JUAN GAYÁ:** Sigamos con un tema de moda en estos momentos, la IA. Esta permite mejorar la protección a las empresas, pero también facilita los ataques a los criminales. Y lo que se suele decir es que los malos siempre van por delante de los buenos. ¿Esto va a tener un impacto en las pólizas (p.ej. nuevas coberturas, exclusiones, nuevos criterios para seleccionar el riesgo, impacto en la fijación de precios...)?

**AGUSTÍN DE LA CUERDA:** Según McKinsey, el 65% de las compañías aseguran utilizar IA. No es una sorpresa a estas alturas, donde vemos como, poco a poco, la integramos incluso en nuestra vida personal. Con múltiples aplicaciones, podemos asegurar que es parte de nuestro futuro.

Aunque es cierto que tiene una parte compleja y complicada. Por un lado, hemos comentado que aumentan los casos de violación de datos sin ataque. La IA incrementa este

riesgo, donde pueden procesarse o compartir datos que incumplan la regulación. Por otro lado, los hackers utilizan IA para realizar ataques más sofisticados. Desde este punto de vista, la fuerza se convierte en una amenaza.

Es importante que esta tendencia se refleje en la evolución de las pólizas para mantener al cliente protegido. Como aseguradores tenemos que conseguir entender la exposición y cuantificarla para poder aceptarla y poner precio. Debemos tener ese compromiso de mantener las pólizas actualizadas.

**JUAN GAYÁ:** La última pregunta para terminar. Aunque ya es generalizada la concienciación y los medios que ponen las empresas en relación con el riesgo ciber, siguen aumentando el número de incidentes. ¿Cómo veis el futuro de este ramo? ¿Y en términos de rentabilidad?

**AGUSTÍN DE LA CUERDA:** Hemos comentado que es un riesgo de evolución rápida, con incidentes crecientes. Pero también vemos que la colaboración cliente-mediador-asegurador tiene realmente buenos resultados, por ello debemos continuar.

Vemos un interés creciente en todos los segmentos de clientes, incluso en PYMES, lo que supone una oportunidad para mediadores y aseguradores.

Es importante que pongamos el foco en el corto plazo, pues actualmente vemos ciclos de precio que no tienen sentido. Si colocamos al ramo en pérdidas de forma recurrente, al final puede dejar de ser interesante para los aseguradores.

*Jorge Nadel*  
Sales Executive de Riskconnect



## Integra la IA en tu marco de ERM

**Esfuézate por tener  
el mismo marco para  
todos tus riesgos**

**“Risk  
under  
one roof”**

*Utilizar la IA en la gestión de riesgos puede dar un poco de miedo porque hay muchas incógnitas. Las posibles eficiencias y perspectivas son ciertamente tentadoras, pero ¿son los riesgos lo suficientemente significativos como para ser un factor decisivo?*







La verdad es que la IA generativa puede mejorar en gran medida sus esfuerzos de gestión de riesgos si se aplica con prudencia. Alrededor del 90% de las organizaciones de servicios financieros encuestadas por Risk.net afirmaron que la IA es una oportunidad para el sector, la empresa y su función. Pero, curiosamente, otra encuesta realizada por Riskconnect reveló que más de nueve de cada diez empresas de diversos sectores prevén amenazas significativas de la IA.

La IA generativa es una herramienta. Y como cualquier herramienta, su valor depende de cómo se utilice. ¿Qué pretende conseguir? ¿Qué objetivos pretende alcanzar con la nueva tecnología? ¿Busca sobre todo acelerar los procesos? ¿O busca descubrir nuevas perspectivas?

La Dra. Ariane Chapelle, experta en riesgo operacional e invitada habitual de Risk@Work, advierte que no se debe crear un marco independiente para gestionar el riesgo de la inteligencia artificial. “Integra la IA en tu marco de ERM. Esfuérzate por tener el mismo marco para todos tus riesgos – risk under one roof”, afirma. “Tienes que ser muy firme en tus objetivos para ver las incertidumbres en torno a esos objetivos”.

## IMPACTO EN LOS RIESGOS

La IA reducirá algunos riesgos de proceso y precisión con la automatización, como el error humano al introducir datos manualmente. Puede analizar cantidades masivas de datos y texto para ayudar a comprender el riesgo a un nivel más profundo que puede utilizarse para orientar la estrategia.

Sin embargo, puede añadir otros riesgos que hay que controlar. En ocasiones, la tecnología puede “alucinar”, es decir, responder a preguntas con información inventada. La verificación humana y el sentido común pueden frenar es-

tas respuestas antes de que se utilicen para fundamentar decisiones.

El sesgo es otro riesgo a tener en cuenta. La IA generativa utiliza información histórica para crear nuevos contenidos. El problema es que lo que era aceptable hace una década puede no serlo hoy.

La privacidad de los datos también es un riesgo importante a tener en cuenta. Sepa con qué se entrena el modelo y cómo se utilizarán sus datos. Los grandes modelos lingüísticos, como ChatGPT, capturan todo lo que se dice y lo incorporan al modelo. Sea consciente de la información que comparte fuera de su organización. No querrá que sus conocimientos exclusivos acaben en manos de sus competidores.

Es importante no sobrestimar ni subestimar el poder de la IA. Por ejemplo, no se puede alimentar una pila de datos y esperar que prediga el mayor riesgo operativo del próximo año como una especie de adivino tecnológico. Tampoco hay que suponer que sólo generará un montón de información inútil o incluso falsa, por lo que no merece la pena.

## IMPACTO EN LAS PERSONAS

¿Le sustituirá la IA? Depende. Como cualquier nuevo avance tecnológico, la IA supondrá el fin de algunos trabajos, pero creará otros.

La IA puede realizar tareas administrativas mejor que los humanos. También puede analizar datos, encontrar patrones e idear soluciones más rápido que cualquier ser humano.

Pero por muy deslumbrante que pueda ser la IA, no se puede aceptar automáticamente su resultado como la últi-

ma palabra. Los humanos seguirán siendo necesarios para revisar, validar y refinar las respuestas que genera la IA. Y los humanos son los encargados de interpretar y aplicar los conocimientos descubiertos por la IA.

Considere el resultado proporcionado por la IA como un punto de partida, una base sobre la que construir más conocimiento o pensar de forma diferente sobre un tema. Corresponde a las personas que trabajan directamente con la IA aportar sus mejores cualidades de pensamiento humano para perfeccionar el contenido, el tono y la voz a fin de adaptarlos a la organización.

La supervisión humana es esencial. De hecho, es tan esencial que la UE la codificó en su Ley de IA de la UE. Esta legislación pionera es la primera a nivel mundial que establece normas para el uso responsable de la IA, incluida una supervisión humana adecuada y una ciberseguridad sólida. En la mayoría de los casos, la IA supondrá más una redistribución o reconversión del talento que una destrucción de empleo. Aquellos que estaban haciendo trabajos que ahora realiza mejor la IA pueden agradecer la oportunidad de aplicar sus conocimientos y su capacidad de pensamiento a un uso mayor.

## DÓNDE UTILIZAR LA IA EN LA GESTIÓN DE RIESGOS

La IA generativa destaca en el análisis de una gran cantidad de información para responder instantáneamente a una pregunta formulada por un ser humano. Puede encontrar ideas, puntos en común, tendencias y conexiones a la velocidad del rayo. Puede simplificar datos complejos y traducir información técnica al lenguaje cotidiano. Y lo hace con mucha más rapidez y precisión que las personas.

En la gestión de riesgos, considere la posibilidad de utilizar la IA generativa para:

- Automatizar las pruebas de control.
- Ordenar, clasificar y organizar datos.
- Analizar datos no estructurados.
- Detectar posibles valores atípicos.
- Descubrir correlaciones, tendencias y riesgos emergentes.
- Modelar escenarios y simulaciones para comprender el impacto de los riesgos.
- Recopilar y analizar datos de riesgos de terceros y amenazas potenciales.



## EMPEZAR AHORA

Con una tecnología que cambia las reglas del juego a una velocidad vertiginosa, puede ser difícil decidir cuál es el momento adecuado para lanzarse. Sin duda, existen muchas incertidumbres y es comprensible que prefiera esperar a saber más antes de comprometerse con la tecnología. Pero corre un riesgo aún mayor si no integra ahora la IA en sus procesos de gestión de riesgos. La ventaja competitiva será para aquellos que aprovechen el poder de la IA más rápidamente.

Si se utiliza correctamente -con las personas, los procesos y la gobernanza adecuados-, la IA en la gestión de riesgos puede ser un activo empresarial sin parangón. Funcionará de forma más eficiente si se encarga de las tareas rutinarias. Funcionará de forma más eficaz, liberando recursos para analizar, supervisar y responder mejor a los riesgos. Y será más ágil, listo para afrontar nuevos retos y aprovechar nuevas oportunidades de negocio.

Para obtener información más detallada sobre la IA en la gestión de riesgos, descargue el libro electrónico *Governance, Risk, and Compliance: The Definitive Guide* y eche un vistazo a las soluciones de Inteligencia Artificial de Riskconnect.

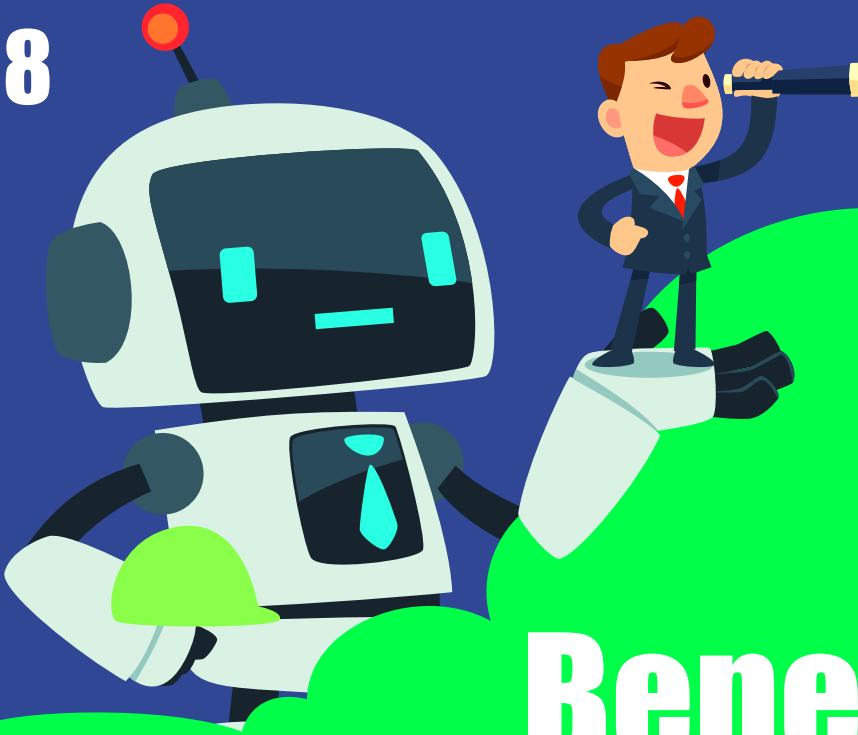


# "TU RED DE CONTACTOS PROFESIONAL"

Más de 16.000 personas unidas a la  
comunidad de AGERS en LinkedIn



38



# Beneficios de la IA para la Gestión de Riesgos

*La inteligencia artificial se refiere a sistemas o máquinas que muestran una inteligencia similar a la humana al realizar tareas complejas, aprender y adaptarse a nuevas situaciones. En el contexto de la gestión de riesgos, la IA permite analizar en profundidad grandes volúmenes de datos para identificar y predecir riesgos con mayor rapidez y derivar las medidas adecuadas. Hoy en día, las empresas no sólo tienen que identificar y minimizar los cada vez más diversos riesgos existentes, sino también anticiparse a las posibles amenazas futuras. Aquí es donde entra en juego la inteligencia artificial (IA), ya que tiene el potencial de cambiar fundamentalmente la gestión de riesgos.*

## **IA EN LOS RIESGOS DE SEGURIDAD**

Los departamentos de seguridad desempeñarán un papel fundamental en la gestión de la información usando la IA. Hace tiempo que ya se utilizan herramientas de IA en el ciclo de inteligencia, en particular en las etapas de recopilación y procesamiento de datos. Ahora, los equipos de inteligencia deben adoptar una IA más potente y, al mismo tiempo, gestionar los inconvenientes rela-

cionados con la información errónea o desinformación de gran volumen, ritmo acelerado y casi indetectable. La información fiable será un algo imprescindible en 2025, y los equipos de inteligencia que puedan equilibrar la velocidad impulsada por la IA con el análisis humano (idealmente impulsado por una red confiable de personas en el terreno) serán un facilitador fundamental, en particular en el espacio de resiliencia ante las crisis, donde la anticipación de los riesgos es clave.





*Santiago Álvarez de Toledo*  
*Country Manager en España y Portugal de International SOS*

### IA EN LOS RIESGOS DE SALUD

La IA ha comenzado recientemente a asumir un papel principal en la atención médica. Existen diversas capacidades en las que la IA está surgiendo como un elemento innovador para el sector médico. A continuación, se muestran algunos ejemplos que se están usando en la actualidad:

**Radiología:** se están desarrollando soluciones de IA para automatizar el análisis y el diagnóstico de imágenes. Esto puede ayudar a resaltar áreas de interés en una exploración para un radiólogo y también está ayudando a permitir una interpretación instantánea en geografías desatendidas o fuera del horario laboral.

**Identificación de riesgos del paciente:** al analizar grandes cantidades de datos históricos de pacientes, las soluciones de IA están apoyando en tiempo real a los médicos para ayudar a identificar a los pacientes en riesgo.

**Atención primaria/Triaje:** varias organizaciones están trabajando en soluciones directas al paciente para clasificar y brindar asesoramiento a través de una interacción basada en Telemedicina (videollamadas). Esto proporciona un acceso rápido y escalable para preguntas básicas y problemas médicos y está ayudando a evitar viajes innecesarios al médico en poblaciones en áreas remotas o desatendidas.

Las mejores oportunidades para la IA en la atención médica durante los próximos años son los modelos híbridos, donde los médicos reciben apoyo en el diagnóstico, la planificación del tratamiento y la identificación de los factores de riesgo, pero mantienen la responsabilidad final por la atención del paciente. Esto dará como resultado una adopción más rápida por parte de los proveedores de atención médica al mitigar el riesgo percibido y comenzar a ofrecer mejoras mensurables en los resultados de los pacientes y la eficiencia operativa a escala.





# Una Mirada al Futuro de la Gestión de Riesgos

## Riesgos Tecnológicos, Cibernéticos e Inteligencia Artificial

*La tecnología avanza a pasos agigantados y, junto con ella, los riesgos asociados a su uso. Los riesgos tecnológicos y cibernéticos han escalado en complejidad y frecuencia, afectando tanto a grandes corporaciones como a PYMES y autónomos. La irrupción de herramientas de inteligencia artificial (IA) plantea una oportunidad de transformación en la gestión de riesgos.*



**Sergio Gómez Rodríguez**  
CEO de INNOVA IBÉRICA, empresa de desarrollo de software de gestión de riesgos y compliance

## INNOVACIÓN EN GRANDES CORPORACIONES

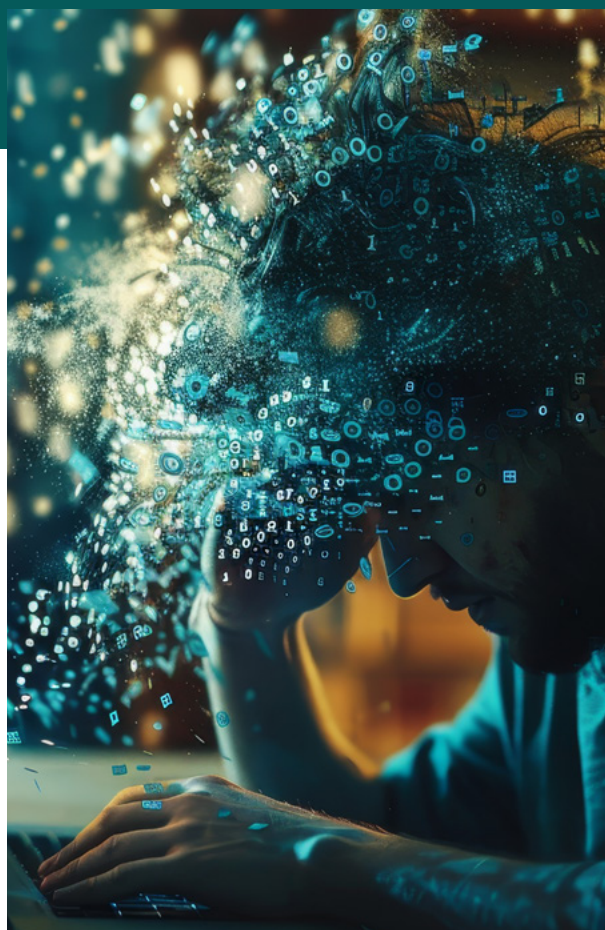
Las grandes empresas han comenzado a utilizar IA para optimizar procesos y reforzar su ciberseguridad. Aplicaciones y modelos de IA como los de OpenAI permiten automatizar tareas, detectar amenazas en tiempo real y analizar grandes volúmenes de datos, mejorando la toma de decisiones. No obstante, estos beneficios vienen acompañados de nuevos riesgos, como la dependencia tecnológica y la exposición a ataques más sofisticados. Los equipos de ciberseguridad deben mantenerse alerta ante posibles vulnerabilidades y desarrollar planes de contingencia sólidos.

