# CIBERRIESGO UN SOLO EMAIL, 6,9 MILLONES DE AFECTADOS... Y UNA DEMANDA COLECTIVA CADA VEZ MÁS PREVISIBLE

## QUÉ ENSEÑA EL CASO ASSURANCEAMERICA SOBRE CIBERRIESGO, violaciones masivas de seguridad de datos y acciones colectivas



*El reciente incidente sufrido por AssuranceAmerica en Estados Unidos confirma una tendencia que muchas empresas todavía infravaloran: una violación de seguridad de los datos ya no es solo un incidente tecnológico, sino un evento capaz de activar costes de respuesta, litigación masiva, deterioro reputacional y revisión crítica del programa asegurador. El caso resulta especialmente útil para el mercado español porque anticipa un escenario en el que las reclamaciones colectivas por exposición de datos personales serán cada vez más relevantes.*

| 6,9 M | 1.822 | 4,44 M $ |
|---|---|---|
| afectados estimados | class actions en 2025 | coste medio del incidente |

## El incidente de AssuranceAmerica

AssuranceAmerica, una managing general agency con sede en Atlanta, opera productos de auto no estándar, renters y commercial auto a través de una red de aproximadamente 9.500 agentes en 14 estados. Esa estructura amplifica el alcance potencial de cualquier incidente producido a nivel de plataforma, ya que la información afectada no se limita a una sola entidad, sino que puede proyectarse sobre toda la red comercial y de clientes conectada al sistema.

Según la información divulgada, la compañía **detectó actividad sospechosa el 17 de marzo de 2026 y la vinculó a un ataque dirigido contra un empleado el día anterior, un patrón coherente con técnicas de phishing orientadas al robo de credenciales**. Lo más significativo no es solo el vector de entrada, sino la dimensión del impacto: el número estimado de afectados pasó de unas 611.000 personas, inicialmente identificadas en una notificación