## BENEFICIOS Y RETOS PARA PYMES Y AUTÓNOMOS

El avance tecnológico no solo es relevante para las grandes corporaciones; las PYMES y autónomos también pueden aprovechar las aplicaciones de IA. Herramientas accesibles, como ChatGPT, facilitan la adopción de IA en tareas de atención al cliente, marketing y análisis de datos, con un coste reducido. Sin embargo, las PYMES enfrentan desafíos específicos, como la falta de recursos para implementar medidas de ciberseguridad robustas y la necesidad de capacitación para el uso adecuado de estas tecnologías.

## CIBERSEGURIDAD Y SOSTENIBILIDAD EN EL USO DE IA

La ciberseguridad se ha convertido en una prioridad para empresas de todos los tamaños. La IA ofrece capacidades avanzadas para detectar comportamientos anómalos y amenazas emergentes, permitiendo a las empresas proteger su infraestructura digital con ma-



yor eficacia. Sin embargo, el éxito en la adopción de estas tecnologías depende de una implementación ética y transparente, que contemple no solo el beneficio económico sino también la responsabilidad social.

## CONCLUSIÓN

La inteligencia artificial y los riesgos tecnológicos están redefiniendo el panorama empresarial y la gestión de riesgos. La adopción de estas herramientas debe ser estratégica, garantizando que su uso no solo mejore la eficiencia, sino que también incremente la seguridad y sostenibilidad. La clave para aprovechar esta revolución tecnológica reside en combinar innovación con responsabilidad, asegurando un enfoque de gestión de riesgos inclusivo y adaptado a la realidad de cada organización.



# MÁS DE 80 PUBLICACIONES

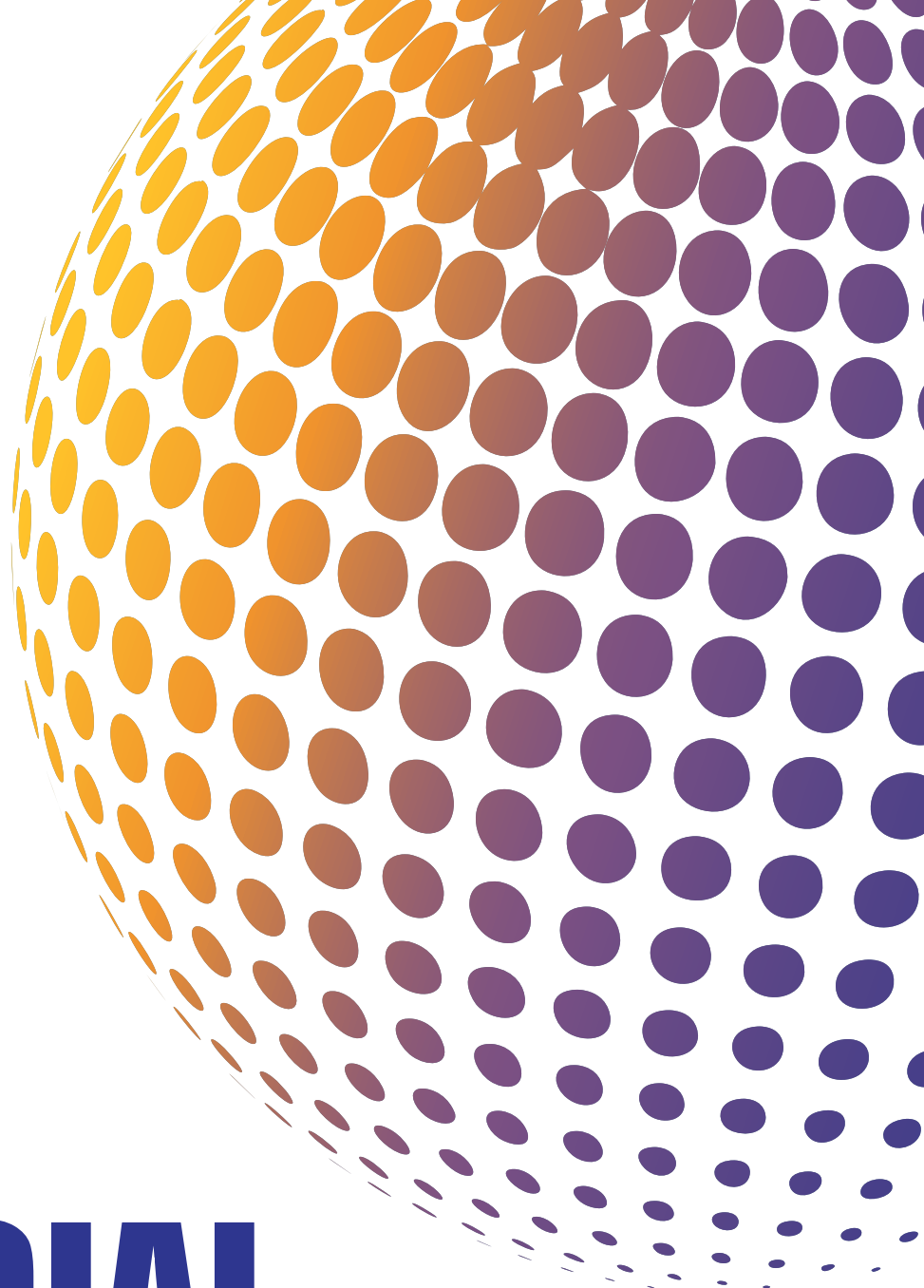
---

Contenido  
especializado:  
guías, manuales,  
memorias, revistas y  
mucho más

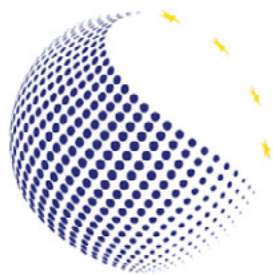
ager̄s







**ESPECIAL**



EUROPEAN RISK  
**FORUM 2024**

**MADRID**   
**FERMA NIGHT**  
22 . OCTOBER

# ESPECIAL

## MADRID FERMA FORUM 2024

(20-21-22 de octubre)

**45** MADRID FERMA FORUM 2024

**46** FERMA FORUM EN DÍAS

**46** DÍA 20 DE OCTUBRE | WELCOME EN EL AYUNTAMIENTO DE MADRID

**48** DÍA 21 DE OCTUBRE | IFEMA, RESUMEN DE LAS SESIONES PLENARIAS Y PODIOS

**52** DÍA 22 DE OCTUBRE | IFEMA, RESUMEN DE LAS SESIONES PLENARIAS Y PODIOS

**55** PANELES DE LOS ESPAÑOLES EN EL FERMA FORUM 2024

**58** AGERS PREGUNTA

**60** FERMA FORUM EN IMÁGENES

**66** FERMA NIGHT 2024 Y CLAUSURA



FERMA ha celebrado este año 2024 en Madrid el **FERMA FORUM del 20 al 22 de octubre**, en un año significativo y crucial por los **50 años de la Federación Europea**.

Durante los tres días y dándole como título al Fórum **“Únete a la revolución del riesgo”**, disfrutamos de los más de **100 ponentes** y se reunieron más de **3.000 asistentes** bajo un contexto global en constante cambio y con desafíos crecientes.

# El Foro Europeo para profesionales de riesgos y seguros

Especialistas de la industria compartieron su experiencia y prácticas, mientras que los asistentes contaron con amplias oportunidades para conectar y compartir ideas. Este enfoque orientado **aprendizaje, networking y sesiones dinámicas** buscó inspirar y crear entre los participantes un ambiente que promoviera la innovación y el éxito dentro de la comunidad de gestión de riesgos.

Los talleres del **FERMA Fórum 2024** abarcaron una amplia gama de temas clave en la gestión de riesgos, destacando la influencia de **la tecnología, la sostenibilidad y la innovación**. Se exploraron áreas como la inteligencia artificial aplicada a los seguros, la ciberseguridad frente a riesgos cibernéticos catastróficos y la adaptación al cambio climático mediante soluciones de captivas. Además, se abordaron estrategias para la gestión de crisis en contextos de guerra, el liderazgo en entornos desafiantes y la evolución de los seguros paramétricos.

Estos espacios ofrecieron una visión integral sobre cómo enfrentar los riesgos emergentes y prepararse para los **desafíos futuros en el sector asegurador**, combinando casos prácticos con reflexiones estratégicas y perspectivas globales.

Dentro del contexto de la pasada edición celebrada en el año 2022 en Copenhague, la convocatoria de este año en Madrid ha duplicado las cifras reuniendo a más de **3,000 asistentes, 126 ponentes, llevándose a cabo más de 10 sesiones plenarias y 33 workshops**.

Se contó con la colaboración de **78 patrocinadores** y fue cubierto mediante entrevistas y artículos por **14 medios de comunicación**, entre los que destacan marcas como: Inese, AM Best, Captive Intelligence, Captive Review, Commercial Risk, Emerging Risks, Insurance Day, Insurance Insider, Intelligent Insurar, Parametric Insurer, Schade Magazine, Seguros News, StrategicRISK y The Insurer.

Todo esto ha sido posible, gracias al incansable trabajo realizado por el **Comité organizador**.

Este evento celebrado en **Madrid**, consolidó al **FERMA Fórum como el mayor hasta la fecha** en cuanto a participación, en comparación con los años anteriores, reflejando el crecimiento y la importancia de la gestión de riesgos a nivel internacional.

# 46 FERMA FORUM EN DÍAS

DÍA 20 DE OCTUBRE | WELCOME EN EL AYUNTAMIENTO DE MADRID



ACCEDA  
RESUMEN  
COMPLETO  
PINCHANDO  
AQUÍ

## 50 Aniversario en la Galería de Cristal

(Palacio de Cibeles, Excmo. Ayto. de Madrid)





Madrid se vistió de gala para recibir a **1,400 invitados** en la majestuosa Galería de Cristal en el Palacio de Cibeles (Excmo. Ayto. de Madrid), celebrando medio siglo de historia de FERMA.

Tras los discursos de la *Directora de FERMA, Typhaine Beaupérin* Chief Executive Officer at FERMA - Federation of European Risk Management Associations y de su *Presidenta Charlotte Hedemark*, se llamó al escenario a los presidentes que desde 1974 han estado al frente de este proyecto tan importante para la representación y crecimiento de la figura de los gerentes de riesgos en Europa.

La junta de Ferma actual sopló las velas, por estos 50 años de incansable trabajo y agradeció a los asistentes los aplausos y las felicitaciones recibidas.

Amenizado por un grupo de música en vivo y con un cóctel repleto de productos de España, entre luces, discursos y un ambiente lleno de emoción, los asistentes comenzaron a vivir la experiencia FERMA FORUM 2024.

La recepción de bienvenida fue un momento muy especial lleno de oportunidades para hacer networking y reunirse con colegas de profesión de diferentes países de Europa.

Un evento que sin duda quedará para el recuerdo.



# 48 FERMA FORUM EN DÍAS

## DÍA 21 DE OCTUBRE | IFEMA, RESUMEN DE LAS SESIONES PLENARIAS Y PODIOS

El lunes 21 de octubre, dio comienzo en el pabellón 7 de IFEMA el FERMA FÓRUM 2024 en un ambiente lleno de emoción y ganas de compartir conocimientos y crear conexiones entre profesionales del sector.

El programa del FERMA Fórum 2024 estuvo diseñado para ofrecer un equilibrio entre aprendizaje, interacción y networking. A lo largo del día, los asistentes participaron en diversas actividades que maximizaron su experiencia y conocimientos en la gestión de riesgos.



## Resumen apertura sesión plenaria

La jornada arrancó con la bienvenida de Charlotte Hedemark, presidenta de FERMA, quién ha compartido una interesante reflexión sobre los riesgos emergentes en Europa, destacando el impacto de la inteligencia artificial y cómo las organizaciones especializadas en la gestión de riesgos y seguros están adaptando sus prácticas y recursos para afrontar este desafío.

**Charlotte Hedemark** expresó que el **Fórum Madrid 2024** ha representado una oportunidad para reflexionar sobre la evolución de la profesión y su importancia estratégica.

Recordó cómo la exploración histórica y la navegación simbolizaban la capacidad de los gestores de riesgos para enfrentar incertidumbres, ahora apoyados por herramientas modernas y conocimiento experto. *Destacó que la función había avanzado de un rol operativo a uno más estratégico, subrayando la necesidad de un enfoque integral para gestionar tanto riesgos asegurables como no asegurables, incluidos el cambio climático, la ciberseguridad y las políticas ESG.*

En esta reflexión se hizo mención a como recientemente, se ha publicado el manifiesto de Políticas 2024-2029 para preparar a Europa para un futuro mejor.

Enfatizó como en este foro se asistirán a sesiones sobre la implementación de legislaciones de la UE, incluyendo la Ley de IA y la directiva de informes de sostenibilidad corporativa. También hizo hincapié en estar comprometidos a equipar a los gestores de riesgos con las herramientas y marcos necesarios para adaptarse al nuevo entorno de riesgos, mediante comités y documentos prácticos.

**Hedemark mencionó las iniciativas de aprendizaje y la certificación RIMAP como pilares para la profesionalización del sector, así como la incorporación de nuevos talentos.**

La CERTIFICACIÓN RIMAP, es un importante proyecto estratégico de FERMA que nos permite crear, acoplar y compartir conocimientos, prácticas y enfoques innovadores entre asociaciones miembros, sus miembros y la sociedad a nivel europeo.

AGERS, es la **única asociación española acreditada por FERMA** para la certificación RIMAP en español, tras haber superado numerosos requisitos para este convenio de equivalencia con el examen original de inglés. Cuenta con un postgrado experto en gerencia de riesgos que desarrolla en colaboración con el Risk Center de la UB, y que a través de su programa facilita y apoya la preparación a la certificación. Con más de **60 certificaciones entregadas**, AGERS continúa apoyando el desarrollo y reconocimiento de los expertos en gestión de riesgos en el ámbito internacional.

En esta imagen podemos ver a una representación de alumnos RIMAP de España que asistieron al FERMA Fórum 2024.

Para concluir, **Charlotte Hedemark** reafirmó que el foro reflejaba el compromiso de FERMA de prepararse para un entorno de riesgos en constante cambio y de fortalecer la capacidad de los gestores de riesgos para enfrentar los retos futuros.

[ACCEDA AL PROGRAMA DEL EVENTO](#)

[ACCEDA AL VÍDEO COMPLETO](#)



### NAVEGAR POR LAS TURBULENCIAS GEOPOLÍTICAS DE EUROPA: LA REVOLUCIÓN DEL RIESGO

En esta sesión se abordan las implicaciones de las transformaciones globales en Europa, destacando los riesgos geopolíticos y el papel de la Unión Europea tras las elecciones europeas y las próximas elecciones en EE. UU. Enfatiza la importancia de la cohesión estratégica en un mundo fragmentado, especialmente en el contexto de la guerra en Ucrania, que afecta la relación de la UE con otros bloques globales, como Estados Unidos. Se aboga por un enfoque proactivo y una acción unificada para enfrentar los desafíos geopolíticos, instando a Europa a aprovechar el cambio y la incertidumbre para construir un futuro resiliente y próspero.

### "CONNECTING FOR RESILIENCE" - CÓCTEL DE MUJERES PATROCINADO POR SWISS RE CORPORATE SOLUTIONS

La sesión buscó destacar a las mujeres líderes en la gestión de riesgos, promoviendo la diversidad e inclusión. A través de un cóctel de networking, se pretendió conectar a mujeres de diferentes orígenes para compartir sus experiencias y perspectivas, con el objetivo de generar cambios positivos y fortalecer una hermandad unificada.

### TRANSFORMACIONES GLOBALES QUE CONFIGURAN EL FUTURO DE EUROPA A MEDIDA QUE AVANZA LA DÉCADA

Se abordó cómo la gestión de riesgos estaba evolucionando en un contexto de inestabilidad geopolítica, conflictos militares, un año electoral clave y el avance de tecnologías como la inteligencia artificial. Se discutió cómo cambiarían la toma de decisiones y la gestión de riesgos en esa nueva era, así como cómo los mercados financieros responderían a la necesidad de que las empresas alcanzaran el objetivo de cero emisiones netas.

### DEL TRAJE NEGRO A LAS ZAPATILLAS BLANCAS: LA TRANSFORMACIÓN DEL SECTOR PARA LA GESTIÓN DE RIESGOS DE SEGUROS PARA LA GENERACIÓN Z Y MÁS ALLÁ DE LOS "ZOOMERS"

En esta sesión, se exploraron las perspectivas de la Generación Z sobre cómo la industria puede ayudarles a desarrollar su potencial y contribuir a la evolución de la gestión de riesgos. Un panel de jóvenes gestores de riesgos compartió sus expectativas sobre sus carreras, mientras que líderes del sector discutieron cómo sus organizaciones están enfrentando el desafío de reemplazar a los jubilados con nuevos talentos jóvenes y capacitados.



# 50 FERMA FORUM EN DÍAS

## Talleres en los Podios

DÍA 21 DE OCTUBRE

ACCEDA A LOS VÍDEOS  
DEL CANAL DE FERMA  
PINCHANDO AQUÍ

### CÓMO ABORDAR LOS RIESGOS HUMANOS Y DESARROLLAR RESILIENCIA FRENTE A LA IA

Desafíos éticos, ciberseguridad y gobernanza asociados con la adopción de la IA. Estos son solo algunos de los temas que se trataron en este taller, donde se destacó la importancia de preparar a las empresas para gestionar los impactos de la IA, desde la fuerza laboral hasta la adopción de nuevos modelos de gobernanza y ciberseguridad.

### TRANSICIÓN HACIA UN SECTOR ASEGURADOR SOSTENIBLE

En este taller se exploraron los roles, responsabilidades y riesgos que enfrentan las empresas en su transición hacia un mercado de seguros más sostenible, destacando cómo la función de riesgos puede jugar un papel estratégico.

### LOS RIESGOS DEL MAÑANA, LAS SOLUCIONES DE HOY

Mostraron cómo las herramientas de financiación de riesgos pueden personalizarse para enfrentar tanto los desafíos actuales como las incertidumbres futuras, ayudando a las organizaciones a mantenerse competitivas en un entorno de riesgos en constante cambio.

### INNOVACIÓN EN LA GESTIÓN DE RIESGOS

AXA, presentó su plataforma innovadora que utiliza inteligencia artificial y análisis geoespaciales para ayudar a las empresas a monitorear activos y gestionar riesgos complejos, como desastres naturales y ciberamenazas.

### CAUTIVOS: LOS PRINCIPIOS DE LAS NACIONES UNIDAS PARA UN SEGURO SOSTENIBLE EN LA PRÁCTICA

En este taller se discutió la integración de los principios de la ONU de seguros sostenibles en las estrategias de riesgos de las empresas, con un enfoque en la sostenibilidad y los objetivos ESG.

### RIESGOS GEOPOLÍTICOS EN UN MUNDO POLARIZADO

En el taller se trata como el mundo enfrenta una polí-crisis, con los riesgos geopolíticos como prioridad para las organizaciones. Con varias elecciones en 2024, el panorama de riesgos está en constante cambio. Expertos en riesgos geopolíticos presentaron los últimos titulares, mientras se discutieron cómo comprender, prepararse y mitigar estos riesgos en evolución.

### LA REALIDAD DE UN CIBERATAQUE

En la sesión se analizó cómo gestionar un ciberataque desde su descubrimiento, los equipos a alertar, los pasos a seguir y la comunicación con empleados y medios.

### REFORZAR LA RESISTENCIA CLIMÁTICA

Generali GC&C presentó una sesión sobre el papel crucial del seguro paramétrico para gestionar los riesgos relacionados con el cambio climático. Este tipo de seguro utiliza desencadenantes predefinidos y datos objetivos para liquidar reclamaciones de forma rápida y transparente.

A través de ejemplos reales, se demostró cómo el seguro paramétrico ayuda a las organizaciones a mejorar su resiliencia ante un entorno de riesgos cambiante. Además, se destacó cómo esta herramienta puede cerrar la brecha de protección aseguradora, especialmente para las comunidades más vulnerables. También se mencionó la colaboración entre Generali y el PNUD, que contribuye a un futuro más sostenible para las comunidades más afectadas por el cambio climático.

### LA OPORTUNIDAD DE INSURTECH

QBE Ventures expuso por otro lado, su colaboración con empresas tecnológicas para transformar la industria aseguradora, destacando cómo tecnologías emergentes pueden mejorar la selección y suscripción de riesgos.

### RISKY BUSINESS, LOS RIESGOS CIBERNÉTICOS Y LA NUEVA NORMATIVA AUMENTAN LA PRESIÓN EN LOS CONSEJOS DE ADMINISTRACIÓN

La sesión abordó cómo los riesgos cibernéticos crecientes están colocando a las salas de juntas en el centro de atención. Se exploraron los riesgos y beneficios de los avances en ciberseguridad y tecnología, y cómo el cambio en las regulaciones afecta a las empresas.

### A RIESGO DE SER INSOSTENIBLES

El taller trató sobre los riesgos en las estrategias de sostenibilidad desarrolladas sin la función de riesgos, incluyendo el greenwashing y otros problemas. Se destacó la importancia de crear una estrategia de alfabetización climática y de sostenibilidad en las organizaciones, y cómo abordar el panorama regulatorio cambiante antes de que sea obligatorio. Además, se subrayó la necesidad de centrarse en las oportunidades que ofrece la sostenibilidad como base para las acciones estratégicas.

### EL CAMINO HACIA UN SECTOR INMOBILIARIO BASADO EN LOS DATOS

La sesión abordó cómo los edificios, responsables del 39% de las emisiones de gases de efecto invernadero, están siendo un foco de atención debido al aumento de los factores ESG en la industria inmobiliaria. Se exploró cómo los datos de valoración fiables y las plataformas tecnológicas son fundamentales para promover la construcción de edificios sostenibles y con mayor valor en el sector inmobiliario y asegurador.



# WEEKLYREPORT

---

agers

## EN UN SOLO CLICK

Estate al día de toda  
nuestra actualidad:  
noticias, eventos, informes  
y mucho más.

Más de 4.500 suscriptores  
lo reciben cada martes

SUSCRÍBETE AQUÍ >>

# 52 FERMA FORUM EN DÍAS

## Paneles Sesión Plenaria

DÍA 22 DE OCTUBRE | IFEMA, RESUMEN DE LAS SESIONES PLENARIAS Y PODIOS

### GESTIÓN DEL CAMBIO: UNA HERRAMIENTA ESTRATÉGICA PARA LOS RESPONSABLES DE RIESGOS

Esta sesión abordó el papel crucial de los gestores de riesgos como impulsores del cambio en las empresas, enfocándose en cómo pudieron mejorar la confianza en las evaluaciones de riesgos y la ejecución de estrategias, al mismo tiempo que promovieron un cambio de mentalidad. También se compartieron experiencias de profesionales destacados que enfrentaron grandes desafíos, como la reestructuración de Solvay y la reinención de las operaciones de Lloyd's en Europa debido al Brexit.

### CIBERBOLSAS PARA RIESGOS CIBERNÉTICOS CATASTRÓFICOS

Se abordó la creciente amenaza de los riesgos cibernéticos a gran escala y la intervención del Estado en este ámbito. Tras los recientes ciberataques y las vulnerabilidades encontradas en las actualizaciones de software, el enfoque de la sesión se centró en la importancia de las soluciones para reducir la brecha en la protección cibernética. Philippe Cotelie, miembro de FERMA, presentó el trabajo de la organización sobre este tema y moderó una discusión internacional sobre posibles soluciones.

### PRESENTACIÓN DE LOS RESULTADOS DE LA PRIMERA ENCUESTA MUNDIAL DE GESTORES DE RIESGOS

Se anunció con entusiasmo el lanzamiento de la primera Encuesta Global de Gestores de Riesgos, realizada por FERMA en colaboración con PwC y con el apoyo de asociaciones de riesgos de EE. UU., América Latina, Asia-Pacífico y África. Esta innovadora encuesta recopiló perspectivas y tendencias de gestores de riesgos de todo el mundo, proporcionando una visión completa sobre la evolución de la gestión de riesgos.

En la sesión, se presentaron los hallazgos clave, destacando los desafíos y oportunidades actuales. Representantes de diferentes continentes compartieron sus opiniones y discutieron los resultados, ofreciendo una perspectiva global sobre el estado de la gestión de riesgos y las estrategias emergentes.

ACCEDA A LOS VÍDEOS  
DEL CANAL DE FERMA  
PINCHANDO AQUÍ

### GESTIÓN DE CRISIS Y SEGUROS EN TIEMPOS DE GUERRA

Los expertos de RSA/Intact, ofrecieron una sesión sobre cómo configurar programas globales multinacionales, cubriendo aspectos prácticos y desafíos comunes al establecer o renovar un programa con un nuevo asegurador. A través de ejemplos de casos reales, brindaron orientación sobre reaseguro, socios locales y los requisitos de ingeniería de riesgos, compartiendo su experiencia en una aseguradora con más de 300 años de trayectoria global.

### LANZAMIENTO DE LIDERAZGO

La sesión permitió escuchar a varios CEOs compartir sus perspectivas sobre la "revolución de los riesgos", en un formato similar al de las charlas Ted x, ofreciendo ideas rápidas y directas sobre cómo enfrentan los desafíos futuros y cómo buscan la excelencia en sus empresas.

## Paneles Sesión Plenaria

DÍA 22 DE OCTUBRE | IFEMA, RESUMEN DE LAS SESIONES PLENARIAS Y PODIOS

### LOS SEGUROS EN LA NUEVA ERA

Este panel busca ampliar el éxito de la sesión previa sobre el mercado de seguros en el FERMA Fórum 2022. En un formato interactivo, figuras destacadas de los socios estratégicos de FERMA discutieron sobre los cambios dinámicos que están transformando el mercado de seguros, adaptándose a las necesidades cambiantes de sus clientes corporativos.

### DISCURSO DE CLAUSURA Y PREMIO A LA MEJOR EXPOSICIÓN

En estas palabras que tuvieron lugar en la clausura, se reflexionó sobre el recorrido y los puntos clave discutidos durante el foro, seguidos de la entrega del Premio al Mejor Stand de la Exposición. Este prestigioso galardón destacó la contribución y creatividad excepcionales de nuestros expositores.

## Talleres en los Podios

DÍA 22 DE OCTUBRE | IFEMA, RESUMEN DE LAS SESIONES PLENARIAS Y PODIOS

### PROGRAMAS GLOBALES DE SEGUROS ¿QUÉ NOS DICEN LOS EJEMPLOS DE CASOS PRÁCTICOS?

Los expertos de RSA/Intact, ofrecieron una sesión sobre cómo configurar programas globales multinacionales, cubriendo aspectos prácticos y desafíos comunes al establecer o renovar un programa con un nuevo asegurador. A través de ejemplos de casos reales, brindaron orientación sobre reaseguro, socios locales y los requisitos de ingeniería de riesgos, compartiendo su experiencia en una aseguradora con más de 300 años de trayectoria global.

### GESTIÓN DE RIESGOS EMERGENTES A TRAVÉS DE LA TECNOLOGÍA Y LA INNOVACIÓN

En un mundo donde los riesgos emergen y cambian rápidamente, es crucial aprovechar todas las oportunidades e información disponible para comprender y abordar estos riesgos complejos. El uso efectivo de datos, tecnología y experiencia compartida, combinado con una mentalidad innovadora y enfocada en el valor, ayudará a los clientes a enfrentar este período desafiante y emocionante. Durante la sesión, Allianz discutió las oportunidades y soluciones para comprender y mitigar estos riesgos de manera más eficaz.

### EMPRESAS EUROPEAS Y RIESGO EMERGENTE EN NORTEAMÉRICA

El taller expuesto por la empresa Lockton abordó los riesgos emergentes que enfrentan las empresas europeas en EE. UU. y cómo desarrollar estrategias personalizadas para mitigar estos riesgos, optimizando los programas de seguros tanto en EE. UU. como en Europa. Se trataron riesgos específicos como los veredictos nucleares, los costos médicos inflacionarios y el cumplimiento de regulaciones federales. Además, se compartieron estrategias para gestionar seguros obligatorios en EE. UU. y mejorar la protección del perfil de riesgos corporativos.

### RIESGO CLIMÁTICO: DE LA GESTIÓN DE RIESGOS A LAS SOLUCIONES DE CAUTIVAS

Los clientes están incorporando información ESG en su análisis de riesgos para encontrar soluciones dedicadas. El papel de las "Captives" se destacó como un punto clave para identificar desafíos ESG y apoyar la estrategia de la empresa, permitiendo integrar prácticas sostenibles en la gestión de riesgos. En este taller, Axa planteó cómo satisfacer las necesidades de los clientes de "Captives" para obtener capacidad



## ACCEDA A LOS VÍDEOS DEL CANAL DE FERMA PINCHANDO AQUÍ

adicional mediante soluciones paramétricas, y se presentó un enfoque de ingeniería de riesgos que abarca desde la prevención hasta la mitigación, cubriendo riesgos naturales, hídricos y emergentes.

### DOMINAR LA ESTRATEGIA DE RIESGOS: TRANSFORMAR LAS MEDIDAS ACTUALES EN IMPACTO ESTRATÉGICO A NIVEL DIRECTIVO

Moody's explicó en su taller como gestionar los riesgos clave que enfrenta un negocio, como ciberataques, interrupciones en la cadena de suministro, problemas crediticios y cambio climático. Se discutió cómo identificar y cuantificar estos riesgos, explorar diferentes escenarios y desarrollar estrategias para mitigarlos. También se destacó el uso de datos y análisis para tomar decisiones informadas y construir estrategias resilientes.

### LA(R)EVOLUCIÓN DE LOS SEGUROS PARAMÉTRICOS

BHSI centró su sesión, en el seguro paramétrico para catástrofes naturales destacando sus características clave, cómo evaluar estas soluciones para adaptarlas a las necesidades específicas, y los errores comunes a evitar. Se presentaron casos prácticos globales y ejemplos de pérdidas históricas que evidencian los pagos rápidos y la transparencia de este seguro. El objetivo fue proporcionar a los asistentes una comprensión de cómo integrar estas soluciones en la gestión de riesgos.

### MÁS ALLÁ DE LOS SEGUROS: LA REVOLUCIÓN DE LA GESTIÓN DE RIESGOS EN LA RECUPERACIÓN DE CRISIS - UNA INMERSIÓN PROFUNDA EN LA RESTAURACIÓN DE LAS INUNDACIONES DE EMILIA ROMAGNA

La presentación realizada por Belfor, mostró cómo los gestores de riesgos han pasado de centrarse en seguros a liderar estrategias de crisis, usando el caso de la restauración de una planta tras una inundación en Emilia Romagna (2023). Se abordaron desafíos como escasez de recursos, costos de seguros y decisiones críticas, destacando la planificación proactiva y estrategias innovadoras para garantizar continuidad y resiliencia empresarial.

### PREPARACIÓN PARA INFORMAR SOBRE LOS DERECHOS HUMANOS

En este taller se abordó como a partir de 2025, las empresas de la UE deberán informar sobre riesgos de derechos humanos como parte de los requisitos ESG según la Directiva de Sostenibilidad Corporativa. Este taller explicó el marco de informes, las responsabilidades del gestor de riesgos y cómo se evaluarán y auditarán estos informes.

### RIESGOS DE RESPONSABILIDAD CIVIL EN TIEMPOS TURBULENTOS

En esta sesión, los líderes de Liberty Specialty Markets (LSM) abordaron los factores que impactan el seguro de responsabilidad, como el entorno legal actual, la inflación, los riesgos emergentes y las tendencias de reclamaciones en Europa y más allá. Se exploraron riesgos asociados con el trabajo híbrido, las redes sociales, el cambio climático y los cambios políticos.

Los asistentes obtuvieron ideas sobre como los especialistas ayudan a mitigar estos riesgos en un entorno empresarial sin precedentes, ofreciendo estrategias prácticas y una perspectiva experta interactiva.

### DOS TEMAS, UNA SESIÓN. RESOLUCIÓN DE PROBLEMAS COMPLEJOS DE GESTIÓN DE RIESGOS MEDIANTE EL USO DE DATOS Y ANÁLISIS, SEGUIDO DE UN ENFOQUE EN EL RIESGO DE ASALTANTE ACTIVO / TIRADOR ACTIVO

Ante un entorno global marcado por tensiones geopolíticas y un panorama de seguridad en evolución, esta sesión llevada por WTW abordó el creciente riesgo de atacantes activos y violencia laboral, destacando su expansión fuera de América del Norte. Se discutieron:

- La naturaleza diversa del riesgo.
- Estrategias de prevención y control.
- La importancia de la gestión de consecuencias en ámbitos financieros, legales, operativos y reputacionales.
- Soluciones emergentes del mercado asegurador para enfrentar esta amenaza en crecimiento.

### GESTIÓN DE RIESGOS EN DISTINTAS ZONAS GEOGRÁFICAS: LECCIONES DE LATAM

En el taller, expertos en gestión de riesgos de América Latina compartieron sus perspectivas sobre los desafíos únicos de esta región diversa. Participaron gestores de importantes empresas de petróleo y gas, aviación e ingeniería y servicios, analizando cómo los retos varían según la geografía y ofreciendo a los asistentes europeos una visión exclusiva sobre estrategias y oportunidades de gestión de riesgos empresariales en sectores clave.

### PFAS (FOREVER CHEMICALS) Y SU IMPACTO EN EL MEDIO AMBIENTE Y LAS EMPRESAS

A través de un análisis experto y conocimientos prácticos, esta sesión ofrece a los participantes una comprensión integral de las regulaciones sobre PFAS y sus amplias implicaciones para las empresas. Ya fueras representante de una pequeña empresa familiar o una gran corporación, esta sesión proporcionó valiosos conocimientos para navegar por el panorama cambiante de las regulaciones sobre PFAS.

# Paneles de los españoles en el FERMA FORUM 2024

**21 DE OCTUBRE**

***“La descarbonización: Desafíos y lecciones de la industria minera de LATAM”.***

El día 21 de octubre Mario Ramírez junto con Ernesto Balarezo CEO de Sierra Metals, Juan Carlos Miljanovich CFO Summa Gold, Ana Pedrouzo, Expert in Mining and Steel in Mapfre Global Risks y Giulio Valz-Gen CEO HOWDEN Perú, presentaron un pódium en sesión plenaria llamado “La descarbonización: Desafíos y lecciones de la industria minera de LATAM”.

Como conclusión general, se destacó la importancia de incorporar la gestión medioambiental en las empresas mineras para mitigar riesgos y garantizar la sostenibilidad.

Estas prácticas reducen el impacto ecológico, fortalecen la responsabilidad social y aseguran el cumplimiento normativo. Además, contribuyen a mejorar la reputación corporativa y evitar sanciones legales. La gestión ambiental es clave para el éxito a largo plazo en el sector minero.

**MARIO RAMÍREZ  
ORTÚZAR**

**Global Risk, Assets &  
Audit Lead at EXOLUM  
- Board member at  
FERMA**



**22 DE OCTUBRE:**

***“La gestión de riesgos en distintas zonas geográficas: Lecciones de LATAM”***

Este taller celebrado el día 22 de octubre fue un excelente punto de conexión entre la Gerencia de Riesgos de LATAM y la Gerencia de Riesgos europea, acercando ambas geografías y generando oportunidades de networking entre los asistentes.

A continuación, Mario Ramírez nos cuenta un resumen de los temas que se abordaron en los talleres y las opiniones que expresaron los ponentes que le acompañaban.



## Paneles de los españoles en el FERMA FORUM 2024

### Entrevista a Mario Ramírez

**AGERS:** Mario, en este taller se destacaron lecciones clave de la gestión de riesgos en LATAM. ¿Qué desafíos específicos creéis que enfrenta la gestión de riesgos en América Latina que podrían servir como aprendizaje para otros mercados?

**MARIO:**

**Alexander Waintrub Fischer** Head of Insurance at LATAM Airlines menciona varios desafíos, incluyendo riesgos operacionales relacionados con la cadena de suministro de aeronaves y motores, riesgos ambientales debido a eventos climáticos intensos, riesgos tecnológicos como caídas de sistemas, y riesgos del mercado asegurador y reasegurador. También destaca la necesidad de cumplir con normativas y regulaciones que varían según el país.

**Tommaso Mascarucci** Head of Financial Risks at the Ecopetrol Group (GE) señala la necesidad de una gestión de riesgos más centralizada para asegurar sinergias entre áreas clave como la continuidad del negocio y la transferencia de riesgos. También menciona desafíos como la descarbonización, el respaldo para proyectos de nuevas energías, y la volatilidad de las coberturas y tasas.

**Jose Manuel Fonseca** MDS Group CEO | Brokerslink President and CEO, destaca las crisis superpuestas e interconectadas que enfrentan las organizaciones brasileñas, incluyendo crisis económicas, climáticas, geopolíticas y sociales. También menciona la importancia de gestionar los riesgos-país y los riesgos operativos propios de la organización.

**Alejandro Reyes Pizarro** Magister en Control de Procesos en Universidad de Chile, menciona la necesidad de estructurar un gobierno corporativo dentro de los más altos estándares, asegurar la continuidad operacional y cumplir con normativas exigentes en materias de delitos económicos, anticorrupción y medio ambiente. También destaca la importancia de equilibrar las variables económicas, sociales y ambientales.



**AGERS:** ¿Hay alguna práctica o enfoque en particular que consideréis transferible a otras regiones con características diferentes?

**MARIO:**

**Alexander Waintrub Fischer**, resalta la importancia de la resiliencia y adaptabilidad, la gestión proactiva de riesgos, la preparación y planificación frente a crisis, y la generación de relaciones de largo plazo con aseguradores y reaseguradores. También menciona la importancia de mantener una buena comunicación con los stakeholders del seguro.

**Tommaso Mascarucci** ofrece cinco consejos, incluyendo cuestionar y revisar la evolución del mapa de riesgos empresariales, anticiparse a los cambios, analizar y monitorear la efectividad de la estrategia de retención y transferencia de riesgos, y transformar los procesos con tecnología.

**Jose Manuel Fonseca**, destaca la importancia de elevar la gestión de riesgos como un tema estratégico, implementar una cultura organizacional enfocada en la gestión de riesgos, asumir una actitud positiva ante el riesgo, y centrarse en la capacidad de adaptación y respuesta a cambios y crisis. También menciona la experiencia de los gerentes de riesgos brasileños en trabajar en crisis constantes y entornos adversos.

**Alejandro Reyes Pizarro**, menciona la necesidad de tener un gobierno corporativo estructurado y bien definido, incorporar la gestión de riesgos en la estrategia de negocios, y entender que hay riesgos asegurables y no asegurables. También destaca la importancia de tener una buena cobertura de seguros para introducir mayor confiabilidad en los modelos de negocios.





**ISABEL MARTÍNEZ TORRE - ENCISO**  
 Non Executive Director  
 | ESG | Global Risk & Crisis Mgmt | Business Continuity | Corporate Governance & Board Effectiveness

## 21 DE OCTUBRE

### “Cómo evolucionar hacia una función de gestión estratégica de riesgos”.

En este taller, se subrayó la creciente relevancia de la posición del director de riesgos. Los ponentes recalcaron que su rol no solo es crucial en sectores tradicionales como el bancario, sino que está ganando protagonismo en muchas otras industrias.

También se habló de la importancia de establecer un lenguaje común entre los profesionales del riesgo, permitiendo que todos hablen el mismo idioma. Un ejemplo clave de esta iniciativa es la acreditación RimapFERMA, que está ayudando a homogeneizar y profesionalizar el sector.

## Entrevista a Isabel Martínez

**AGERS:** Marisa, en tu presentación hablaste sobre la evolución hacia un rol más estratégico en la gestión de riesgos. ¿Cuáles crees que son los principales obstáculos que enfrentan los gestores de riesgos al intentar posicionarse como socios estratégicos dentro de sus organizaciones?

**ISABEL MARTÍNEZ:** La evolución positiva de la gestión de riesgos en las empresas españolas se enfrenta a diversos obstáculos, principalmente debido a la naturaleza de los riesgos y a la gobernanza de las empresas y la sociedad española. Más del 85% del tejido empresarial español está formado por pequeñas y medianas empresas, que no siempre cuentan con funciones de gestión de riesgos ni cumplen con normativas comunitarias como las directivas de reporting. En muchas de estas empresas, la gestión de riesgos se limita a aspectos operacionales, lo que depende del tamaño y la cultura organizacional. Sin embargo, existe una creciente conciencia sobre la importancia de integrar la función de riesgos en todos los niveles de la empresa, lo que facilitará un enfoque más estratégico a largo plazo. Además, la naturaleza de los riesgos está cambiando, volviéndose más compleja, dinámica e interconectada, lo que exige conocimientos técnicos especializados.

**AGERS:** ¿Qué habilidades o competencias consideras clave para lograr esta transición?



**ISABEL MARTÍNEZ:** Los gerentes de riesgos en las empresas españolas están evolucionando de un enfoque técnico y asegurador hacia una gestión estratégica e integral, abarcando todos los aspectos del riesgo dentro de la organización. El objetivo es proporcionar al C-suite una visión completa y en tiempo real de los riesgos, permitiendo decisiones alineadas con los objetivos corporativos. Este enfoque dinámico implica la identificación de riesgos operativos y estratégicos, sus interrelaciones y acciones para mitigar su impacto, utilizando tecnologías como la inteligencia artificial y el análisis de datos. Además, es fundamental que los profesionales del riesgo continúen su formación técnica y en habilidades de gestión, y se certifiquen en programas como el FERMA Rimap. La integración de los riesgos ESG (ambientales, sociales y de gobernanza) en la estrategia de gestión de riesgos, en cooperación con funciones como sostenibilidad, auditoría interna y compliance, es clave para garantizar decisiones responsables que promuevan la sostenibilidad y la resiliencia organizacional.

# 58 AGERS Pregunta

## ¿Qué ha supuesto el FERMA FORUM Madrid 2024 para tu empresa?

AGERS pudo vivir de primera mano esta experiencia, teniendo la oportunidad de entrevistar a perfiles muy diversos, recogiendo la opinión sobre el evento, tanto de grandes profesionales del sector como antiguos alumnos del Centro de Estudios de Agers (CEA) o de la Universidad Autónoma de Madrid.

A través de un plató de grabación gestionado por el equipo de AGERS, los participantes compartieron sus experiencias del evento y cómo este se relacionaban con las actividades y objetivos de sus organizaciones. Estas entrevistas reflejaron una variedad de perspectivas sobre la importancia del FERMA Fórum y su impacto en la comunidad de gestión de riesgos y seguros.

Si quieres profundizar más sobre estas perspectivas podrás acceder a continuación a los enlaces de las entrevistas en nuestro canal de Youtube

### Jorge Nadel Ciorcia

*Sales Executive de Riskconnect*



### Constanza Gállegos

*Country Manager at Berkshire Hathaway Specialty Insurance*



### Alfredo Arán Iglesia

*Senior Advisor de Howden Group*



### Ana Molinero Sánchez

*Responsable de Distribución para la compañía de seguros de Beazley*



# ENTREVISTAS A LOS ALUMNOS DE LA UNIVERSIDAD AUTÓNOMA DE MADRID Y DEL CEA



Durante el FERMA Forum 2024 en Madrid, se realizaron entrevistas a varios alumnos de la Universidad Autónoma de Madrid (UAM), conducidas por Gonzalo Iturmendi Morales, propietario del Bufete G. Iturmendi y Asociados. Estas entrevistas ofrecieron una visión fresca y cercana sobre la percepción que tienen los estudiantes sobre la gestión de riesgos y seguros, así como su experiencia en este evento de alto nivel. A través de sus testimonios, se exploraron sus expectativas, sorpresas y aprendizajes, mostrando cómo el foro ha ampliado su perspectiva sobre el sector y les ha permitido conectar con profesionales del área, así como reflexionar sobre su futuro en la industria del riesgo y los seguros.

## Daniel Alonso

*Alumno de la UAM*



## Manuel Chavarrén

*Alumno de la UAM*



## David Cruanyes

*Asesor de Riesgos y Seguros Quality Brokers*



## Marco Zurdo

*Alumno de la UAM*





# 60 FERMA FORUM 2024 en imágenes

20 DE OCTUBRE





ACCEDA  
A LA  
GALERÍA  
DE FERMA  
PINCHANDO  
AQUÍ





# 62 FERMA FORUM 2024 en imágenes

21 DE OCTUBRE





21 DE OCTUBRE

ACCEDA A LA GALERÍA DE FERMA PINCHANDO AQUÍ





# 64 FERMA FORUM 2024 en imágenes

22 DE OCTUBRE





22 DE OCTUBRE

ACCEDA A LA GALERÍA DE FERMA PINCHANDO AQUÍ





# 66 FERMA NIGHT 2024 y clausura

El broche final fue una celebración bajo el cielo de Las Ventas. La Madrid FERMA NIGHT reunió a 1,400 asistentes y patrocinadores de prestigio además de otros líderes del sector. Tras tres intensos días de conferencias, talleres, proyectos y reuniones, llegó la tan esperada FERMA NIGHT, una noche única de networking, entretenimiento y celebración.

Este evento de cierre fue una gran ocasión para festejar nuestros logros y el trabajo conjunto, así como una oportunidad para fortalecer los lazos establecidos durante el foro.

Fue el momento perfecto para reflexionar sobre lo aprendido, compartir opiniones y disfrutar de una velada entre todos los compañeros, mientras rendimos un merecido homenaje a todos los gestores de riesgos y colaboradores que han dedicado su tiempo y esfuerzo durante el evento, teniendo un especial tributo a aquellos directores que nos dejaron y ya no están con nosotros.



VÍDEO  
FERMA NIGH

GALERIA  
IMÁGENES  
FERMA NIGH



## Discursos

La noche comenzó con una cálida bienvenida de los presidentes de **FERMA** (Charlotte Hedemark), de **AGERS** (Juan Carlos López Porcel) e **IGREA**, (Daniel San Millán), quienes quisieron expresar su sincero agradecimiento a todos los asistentes, reconociendo la valiosa presencia de cada uno de ellos durante los tres días. Fue un momento especial en el que se destacó la importancia de la participación y el compromiso de todos los presentes, quienes contribuyeron al éxito de este evento.



## Colaboradores

Este evento tan especial no habría sido posible sin el valioso respaldo de nuestros colaboradores. Gracias a su esfuerzo y compromiso, pudimos ofrecer una celebración memorable para todos los presentes.

Junto a nuestros colaboradores Torero, quienes asumieron un compromiso destacado con el evento, Picadores, que brindaron apoyo de alto nivel y contribuyeron al desarrollo y organización del foro, y Banderilleros, que ofrecieron una plataforma de alto nivel para la discusión y el intercambio de conocimientos.



# 68 FERMA NIGHT 2024 y clausura

22 DE OCTUBRE, BROCHE DE ORO EN LA PLAZA DE TOROS DE LAS VENTAS

## HABLEMOS DE LOS SPONSORS TOREROS:

Son los colaboradores principales, que han asumido un compromiso destacado con el evento.

En este caso, los patrocinadores son Colin Vega Fletes, conocido Gabinete jurídico de México y Jhasa, conocido Bróker de nacionalidad española, quienes apoyaron de manera significativa la celebración de la FERMA Night 2024.

**COLIN VEGA FLETES**  
ABOGADOS



*“El reunir a los protagonistas y jugadores destacados del mundo del seguro es fundamental para nutrir y compartir experiencia, conocimiento y anticiparse al futuro”.*



Francisco Fernández Guerra Fletes

**HASA**  
Insurance & Reinsurance Broker



*“FERMA FORUM es un evento clave que reúne a los principales actores del sector de la gestión de riesgos, creando un espacio inigualable para el intercambio de ideas y la colaboración entre profesionales. Para Jhasa en la noche FERMA no solo se celebran los avances del sector, sino que representa una plataforma esencial que refuerza la importancia de la gestión de riesgos como pilar fundamental para la sostenibilidad empresarial. Además, pone de relieve el valor de innovar y adoptar nuevas estrategias ante un entorno cada vez más cambiante.*

*Este año, con su celebración en Madrid, se refuerza el papel de España, como punto de encuentro estratégico para el sector, subrayando su creciente influencia en el ámbito europeo.*

*Este evento es fundamental para fortalecer las relaciones profesionales en el ámbito de los seguros y avanzar juntos hacia un futuro más resiliente, subrayando la necesidad de estar preparados para afrontar los desafíos futuros y continuar liderando el cambio con las mejores prácticas y soluciones innovadoras”.*



Jacobó Lacalle Baigorri



### HABLEMOS DE LOS SPONSORS PICADORES:

Los Sponsors Picador fueron organizaciones que brindaron apoyo de alto nivel y contribuyeron de manera importante al desarrollo y organización del foro donde contamos con grandes firmas como **Addvalora, AON, Asterra, Everest, Generali, Herbert Smith Freehills, MDS Group, Munich Re y Marsh.**

### HABLEMOS DE LOS SPONSORS BANDERILLEROS:

Por último, pero no menos importante, destacamos el apoyo de los Sponsors Banderilleros entre los que se encuentran importantes firmas como **AIG, Dac Beachcroft, HDI, Howden, Liberty, MSIG, QBE, RSA, Sompo y WTW.**

Cada grupo de patrocinadores fueron claves en el éxito del evento, y su colaboración permitió ofrecer una plataforma de alto nivel para la discusión y el intercambio de conocimientos sobre la gestión de riesgos en Europa.





# 70 FERMA NIGHT 2024 y clausura

22 DE OCTUBRE, BROCHE DE ORO EN LA PLAZA DE TOROS DE LAS VENTAS

## Actuaciones



La noche se llenó de energía y diversión con la actuación en vivo de **“Los Risky Martins y Los Algorítmicos”**. Esta banda, integrada por gestores de riesgos, como Nacho del Corral (Grupo Santander), Juan Velázquez (QBE), Gordon Smith (Liberty Specialty Markets), David Johnson (Gleeds), José María Aparicio (Swiss Re Corporate Solutions), Ignacio Camello (Everest) y Adias Gerbaud (Axa XL), deleitaron al público con su música. Sorprendió al público al demostrar su talento musical y su sentido del humor. Su presentación fue un momento lleno de entusiasmo que reflejó la creatividad y el compañerismo del sector, dejando unas sensaciones inolvidables entre los asistentes.



El cierre de la noche estuvo a cargo de la **“Luback Band”**, conformado por Cristian del Corral, Yago Saéz, Marcus Wilson, Manuel Fernández y Héctor Cerbián, con la colaboración especial de Ignacio del Corral. Cautivó al público con su gran talento y carisma. Además, dedicaron un emotivo homenaje a los compañeros que ya no están, creando un momento especial de unión y recuerdo.

Este gesto tocó el corazón de los asistentes, dejando un ambiente lleno de emoción para finalizar la velada.

Sin duda, fue una despedida significativa que dejó a todos con ganas de volver a encontrarse en el próximo FERMA FORUM.





# PhotoCall

El photo call fue uno de los puntos más animados del evento, donde los asistentes tuvieron la oportunidad de capturar momentos especiales en un espacio diseñado para ello. Se convirtió en un lugar ideal para inmortalizar recuerdos, reforzar conexiones y compartir la experiencia del evento en redes sociales. Una parada obligatoria que sumó estilo y diversión a la noche.





# 72 FERMA NIGHT 2024 y clausura

## Sala Vip



En este espacio exclusivo se llevó a cabo un encuentro clave que reunió a las Juntas Directivas de AGERS, su Consejo Consultivo, IGREA, FERMA, su Comisión Científica, así como a los Sponsors de la FERMA Night. Este evento sirvió como punto de encuentro entre líderes y expertos del sector, fomentando el intercambio de ideas e impresiones del FERMA durante sus tres días de celebración.







# Únete a AGERS y sé parte del cambio



EVENTOS



FORMACIÓN



NETWORKING



PUBLICACIONES

La mayor comunidad para  
los profesionales de  
**RIESGOS Y SEGUROS**  
en España

**HAZTE SOCIO**

agers

# LA ASOCIACIÓN

**76** **EL CENTRO DE ESTUDIOS DE AGERS:** DESARROLLAR TALENTO EN LA GESTIÓN DE RIESGOS

**90** **EVENTOS DE LA ASOCIACIÓN:**

**90** «PROGRAMAS DE SEGUROS INTERNACIONALES»

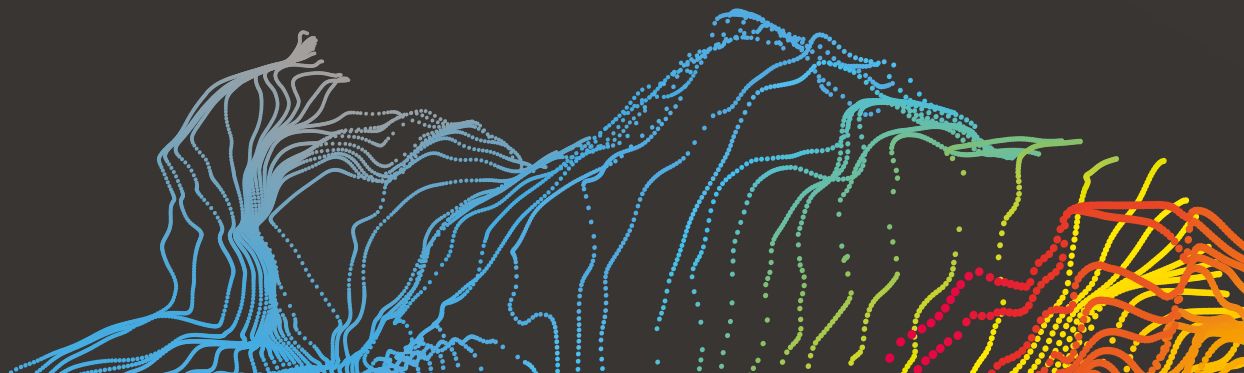
**92** DESAYUNO «DE TÚ A TÚ» CON ALEJANDRA GALDOS DE HSF Y MARTA VEGA DE EXOLUM

**94** FORO SOBRE LITIGIOSIDAD EN USA CON BHSI

**96** LA COYUNTURA DEL SEGURO DE CRIME Y LOS RETOS CIBERNÉTICOS

**98** ENVEJECIMIENTO COMO RIESGO EMPRESARIAL

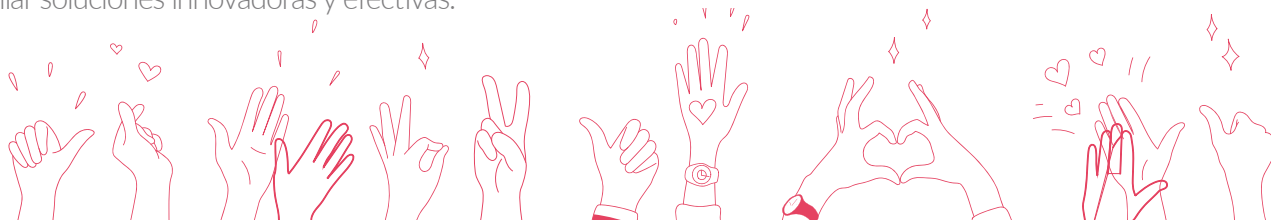
**100** NUEVAS GUÍAS SOBRE CIBERSEGURIDAD E INTELIGENCIA ARTIFICIAL





# Desarrollar talento en la gestión de riesgos

En un entorno marcado por la incertidumbre y el cambio constante, la gestión de riesgos es fundamental para la sostenibilidad y el éxito de cualquier organización. Desde el Centro de Estudios impulsamos la formación y colaboración entre profesionales de diversas disciplinas, que enriquece los equipos y permite desarrollar soluciones innovadoras y efectivas.



Lucía Márquez de la Plata y Carmen Alonso

## La Mentorización y el Intercambio de Experiencias Esenciales

### Reconociendo el Camino Recorrido (2022-2025): Un Viaje de Crecimiento

**Carmen Alonso, CEA.-** Durante los últimos tres años, he tenido el privilegio de liderar el Centro de Estudios con el objetivo de contribuir a su crecimiento y posicionamiento. Desde el primer día, asumí este reto con la aspiración de dejar una huella positiva en los proyectos del centro y en la asociación. *Para mí, la mentorización ha sido un proceso esencial que enriquece tanto al mentor como al mentee.* Este último año ha sido especialmente significativo, pues he acompañado de cerca a una persona de mi equipo en su preparación para asumir nuevas responsabilidades, un proceso que ha sido mucho más que una transferencia de conocimientos: una oportunidad para transmitir visión, valores y la pasión que siento por este proyecto.

*“Los mentores están a nuestro alrededor. ¿Quién te hace sentir segura, inspirada, centrado y está dispuesto a compartir su experiencia?” Anna Letitia Cook*

#### PLANIFICAR UN RELEVO EFECTIVO ES FUNDAMENTAL

**Carmen Alonso.-** “Planificar un relevo efectivo es esencial para mantener aquello que nos hace únicos: las fortalezas que definen nuestra propuesta de valor y que, con el tiempo, han dado forma a la identidad del CEA. Preservarlas no solo es cuestión de proteger nuestro prestigio, sino de reafirmar

un compromiso duradero con un propósito que nos permita seguir siendo una fuente de conocimiento, inspiración y crecimiento. Al mismo tiempo, este proceso abre espacio para la innovación y la evolución, sin duda, una de las mayores recompensas para un mentor: ver cómo su mentee asume el proyecto y aporta su propio estilo, asegurando así una transición sólida y llena de posibilidades para el futuro del CEA.”

#### ADAPTACIÓN Y RESILIENCIA EN UN ENTORNO CAMBIANTE

Mi tiempo al frente del CEA ha sido un aprendizaje continuo y una oportunidad para adaptarme y aportar valor al sector. Cada reto diario me ha **motivado a repensar** cómo apoyar a profesionales que son fundamentales para nuestra sociedad. Este propósito solo ha sido posible gracias al **respaldo y compromiso de una red excepcional**: una Junta Directiva que comparte nuestra visión, un Consejo Académico de alto prestigio, y un equipo docente excepcional apasionado y dedicado. Juntos, hemos construido una comunidad de aprendizaje y crecimiento que da vida a la misión del CEA.

*“A lo largo de este viaje, he aprendido que el compromiso y la colaboración son las piedras angulares para superar cualquier reto y construir un proyecto sólido y duradero.”*

Para lograr una transición exitosa, no basta con transferir responsabilidades; es crucial permitir que el nuevo responsable asuma el proyecto con autonomía y libertad para innovar. Por eso, en 2025, Lucía Márquez de la Plata tendrá la oportunidad de liderar el Centro y aportar su visión para seguir enriqueciendo el proyecto.

### PREGUNTAS PODEROSAS Y ESCUCHA ACTIVA

**Lucía Márquez de la Plata.-** Directora del CEA- Asumo esta responsabilidad con profunda motivación, comprometida a fortalecer todo lo que se ha logrado hasta hoy. Mi propósito es impulsar el crecimiento del centro y la asociación, apoyándome en los sólidos pilares que me han transmitido. Esta visión, construida a lo largo del tiempo, se apoya en dos ejes fundamentales: potenciar las fortalezas y la capacidad de innovar frente a los nuevos retos.

Por un lado, **reforzar los principios clave** que me ha transmitido “mi mentora”: la importancia de una comunicación clara, entender y conocer los fundamentos y prácticas de la gestión de riesgos y sus implicaciones, un trato cercano y personal, el cuidado de los detalles y un compromiso genuino con el desarrollo del talento para que las organizaciones alcancen la excelencia en la gestión de riesgos y seguros.

Por otro lado, **la innovación**, que no es una ruptura, sino un proceso de ‘afianzar, evolucionar y avanzar’. Me inspira profundamente poder continuar este camino, innovando desde una base tan bien cimentada, para ofrecer soluciones formativas especializadas y de gran valor.

“Carmen me ha brindado todas las claves, me ha mostrado el camino, y, con una generosidad inmensa, me ha dado las



herramientas, el conocimiento y el espacio para crecer y construir mi propia visión. Me ha impulsado a desplegar mis alas, me ha animado a aportar mi perspectiva y me ha dado la confianza para volar alto en esta nueva etapa. Desde mi experiencia en comunicación, gestión de proyectos y formación, tomo con gratitud y responsabilidad el legado que me ha confiado, con la intención de sumar a su legado y de honrar su guía, que siempre llevaré en el corazón.”

### UN FUTURO CON NUEVA ENERGÍA Y DIRECCIÓN

**Carmen Alonso.-** Finalizar esta etapa me deja un sentimiento de gratitud y satisfacción, sabiendo que he aportado al crecimiento de un proyecto que seguirá adelante con una nueva dirección. Este tiempo me ha enseñado lo importante que es adaptarse, planificar con sentido y mantener intacta la motivación.

A lo largo de estos años, **la colaboración y el compromiso** han sido claves en mi camino. Agradezco especialmente a **Gonzalo Iturmendi** (Presidente del CEA), **mi mentor**, por su apoyo e inmensa generosidad, su dedicación y pasión natural por la enseñanza y la formación de otros- **Gracias, Gonzalo, por acompañarme y por inspirarme a dar siempre lo mejor.**

En resumen, destaco los valores de mentorización, continuidad e innovación como pilares para el desarrollo de la gerencia de riesgos en el Centro de Estudios.



En 2024, hemos reforzado nuestra misión de formar y fortalecer capacidades en gestión de riesgos, ofreciendo oportunidades de capacitación a una amplia comunidad de profesionales –desde empresas, aseguradoras, mediadores y expertos– en cada etapa de su desarrollo.

# PLAN DE

# FORMACIÓN

# 2025

*¡Asegúrate el éxito en la gestión  
de riesgos y seguros!*

- + Contenidos de plena actualidad
- + Importantes novedades
- + En tres modalidades diferentes
- + Accesible desde cualquier lugar
- + Equipo docente referente en el sector

DESCARGA EL PLAN DE FORMACIÓN PINCHANDO AQUÍ



El CEA presenta su innovador Plan de Formación 2025, diseñado para impulsar la excelencia en la gestión de riesgos y seguros. Esta propuesta estratégica responde a un sector en transformación, ofreciendo herramientas actuales para enfrentar desafíos como la ciberdelincuencia, la inteligencia artificial y los riesgos climáticos. Con un equipo docente de referencia, el plan introduce novedades clave para preparar a los profesionales frente a riesgos emergentes y modernos.

## Novedades en el plan de formación

### RIESGOS CIBERNÉTICOS

*"Este es uno de los principales riesgos que pueden provocar daños elevadísimos en nuestras organizaciones. Si no quieres limitarte a preocuparte, sino también ocuparte, los contenidos de este curso te permitirán avanzar en este riesgo tan complejo"*

**Juan Gaya -**

Director Riesgos y Seguros, El Corte Inglés



### CUANTIFICACIÓN DE RIESGOS

*"La cuantificación de riesgos es una herramienta clave en la gestión moderna, permitiendo una toma de decisiones más sólida y basada en datos. Es un conocimiento esencial, incluso en un nivel introductorio, para enfrentar los desafíos actuales."*

**Rodrigo López Calleja -**

Head of Global Risk and Insurance- Globalvia



### LOS 100 PRIMEROS DÍAS EN LA GESTIÓN DE RIESGOS

*"El alcance de la gestión de riesgos es tan amplio que puede resultar abrumador. En este curso estructuramos los primeros pasos que ayudarán a enfocar los primeros 100 días de forma efectiva."*

*"En este curso te ayudaremos a planificar qué aspectos son claves en cualquier compañía y cómo se deberían priorizar los proyectos para generar el mayor impacto positivo en la organización a través de contenidos avanzados, de las herramientas y el contexto práctico necesario para abordar con confianza los principales retos al iniciar la función de gestión de riesgos."*

**Edgar García Corominas -** Chief Risk Officer-  
Internal Audit director – CELSA GROUP

**Victor Garcia -** VP Internal Audit & Risk  
Management – Archroma



### RIESGOS DE SOSTENIBILIDAD

*"En el contexto de nuevas regulaciones (CSRD, CSDDD, Taxonomía, etc.) y una creciente demanda de transparencia en temas ESG, la formación sobre Gestión de Riesgos global, y específicamente la gestión de riesgos de sostenibilidad, ofrece a las empresas y a los gerentes de riesgos las herramientas necesarias para su gestión de manera integral. Aprenderán a identificar y analizar riesgos asociados a factores ambientales, sociales y de gobernanza, además de adaptarse a la nueva directiva europea que establece exigencias para el reporting de impactos financieros y no financieros. Este curso proporciona una guía práctica para la gestión de riesgos de sostenibilidad y el cumplimiento normativo"*

**Isabel Martínez Torre-Enciso -** Non Executive  
director. ESG. Global Risk & Crisis Mgmt.



### GESTIÓN DE RIESGOS DE RC DE PRODUCTO Y DE LA INTELIGENCIA ARTIFICIAL.

*"Este curso es ideal para profesionales de distintas áreas transversales y gestión de riesgos interesados en integrar la IA de manera segura y ética en sus productos y servicios"*

*"Diseñado para proporcionar un entendimiento integral sobre los riesgos legales y de responsabilidad civil vinculados a la inteligencia artificial en productos, lo que permite a los profesionales no solo conocer el marco regulatorio, sino también adoptar prácticas de gestión de riesgos que garanticen un uso responsable y seguro de la IA en productos y servicios, identificar los riesgos específicos de productos basados en IA, comprender la normativa vigente y anticipar posibles cambios regulatorios que podrían afectar a la organización."*

**Gonzalo Iturmendi -** Dirección Bufete G.Iturmendi y Asociados. Presidente del CEA. Secretario de AGERS.

**Jesús Jimeno Muñoz -** PhD- Lawyer- Curator Global Shapers Madrid- Legal Risk Lab- DSG ABOGADOS



# IN-COMPANY

El Centro de Estudios de AGERS, especializado en realizar cursos incompany adaptados a las necesidades de las organizaciones y sus equipos.

## Perfiles profesionales

1. Equipos técnicos empresa

2. Suscriptores especializados en riesgos empresariales

3. Desarrollo Negocio

4. Mediadores a nivel Nacional

5. Gerentes de riesgos

- Especialización en análisis y evaluación riesgos distintos roles
- Análisis riesgos de daños materiales
- Responsabilidad Civil
- Continuidad de negocio y Pérdida de beneficios.
- Tratamiento de riesgos y transferencia seguros
- Riesgos ciber y medioambiental y su aseguramiento
- Gestión de siniestros

## Cursos impartidos

**REALE SEGUROS**

**MAPFRE**

**AXA**

**XL Insurance Reinsurance**

**BARCELONA**  
COL·LEGI DE MEDIADORS D'ASSEGURANCES

**AUNNA**  
ASOCIACIÓN

grupo **elecnor**

**Espabrok**  
GENERAMOS CONFIANZA

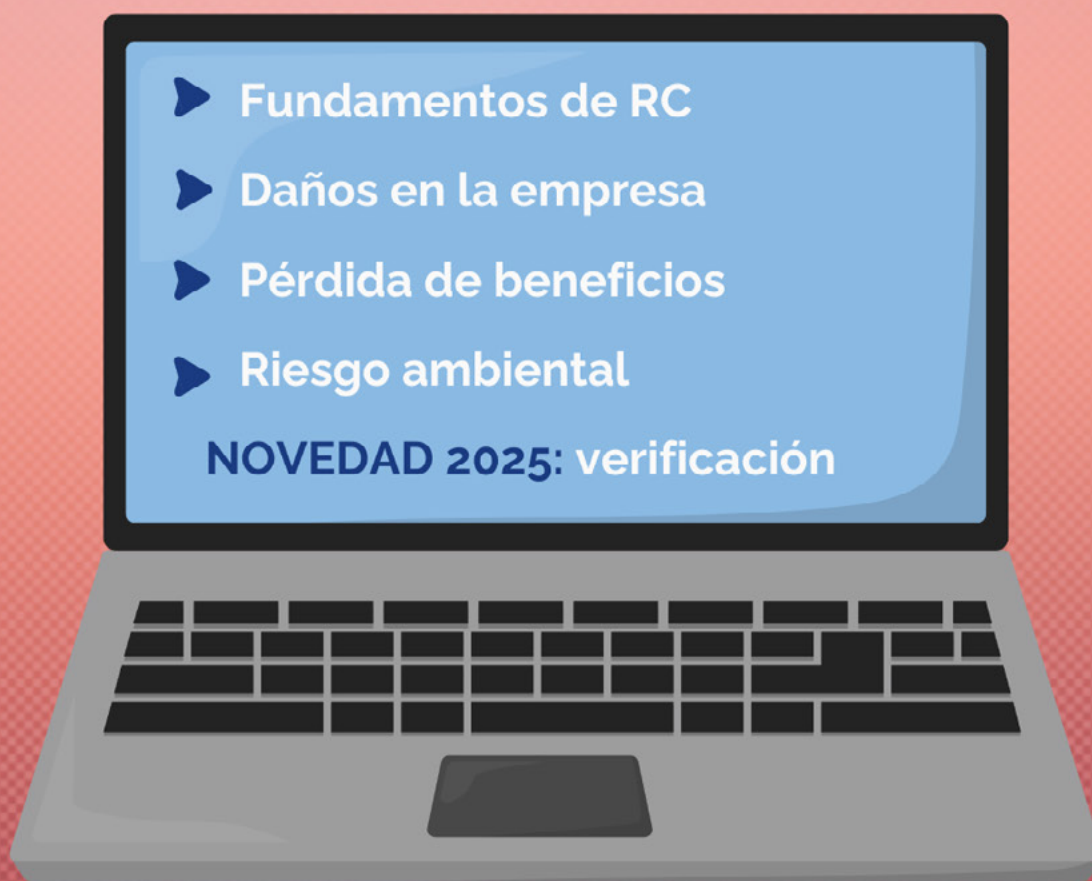
**COLEGIO PROFESIONAL DE MEDIADORES DE SEGUROS DE VALENCIA**

**Senda**  
Vivir seguros.

MÁS INFORMACIÓN PINCHA AQUÍ

# Los esenciales de AGERS

# Cursos online



- ▶ Fundamentos de RC
- ▶ Daños en la empresa
- ▶ Pérdida de beneficios
- ▶ Riesgo ambiental

**NOVEDAD 2025: verificación**

Aprende, actualiza y domina la gestión de riesgos y seguros desde cualquier lugar

 **ACCEDE AQUÍ**



# 82

AGERS es la única asociación española acreditada por FERMA (Federación Europea de Asociaciones de Gerencia de Riesgos) para la certificación RIMAP en español, tras haber superado numerosos requisitos para este convenio de equivalencia con el examen original. Es una certificación profesional independiente que mide y certifica las competencias y experiencia de los profesionales (normalmente en activo) que quieren obtenerla.

La certificación RIMAP, dirigida a gestores de riesgos y seguros, así como a otros profesionales involucrados en áreas de auditoría, derecho, finanzas, procurement, continuidad de negocio, salud y bienestar, homologa a nivel europeo a aquellos gestores de riesgos que quieren dar un salto cualitativo en su desarrollo profesional.

Permite crear, acoplar conocimientos, prácticas y enfoques innovadores entre los miembros de las distintas asociaciones y la sociedad a nivel europeo. Proporciona reconocimiento y oportunidades a nivel internacional, alta cualificación, competencia laboral y reputación para las organizaciones que cuenten con profesionales certificados.

La certificación se obtiene tras la preparación y superación de un examen de 2 horas de duración que implica superar conocimientos, metodologías y herramientas propuestos por FERMA para homogeneizar criterios, lenguaje y prácticas de los profesionales involucrados en este rol dentro de sus organizaciones.

## ABIERTAS DOS NUEVAS CONVOCATORIAS CERTIFICACIÓN RIMAP EN 2025

**1** Rellena tu Inscripción

**2** Sesión Informativa

**3** Material y acceso a training online

**4** Tutoría de dudas

**Examen en español**

**Próximas convocatorias:**  
 05 junio 2025 | 06 noviembre 2025

Modalidad online | 2 horas de duración

**660€**  
IVA no incluido

**600€ para asociados**

**RESERVA TU PLAZA PINCHANDO AQUÍ**

FERMA, al igual que AGERS, comparte los objetivos de desarrollo y la profesionalización de los gerentes de Riesgos.

¿Cómo continuar tras la certificación Rimap alcanzando un ERM más maduro? Anualmente desde FERMA se celebran anualmente el Workshop Advanced y el Lloyds Program. Desde el CEA informamos de la programación anual.



Certificados RIMAP en español en el Ferma Forum 2024

**Los criterios para mantener la Certificación RIMAP en nuestra web y estamos a vuestra disposición para orientar cómo conseguir los CPD**

# CERTIFICADOS DESDE 2018

AGERS celebra más de 60 certificaciones RIMAP en Español:  
Un paso significativo hacia la profesionalización y homologación europea.

2018



Rafael Bauer  
(Mapfre)



Pedro López  
(Grupo ALM)



Juan Carlos Sánchez  
(Correos)



Ignacio Aznar  
(Cyc Ingenieros)



Gustavo Molina  
(Profunda Gestión de Riesgos Empresariales)



Esther López  
(Esteve)



Carlos Montesinos  
(CGPA)



Luis Lancha  
(SENER)



Javier Cobian  
(COBIAN INSURANCE BROKER SL)

2020

2021



Ismael Muñoz  
(Marsh)



Reyes Fuentes  
(Aleatica)



Miguel Eusa  
(Tabacalera S.L.U.)



Iñigo Rodríguez,  
(Velatio)



Balbino Luna  
(Correduría Asociada a Willis Network)



Cinthia Prado  
(Indra)



Cintia García  
(Vantevo)



Cristina Gómez  
(Moeve)



David Cruanyes  
(Quality Brokers)

2022



Eva Perez  
(Impala Terminals Group)



Jorge Granda  
(Caja Rural de Asturias)



Jose María Buendia  
(Moeve)



Alvaro Hernandez  
(Grenergy Renovables)



Antonio López  
(Bankinter)



César Asunción  
(Bankinter)



Eduardo Ortiz  
(Recoletos Consultores)



Ignacio Martín  
(Repsol)



Javier Vazquez  
(Idealista)

2023



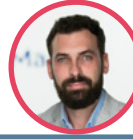
Jordi Huguet  
(Corredor d'asseurances)



Juan Carlos Díaz  
(Ferrer & Ojeda)



María Martínez  
(IDOM Consulting)



Miguel Yébenes  
(Marsh)



Susana Sánchez  
(Mutual Médica)



Noelia Agulló  
(Coinbroker)



Inma Fabregat  
(Mediador Seguros)



Aitor Alberdi  
(GV42)



Giovanni Cezimbra  
(Francel Seguros)



Pablo Gaitan  
(SCV Seguros)



Cristina Perez  
(Pascual)



Álvaro Rodrigo Miño  
(Aleatica S.A.U.)



Víctor Lombardero  
(QUADIS)



Isabel Arroyo  
(Recurrent energy)



Francisco Norte  
(Asevasa)



Miquel Àngel Seguí  
(Mutual Médica)



Juan José Pages  
(Asycor)



Roberto Ramírez  
(Rmz Asesores)

2024



Marta Vega  
(Exolum)



Mario Ramírez  
(Exolum)



Francisco José Cáceres  
(Andamur, S.L.U.)



Iván Pérez  
(Allianz)



Xavier Vilaró  
(Grupo Risk Management)



Ysabel Machado  
(WTW)



Carlos Calderón  
(Tres Mares)



Sebastián Perelló  
(Servibroker)



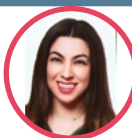
Alejandro Altares  
(Marsh)



Alejandro Mocholi  
(FerrandizMocholi)



Álvaro Villaseca  
(Mapfre)



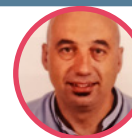
Marta Lavín  
(Sedisa)



Ignacio Ripols  
(E-tec)



César Martín  
(Alsa)



Manuel Noya  
(Cosmobrok)



Benjamín Cedeño  
(Expertropolis)

¡Enhorabuena a todos los certificados!

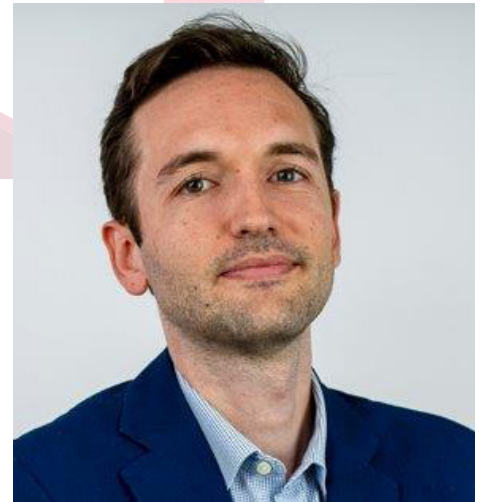
84

# Voces RIMAP: innovación en riesgos y seguros

El Centro de Estudios de AGERS abre una nueva sección con el objetivo de dar voz a sus alumnos certificados y que puedan contar su experiencia en la aplicación práctica de los conocimientos obtenidos en su formación.

Álvaro Rodrigo Miño

Líder de Riesgos en ALEATICA, S.A.U./ Alumni CEA-  
7ª Edición Postgrado Experto en Gerencia de Riesgos.  
Certificado RIMAP 2023



## Gestión de Riesgos desde 0

Mi trayectoria profesional se inicia en colaboración con la Universidad Pontificia de Comillas cursando dos prácticas, primero en el despacho de abogados "Uría Menéndez" en el Departamento de Derecho Mercantil, y posteriormente en la consultora "Servicios profesionales integrados" para la realización de labores contables y fiscales.

Terminada la doble licenciatura en Derecho y Administración de Empresas me uno a Deloitte, al Departamento de Auditoría Financiera para los sectores de Telecomunicaciones, Energía y Utilities. Durante los dos primeros años participo como asistente en auditorías financieras de grandes clientes españoles y a partir del segundo año comienzo a realizar también asignaciones propias de auditoría interna, gestión de riesgos, control interno, compliance y forensic.

Posteriormente, y tras casi cinco años en Deloitte, donde alcanzo la categoría de Experienced Senior, me incorporo a ALEATICA con el objetivo de diseñar e implementar el sistema de gestión integral de riesgos en toda la Organización, siguiendo los mejores estándares internacionales (COSO ERM e ISO 31000). Asimismo, entre mis actividades actuales destacan temas relacionados con control interno, cultura de riesgos, reporting, proyectos de Continuidad del Negocio, Protección de Datos y Ciberseguridad, etc.

Dada mi experiencia en materia de gestión de riesgos, decido cursar el Posgrado Experto en Gerencia de Riesgos impartido por AGERS y la Universidad de Barcelona y obtener posteriormente la certificación Rimap. Entre

las razones que me motivaron a realizar esta certificación destacaría.

- Recabar un reconocimiento formal a nivel europeo que ponga de manifiesto mis conocimientos y capacidades sobre la materia, y especialmente de cara a terceros. Se trata de una certificación que se traduce en una garantía de profesionalidad y experiencia en gestión de riesgos.
- Ampliación y consolidación de mis conocimientos sobre la gestión de riesgos y seguros, y cómo proceder a su aplicación en el día a día.
- Mayor actualización y red de contactos sobre este campo.

### GESTIÓN DE RIESGOS DESDE CERO

Podemos afirmar que actualmente la gestión profesionalizada de los riesgos y oportunidades es una palanca de valor que contribuye al éxito sostenible a largo plazo de cualquier organización.

A medida que las entidades crecen, van tomando conciencia de que la gestión proactiva e integral de los ries-



gos les ayuda a mejorar su resiliencia, competitividad y capacidad para adaptarse a un entorno cada vez más dinámico. Ahora bien, ¿por dónde comenzamos a estructurar toda esta disciplina?

En primer lugar, se requiere de un análisis detallado de los marcos metodológicos que en materia de gestión de riesgos podemos emplear. En concreto, podemos tomar como referencia los dos estándares internacionales más empleados: COSO ERM e ISO 31000. Si bien ambos marcos presentan muchos puntos en común, existen diferencias clave que pueden ayudar a una organización a decantarse por uno u otro modelo. La selección de un marco u otro, o la combinación de ambos, dependerá entre otras cuestiones de las necesidades específicas de la organización, sus objetivos en materia de gestión de riesgos, su entorno y cultura. Por ejemplo, una organización tecnológica que opere en un entorno muy dinámico podría optar por el marco ISO 31000 al proporcionar una guía más sencilla y flexible que COSO ERM.

Analizados estos estándares, y determinado el marco a aplicar en la gestión de riesgos, podemos hablar de una serie de pasos o etapas generales:

1. **Entendimiento del contexto** tanto interno como externo, es decir, análisis de todos aquellos factores que pudieran afectar a la organización en su desempeño (políticos, económicos, medioambientales, compliance, capital humano, tecnológicos, etc.). Lo anterior incluye además el análisis de las partes interesadas y en específico de sus expectativas y necesidades.
2. **Comprender la estrategia y objetivos de la organización.** Este punto resulta clave de cara a la alineación de la estrategia y objetivos con la gestión de riesgos. Dicho en otras palabras, es necesario identificar, evaluar y gestionar aquellos riesgos y oportunidades que pudieran impactar sobre la estrategia y los objetivos del negocio, y todo ello de acuerdo con el apetito y tolerancias definidas.
3. **Asegurar el compromiso del Consejo y la Alta Dirección.** El liderazgo y apoyo de estos actores resulta clave de cara a: a) Garantizar el correcto diseño e implementación del sistema de gestión de riesgos en la organización (por ejemplo, a través de la definición de roles y responsabilidades, incentivos, políticas y normas, etc.), b) Fomentar realmente una cultura de riesgos en la organización iniciándose desde los niveles más altos hacia abajo, y c) Proveer de los recursos necesarios para una adecuada gestión de riesgos.
4. **Identificación de riesgos.** Aplicar técnicas para identificar los riesgos que pudieran afectar a la estrategia y ob-

jetivos de la organización (por ejemplo, brainstorming, encuestas y cuestionarios, DAFO, PESTEL, lecciones aprendidas, análisis de procesos, etc.) y proceder a su documentación en un registro o inventario, al mismo tiempo que se desarrolla un universo o taxonomía de riesgos.

5. **Evaluación de riesgos y priorización.** Evaluar riesgos de acuerdo con las escalas de impacto y probabilidad definidas por la organización, y en función de su exposición, proceder a su priorización de cara a su respuesta. La organización determinará si se trata de una evaluación cuantitativa, cualitativa o ambas.
6. **Tratamiento de riesgos.** Definir cómo se van a tratar los riesgos (evitar, aceptar, reducir o transferir / compartir). Seleccionada la respuesta, en función de la exposición del riesgo, se podrán definir planes de mitigación a implementar que habrán de ser objeto de seguimiento activo conjuntamente con su responsable.
7. **Monitoreo y revisión.** El sistema de gestión y mapa de riesgos ha de ser revisado y en su caso actualizado con la periodicidad que se determine. De esta forma se garantiza que la gestión de riesgos está siendo eficaz y que los tratamientos de respuesta son efectivos.
8. **Comunicación y consulta.** La información sobre riesgos ha de ser reportada con el correspondiente grado de detalle y la frecuencia oportuna a los distintos stakeholders. Asimismo, se ha de garantizar que todos los empleados cuentan con acceso a canales óptimos para informar sobre nuevos riesgos o cambios materiales sobre los riesgos.
9. **Capacitación y concienciación.** Promover una auténtica cultura de riesgos en la organización, es decir, fomentar una cultura de conciencia del riesgo, propiedad, responsabilidad y aprendizaje, promover un diálogo abierto y constructivo sobre riesgos y oportunidades y mejorar las capacidades de riesgo (habilidades, conocimientos, herramientas y sistemas).
10. **Mejora continua:** Revisar, actualizar e incorporar mejoras al sistema de gestión de riesgos.

**En conclusión,** y si bien las etapas anteriores no constituyen una referencia absoluta, sí que han de entenderse como un marco que todo gestor de riesgos debería plantearse en la implementación de un sistema de gestión de riesgos eficaz.

Desde mi experiencia, contar con una checklist de actividades resulta de gran utilidad al aportar una estructura o guía alineada con los mejores marcos metodológicos de aplicación sobre la materia, aporta eficiencia en términos de tiempo y recursos, y permite un seguimiento más oportuno de todo este proceso.

## PREGUNTA PARA SIGUIENTES CERTIFICADOS RIMAP



¿Cómo estás aplicando actualmente en tu empresa lo aprendido con la certificación RIMAP? / ¿Se está teniendo en cuenta? **Álvaro Rodrigo Miño**

# VIII EDICIÓN PREMIO JULIO SÁEZ

[PUBLICACIONES  
PREMIADAS  
PINCHANDO AQUÍ](#)

Este reconocimiento rinde homenaje a Julio Sáez, uno de los grandes impulsores del desarrollo de la gestión de riesgos en España, recordado como una figura clave en el sector.



[BASES CONVOCATORIA PREMIO JULIO SAEZ 2025](#)



UNETÉ A  
NUESTRA  
COMUNIDAD

9:30  
Wednesday

agers

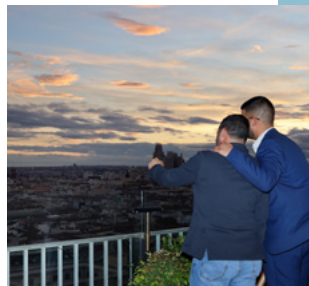
PINCHA AQUÍ





88

# RISKER FEST II



El Centro de Estudios de AGERS (CEA) acogió con gran éxito la segunda edición del Risker Fest, un encuentro presencial exclusivo de su comunidad Alumni, consolidando este evento como una cita clave para los profesionales del sector de la gestión de riesgos y seguros. Se ha convertido en un espacio imprescindible para fortalecer vínculos entre compañeros del sector y generar sinergias entre profesionales interesados en esta área.

Los alumnos asistentes disfrutaron con la intervención de Carmen Bustos, socia fundadora de Soulsight y Wander, una líder excepcional en el mundo de la innovación y la transformación de las organizaciones, que compartió una experiencia inspiradora bajo el título: «Una mirada humanista y creativa».

La comunidad Alumni de AGERS, que nació en 2021, tiene como objetivo reunir a los asociados y a los alumnos de los postgrados universitarios que ofrece, proporcionando una oportunidad única para intercambiar ideas y estrechar lazos.

El Club Financiero Génova fue el escenario del encuentro, en el que se disfrutó de la ceremonia de graduación de la 6ª edición del Programa de formación avanzada en Gestión de Riesgos y Seguros, en colaboración con la Universidad CEU-Cardenal Herrera, la 7ª edición del Postgrado experto en Gerencia de Riesgos, en colaboración con la Universidad de Barcelona, y de los alumnos certificados RIMAP (European Risk Management Certification), en un evento orientado a fomentar el networking entre los asistentes.

¡TE ESPERAMOS EL AÑO QUE VIENE EN EL RISKER FEST III!

## Testimonios Alumnis RISKER FEST

### “ LA IMPORTANCIA DE EVENTOS COMO EL RISKER FEST

“Este tipo de eventos, pone en valor las formaciones y actividades que desde AGERS nos dan la oportunidad de participar y de adquirir conocimientos. Pero, sobre todo, la oportunidad de poder estar en contacto con compañeros de diferentes industrias, que entre todos nos complementamos y nos enriquecemos. Es lo más importante, poder reunirnos de vez en cuando y complementarnos”;

**Alejandro Altares-**

**Senior Client Executive-Marsh**



### “ EL SIGNIFICADO DE SER ALUMNI DE AGERS

“La importancia de poder estar en contacto con los profesionales del sector, y de poder acceder a una formación actualizada, permanente y con conocimientos útiles para el día a día”

**Alfredo Portillo-**

**Insurance Specialist-Sener**

### “ EL VALOR DEL NETWORKING CON PROFESIONALES DEL ÁREA

“Estos eventos te permiten conocer a gente del sector y conectar con gente de toda la vida para actualizarnos, hablar de cosas de actualidad, ... Pero sobre todo, el networking que a nivel personal te llevas, el poder estar en contacto con amigos y profesionales del sector se agradece”

**Ulysses Grundey-**

**Head of Sales FINEX Spain-WTW**





# «Programas de Seguros Internacionales»

EL CLUB DE ASEGURADORES INTERNACIONALES (CAI), EN COLABORACIÓN CON LA ASOCIACIÓN ESPAÑOLA DE GERENCIA DE RIESGOS Y SEGUROS (AGERS) Y ALLIANZ COMMERCIAL, HA ORGANIZADO UN DESTACADO DEBATE SOBRE LOS «PROGRAMAS DE SEGUROS INTERNACIONALES». EL EVENTO, MODERADO POR FRANCESC RABASSA, DIRECTOR GENERAL DE CA LIFE INSURANCE EXPERTS, SE CENTRÓ EN LA GESTIÓN EFECTIVA DE RIESGOS GLOBALES, EL CUMPLIMIENTO DE REGULACIONES LOCALES Y LA OPTIMIZACIÓN DE COSTOS DE SEGUROS.

LA ASOCIACIÓN  
20/06/2024



Alejandra Triviño, responsable de Infraestructura de Seguros para Europa, LatAm y Medio Oriente en Ferrovial, explicó que los seguros internacionales están diseñados para cubrir riesgos en distintas geografías, adaptándose a las necesidades de empresas internacionalizadas. Triviño destacó las diversas modalidades de seguros que varían según la ubicación de la empresa matriz y sus filiales.

Ana Garmendia, abogada y asociada en Herbert Smith Freehills, subrayó la importancia de coordinar las pólizas locales con la póliza maestra de la empresa para garantizar una cobertura adecuada y evitar sanciones regulatorias. Además, Milagros Sanz, consultora de apoyo profesional en Herbert Smith Freehills, ofreció recomendaciones para el manejo de siniestros bajo un programa de seguro internacional. Sanz destacó la importancia de contar con una estrategia clara para la gestión de reclamaciones, asegurando que las respuestas sean rápidas y efectivas para minimizar el impacto en las operaciones de la empresa.

Raquel Caballero, gerente de seguros del departamento legal de Mango, destacó la preferencia de su empresa por pólizas locales integrales dentro de una modalidad premium, enfatizando la necesidad de conocer bien los riesgos para configurar adecuadamente los seguros y recibir asesoramiento adecuado.

Asier López, jefe regional de Multinacional Iberia en Allianz Commercial, resaltó la importancia de gestionar siniestros de manera efectiva con equipos locales y una red sólida de peritos. López señaló que una coordinación eficaz y una red internacional sólida son esenciales para asegurar una gestión de riesgos homogénea en todas las filiales de la empresa.

Karine Chihimi, líder de práctica de mercado multinacional y estrategia de distribución en Allianz Commercial, habló sobre las tendencias actuales en los programas de seguros internacionales, incluyendo el uso creciente de seguros cautivos y la digitalización de los servicios. Chihimi enfatizó que la digitalización permite una gestión más eficiente y una mayor transparencia en las pólizas de seguros, faci-

## PROGRAMAS DE SEGUROS INTERNACIONALES



### MODERADOR

Francesc Rabassa Montesinos (*Director General CA Life Insurance Experts*)

### PONENTES

#### Visión Aseguradora:

Asier López (*Regional Head of Multinational Iberia Allianz Commercial*)

Karine Chihimi (*Multinational Market Practice Leader & Distribution Strategy Allianz Commercial*)

#### Visión Cliente/Gerente de Riesgos:

Alejandra Triviño Hage (*Head of Infrastructure Insurance Europe, LatAm & Middle East Ferrovial*)

Raquel Caballero (*Insurance Manager Legal Department MANGO*)

#### Visión Jurídica:

Milagros Sanz (*Lawyer/ Professional Support Consultant en Herbert Smith Freehills*)

Ana Garmendia Prieto (*Lawyer & Associate en Herbert Smith Freehills*)

tando el seguimiento y la administración de reclamaciones en múltiples jurisdicciones.

Este debate subraya la necesidad de una coordinación global efectiva y la adopción de herramientas digitales para la gestión y seguimiento de pólizas, destacando la evolución constante en el campo de los seguros internacionales.



ACCEDA AL VÍDEO COMPLETO PINCHANDO AQUÍ

92

**Desayuno**

**«DE TÚ A TÚ» con**

**Alejandra Galdos de HSF  
y Marta Vega de Exolum**



**LA ASOCIACIÓN  
20/09/2024**



**ACCEDA AL VÍDEO COMPLETO PINCHANDO AQUÍ**



**AGERS CELEBRÓ OTRO EMOCIONANTE DESAYUNO «DE TÚ A TÚ», UNA SESIÓN EXCLUSIVA QUE CONTÓ CON LA PARTICIPACIÓN DE ALEJANDRA GALDOS, ABOGADA DEL EQUIPO DE DISPUTE RESOLUTION DE HERBERT SMITH FREEHILLS, Y MARTA VEGA, RESPONSABLE DE RIESGOS Y SEGUROS DE EXOLUM.**

Durante el evento, Alejandra compartió su experiencia profesional en un entorno cercano y fresco. Conversamos sobre los retos y oportunidades a los que se enfrenta en su carrera, abordando desde sus inicios hasta su actual labor en la gestión de disputas legales complejas. Habló sobre cómo equilibra la representación de diferentes intereses dentro de su despacho y destacó la importancia de mantenerse flexible y resiliente en un entorno dinámico y cambiante.

Además, Alejandra contó varias anécdotas personales y profesionales que resaltaron su trayectoria y cómo ha superado los desafíos en los tribunales y en su carrera. También reflexionó sobre la importancia de adaptarse a las necesidades de la industria y mantenerse actualizada en un entorno en constante evolución.

Marta Vega, como moderadora, guió la conversación de manera brillante, invitando al público a participar y fomentar el debate sobre las complejidades del mundo del riesgo y las oportunidades emergentes para los profesionales del sector.

Alicia Soler, Directora de AGERS, expresó su agradecimiento a las ponentes y a los asistentes, destacando que estos encuentros contribuyen a compartir conocimiento e inspirar a los profesionales de la gerencia de riesgos. «Este tipo de espacios nos permiten profundizar en temas clave y fomentar un entorno de colaboración y aprendizaje continuo».

Como parte de la sesión siempre realizamos una grabación de la intervención completa de ambas ponentes para aquellos que no pudieron asistir. La grabación está disponible en todos los canales de AGERS.



**Próximo "De tú a tú"**  
 Con Sara García de Iberia  
 y Marta Vega

**EVENTO HÍBRIDO**

\*Plazas presenciales limitadas

**Sara García González-Horrero**

**Marta Vega**  
 Responsable Riesgos y seguros en EXOLUM

agers alumni CEA Centro de Estudios de AGERS



# Foro sobre Litigiosidad en USA con BHSI

LA ASOCIACIÓN  
01/10/2024

EL PASADO 1 DE OCTUBRE DE 2024 EL EQUIPO DE BHSI, LIDERADO POR CONSTANZA GÁLLEGOS, BEATRIZ RUBIO Y JAVIER VILLALBA, TUVO LA OPORTUNIDAD DE DIRIGIRSE A LOS MIEMBROS ASOCIADOS DE EMPRESAS DE BARCELONA DE AGERS ACERCA DE LAS TENDENCIAS DE LA LITIGIOSIDAD EN ESTADOS UNIDOS PONIENDO ESPECIAL FOCO EN LAS EXPOSICIONES DE RESPONSABILIDAD CIVIL.



La sesión principalmente se centró en 3 aspectos siendo estos el panorama jurídico, **consideraciones de suscripción** y la inflación social. En el primer bloque Constanza menciona los **daños punitivos** definidos como la sanción económica incluida dentro de la indemnización con un ánimo de castigar una conducta reprochable, la competencia del jurado en reclamaciones de daños y de responsabilidad civil frente al papel del juez y la obligación de cada parte de correr con sus propias costas (contingency fee). Igualmente en la sesión se tuvo oportunidad de comentar factores de riesgo dentro de la **litigiosidad en Estados Unidos** como son agresividad y tenacidad de los demandantes y de sus abogados a la hora de cuantificar y de perseguir sus reclamaciones, las acciones colectivas en aumento sobre todo en la RC producto o la amenaza de acusar a las aseguradoras de mala fe lo que supone un aliciente para llegar a acuerdos, la cada vez más extendida presencia de reclamaciones por daños medioambientales en relación con las PIFAS o el llamado Forum shopping. Hubo mención a la cada más creciente presencia de los fondos de litigación.

Este caldo de cultivo ha provocado lo que se conoce coloquialmente como “agujeros judiciales” o “Hell Holes” en los que podemos hablar de **8 estados** en los que resultan especialmente desproporcionadas las cantidades que se conceden a los reclamantes. Este año ocupa el primer lugar Pennsylvania, unas jurisdicciones en la que se favorece el fórum shopping.

Factores importantes para las consideraciones de suscripción ante la presencia en USA son la existencia de un **programa internacional**, posible exigencia estatal, cuáles son las coberturas necesarias y cómo se comportarán los gastos de defensa ante ellas. Importante también considerar ante las exportaciones cómo se exporta la mercancía allá, la cobertura del distribuidor y las cláusulas de acuerdos de exención de responsabilidad junto con el tratamiento dado por la póliza a los daños punitivos.

En último lugar, se trató la **inflación social** como un elemento que acrecienta el coste último de los siniestros que para las aseguradoras muy por encima de la inflación general o económica y se dieron referencias a las causas que generan dicha inflación social como una mayor litigiosidad provocada por los efectos llamada de sentencias cada vez mayores, mejores técnicas de selección de jurados, búsqueda de argumentos psicológicos como el sesgo del ancla y la teoría del reptil para causar en los potenciales jurados la sensación de desamparo frente a las grandes corporaciones. Se dieron ejemplos de 3 casos en los que esto especialmente era evidente.

La sesión concluyó con un animado debate acerca de cómo podían los asegurados **proteger sus riesgos** en Estados Unidos y de cuáles eran los principales desafíos que se enfrentaban a la hora de desarrollar sus programas

**¡Transforma tu conocimiento  
con AGERS!**

Más de **300 videos** en el canal  
¡Síguenos!



**#CanalAGERS**



**ager̄s**



# Howden y AGERS Abordan la Coyuntura del Seguro de Crime y los Retos Cibernéticos

## en un Desayuno de Trabajo

EN UN EVENTO ORGANIZADO POR **HOWDEN Y AGERS** (ASOCIACIÓN ESPAÑOLA DE GERENCIA DE RIESGOS Y SEGUROS), SE ANALIZÓ EL ESTADO ACTUAL Y LOS DESAFÍOS DEL MERCADO ASEGURADOR EN RELACIÓN CON EL SEGURO DE "CRIME" Y LOS CRECIENTES RIESGOS CIBERNÉTICOS. ESTE DESAYUNO DE TRABAJO, CELEBRADO EN LAS OFICINAS DE HOWDEN, BRINDÓ A LOS ASISTENTES UNA VISIÓN PROFUNDA DE LAS NECESIDADES EMERGENTES EN UN MERCADO CADA VEZ MÁS AFECTADO POR LA DIGITALIZACIÓN Y LAS AMENAZAS EN LÍNEA.

LA ASOCIACIÓN  
07/10/2024





El evento contó con la colaboración de la Comisión de Ciberseguridad de AGERS y de reconocidos expertos, entre ellos **Manuel Pérez Martín de la Hinojosa**, Head of Cyber para el sur de Europa y LatAm en Howden, y **Max Deltenre**, Responsable de Líneas Financieras de la misma compañía. En sus intervenciones, los especialistas abordaron la interacción y, en algunos casos, el solapamiento entre las coberturas de Crime y Cyber, así como las mejores prácticas para proteger a los clientes.

Según explicó **Manuel Pérez**, aunque las coberturas de Crime y Cyber suelen ser solicitadas conjuntamente, cada una cumple funciones específicas: el seguro de Crime cubre fraudes como transferencias no autorizadas de fondos, mientras que el seguro de Cyber protege contra brechas de datos, costos de recuperación y daños reputacionales derivados de ataques cibernéticos.

**Max Deltenre**, por su parte, subrayó que el objetivo principal de esta jornada fue analizar cómo se solapan las coberturas de seguros de Crime y Cyber, además de promover buenas prácticas para transferir estos riesgos al mercado asegurador, protegiendo así a los clientes de los riesgos asociados con actos fraudulentos y ciberataques.



Este encuentro se destacó como un espacio para fortalecer la resiliencia y la seguridad del sector asegurador en España, ofreciendo a los gerentes de riesgos una comprensión más profunda de las necesidades actuales del mercado de Crime y de los enfoques estratégicos que pueden adoptar frente al avance de los ciberataques.



[ACCEDE A LAS ENTREVISTAS](#)



## FUNDACIÓN MUTUALIDAD Y AGERS DEBATEN EL Envejecimiento como Riesgo Empresarial

LA **FUNDACIÓN MUTUALIDAD Y AGERS** (ASOCIACIÓN ESPAÑOLA DE GERENCIA DE RIESGOS Y SEGUROS) ORGANIZARON UN WEBINAR PARA ABORDAR EL ENVEJECIMIENTO COMO RIESGO EMPRESARIAL. EN UN DEBATE QUE REUNIÓ A EXPERTOS EN GESTIÓN DE RIESGOS, RECURSOS HUMANOS Y DIRECTIVOS DE DIVERSAS ENTIDADES, SE EXPLORARON LOS RETOS Y OPORTUNIDADES QUE PRESENTA EL ENVEJECIMIENTO DE LA FUERZA LABORAL PARA LAS EMPRESAS EN ESPAÑA.

LA ASOCIACIÓN  
07/11/2024



**Blanca Narváez**, Directora General de la Fundación Mutualidad, como moderadora, junto a **José Miguel Rodríguez Pardo**, Presidente de la Escuela de Pensamiento de la Fundación Mutualidad, **Gonzalo Iturmendi**, Secretario General de AGERS y Socio Director de Bufete G. Iturmendi y Asociados y **Gregorio Gil de Rozas**, Head of Retirement de Willis Tower Watson, como ponentes destacaron la importancia de la gestión intergeneracional y la colaboración en los equipos de trabajo, promoviendo un enfoque que integre tanto a empleados jóvenes como a profesionales senior. La discusión también incluyó recomendaciones para incluir la edad en las políticas de diversidad e inclusión, sugiriendo que los Consejos de Administración impulsen una «mesa de edad», para tratar estos temas de forma estructurada, similar a otros ejes de diversidad como género y orientación sexual.

Señalaron que las organizaciones deben tomar medidas preventivas para evitar los riesgos legales derivados del edadismo y otros posibles conflictos de discriminación. La ley 15/2022 fue citada como un marco jurídico que ampara los derechos fundamentales de los empleados senior, con ejemplos de reclamaciones y sanciones considerables impuestas a empresas por incumplir estos principios. Los expertos recomendaron que los Consejos de Administración y los departamentos de Recursos Humanos evalúen el potencial impacto de estos riesgos en sus decisiones estratégicas.

Además de las implicaciones legales, se subrayó la necesidad de ofrecer oportunidades de formación continua a los empleados senior, promoviendo la transferencia de conocimiento y mentorías entre generaciones. Esta medida, explicaron los expertos, no solo ayuda a reducir el riesgo de pérdida de talento experimentado, sino que también favorece una cultura organizacional inclusiva y colaborativa.

Finalmente, los panelistas instaron a las organizaciones a desarrollar metodologías de gestión de riesgos que incluyan fases de diagnóstico, control, financiación y administración, y a establecer códigos de buenas prácticas y ética para abordar el edadismo. «La colaboración intergeneracional no solo es posible, sino que es esencial para construir organizaciones resilientes y socialmente responsables», concluyeron los expertos en un llamado a potenciar el diálogo y la convivencia en el entorno laboral.

ACCEDA  
AL VÍDEO  
DE LA  
ENTREVISTAS



ACCEDA AL VÍDEO COMPLETO DEL WEBINAR



100

# Nuevas Guías sobre Ciberseguridad e Inteligencia Artificial



LA ASOCIACIÓN  
28/11/2024

AGERS PRESENTÓ EL 28 DE NOVIEMBRE DOS NUEVAS GUÍAS CLAVE PARA EL SECTOR EN LA SEDE DE UNESPA, A QUIEN AGRADECEMOS LA ACOGIDA PARA TODOS LOS ASISTENTES PRESENCIALES Y VIRTUALES: LA «GUÍA DE CASOS PRÁCTICOS DE SINIESTROS CIBERNÉTICOS» Y LA «GUÍA SOBRE LA GESTIÓN DEL RIESGO EN LA INTELIGENCIA ARTIFICIAL». LA CITA ATRAJO A PROFESIONALES DEL SECTOR ASEGURADOR Y DE RIESGOS, INTERESADOS EN LAS ÚLTIMAS ESTRATEGIAS PARA MITIGAR AMENAZAS

ACCEDA A LA PRESENTACIÓN COMPLETA PINCHANDO AQUÍ



La primera mesa redonda de la jornada estuvo conformada por Manuel Pérez Martín de la Hinojosa, Head of Cyber, Southern Europe and LatAm HOWDEN, Carmen Segovia Blázquez, Director FINEX y Ciber riesgos en Willis Towers Watson, Belén Medina Vazquez, Insurance Manager de GLOBALVIA, Juan Manuel Gayá Soler, Director de Gerencia de Riesgos en El Corte Inglés e Iñaki Reclusa, Head of Risks en Sanitas.



Los expertos destacaron la importancia de incorporar ciberseguridad en los planes de continuidad de negocio, enfatizando que los riesgos tecnológicos son también riesgos empresariales. Se abordaron lecciones aprendidas de siniestros recientes y la necesidad de estar alineados con los consejos de administración. Además, se puso en práctica un caso de «ransomware» y cómo los avances en inteligencia artificial pueden ser tanto una amenaza como una herramienta para fortalecer la seguridad. La Guía Cyber incluye casos prácticos y recomendaciones para prevenir incidentes o gestionar eficazmente su impacto.



Por otra parte, en la presentación sobre inteligencia artificial intervinieron: Jesus Jimeno, Abogado de DGS Abogados, Irantxe De Anda, Delegada de Protección de Datos y Directora de Cumplimiento en Grupo EYSA, Nelia Argaz, Cyber Security & Business Resilience Leader for Continental Europe en Marsh y Rafael Anson, Socio y Profesor en Bufete Mas y Calvet , quienes incidieron en el marco jurídico y los riesgos asociados al uso de estas tecnologías en las organizaciones. Analizaron cómo establecer una gobernanza sólida y ética en su implementación, con un enfoque preventivo que equilibre innovación y responsabilidad. Se-

gún los ponentes, las empresas deben anticipar los riesgos y adaptar sus estrategias para aprovechar de forma segura las ventajas de la IA.

El evento ha concluido con un café-networking que permitió a los asistentes intercambiar impresiones sobre los contenidos presentados. AGERS reafirma con esta iniciativa su compromiso con la formación y divulgación de mejores prácticas en la gestión de riesgos, consolidándose como un referente en el sector.

En los próximos días incluiremos más contenido en nuestros canales de Youtube y más imágenes en flickr y redes sociales, síguenos para estar atento a ellas.

# GUÍA CYBER CASOS PRÁCTICOS DE SINIESTROS CIBERNÉTICOS

SU GESTIÓN Y LA PARTICIPACIÓN  
DEL SEGURO

PINCHA AQUÍ 

## MIEMBROS COMISIÓN RIESGOS TECNOLÓGICOS:

**Juan Gayá** (El Corte Inglés) – Coordinador  
**África Sánchez** (El Corte Inglés)  
**Belén Medina** (Globalvia)  
**Eva Pérez** (Duro Felguera)  
**Álvaro González** (Aena)  
**Juan Miguel García y David Martínez** (Cepsa)  
**Ignacio Reclusa** (Sanitas)  
**Ana Ruiz** (Noatum)  
**Juan Ramón Claver** (Abertis)  
**Esther López** (Esteve Pharmaceuticals)  
**Pedro Morato** (Transfesa)  
**Raquel Caballero** (Mango)

## EXPERTOS COLABORADORES

**Veronica Jimenez Romero**,  
Director Specialty Cyber Insurance  
AON

**Carlos Bereciartua Gonzalez**,  
Director Cyber Consulting AON  
Spain

**Erick Guillermo Erazo**, Cyber  
Security Consultant AON

**Eloy Gonzalez**, Financial Lines  
Claims Team Leader and CE Cyber  
Claims Hub Leader at Chubb  
Martin Souto Sales Director Dar-  
kData

**Manuel Huerta de la Morena**,  
CEO de Lazarus Technology, S.L.

**Juan Manuel Martínez Álcala**,  
CTO de Lazarus Technology, S.L.

**Manuel Pérez Martín de la Hi-  
nojosa**, Head of Cyber, Southern  
Europe & LatAm Howden Group  
Carmen Segovia Director FINEX y  
Ciber riesgos WTW





# GUÍA LEGAL RISK LAB

## GESTIÓN DEL RIESGO DE LA INTELIGENCIA ARTIFICIAL

[PINCHA AQUÍ](#)



### MIEMBROS COMISIÓN RIESGOS TECNOLÓGICOS:

#### Coordinador

**Jesús Jimeno Muñoz** (*Legal Risk Lab*)  
**Rafael Anson Peironcely** (*Bufete Mas y Calvet*)  
**Sonia Lecina López** (*SEPBLAC*)  
**Elvira Torres** (*S22 Digital*)  
**Alfredo Zorzo Losada** (*One eSecurity*)  
**Alberto Muñoz Villareal** (*Muñoz Arribas Abogados*)  
**Jorge Martínez Ramallo** (*MIG-WELLHUMAN*)  
**Ignacio Reclusa Etayo** (*Sanitas*)  
**Edgar García Corominas** (*Amazon*)  
**Iratxe de Anda Rodríguez**  
**Eva Pérez Pastor** (*Duro Felguera*)  
**Lorena Jurado Jabonero** (*Calidad Pascual*)  
**Almudena Benito** (*WTW*)  
**Eva M<sup>a</sup> Fandiño Vázquez** (*Enagas*)  
**Nelia Argaz Durango** (*Marsh*)

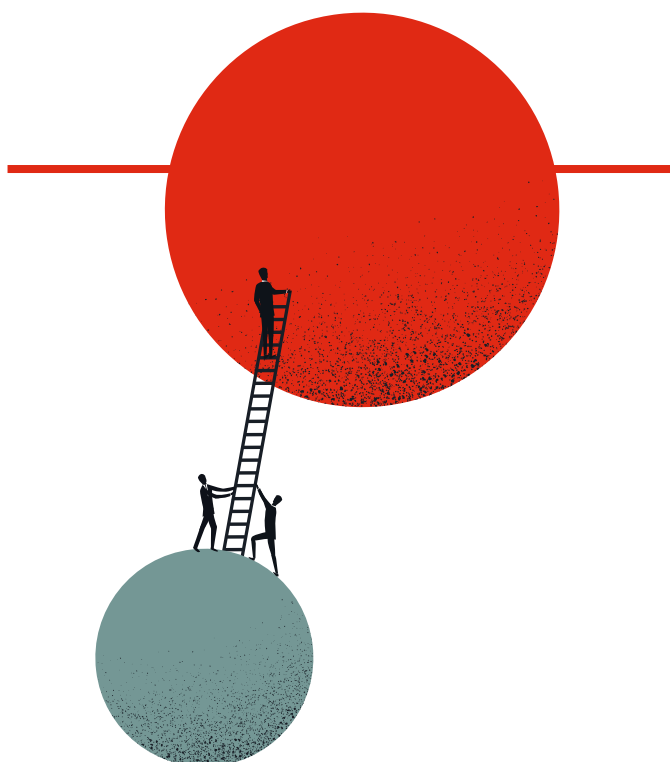
### EXPERTOS COLABORADORES

**Juan Carlos Martínez**, *Director de Datos e IA en AON Iberia*  
**Adrián Feliu**, *Inteligencia Artificial y Ciberseguridad Howden*  
**Juan Manuel Quintana**, *Inteligencia Artificial y Ciberseguridad Howden*  
**Víctor Javier Ramos**, *IP CTO en Huawei*  
**Fernando Ariza**, *Director General Adjunto en Mutualidad de la Abogacía*  
**Fabian Vidal**, *CISO Sanitas*

**104**

**Julio - Diciembre 2024**

# NUEVOS Asociados AGERS 2024



**EBSCO**

 **innovaibérica**

 **IRISGLOBAL**

 **OHLA**  
Progress Enablers

 **Profand**

**renfe**

 **ULMA**

 **VidaCaixa**

**Wesolowski**  
ABOGADOS

# #TODOAGERS EN SPOTIFY



Más de 3.5k escuchas y muchos podcasts para descubrir



agers



# Colaboradores 2024

## Platinum

COLIN VEGA FLETES  
ABOGADOS



 **MAPFRE**



## Golden

grupo  addvalora



Allianz 



**AON**



**beazley**

**BHSI**  
BERKSHIRE HATHAWAY SPECIALTY INSURANCE

**CHUBB®**

CLYDE & CO



**DAC BEACHCROFT**

**everest™**



**HDI**

**HOWDEN**

**innovaibérica**

**Marsh**

**Munich RE**

 **QBE**



 sedgwick®



 **Swiss Re**  
Corporate Solutions

**wtw**

 **ZURICH®**

## Silver

**FBA socios**  
SERVICIOS DE PERITACION ESPECIALIZADA

**HIGH DOME**  
PCC

**HASA**  
Insurance & Reinsurance Broker



 **Liberty**  
Specialty Markets



**RSA**



# AGERS en Instagram

Talento joven,  
¡Este es tu lugar!



¡Síguenos!

@agers.asociacion





# RECORRE EL CAMINO CON NOSOTROS



agers

WWW.AGERS.ES - @AGERS\_ - #TodoAGERS  
AGERS · Asociación Española de Gerencia de Riesgos y Seguros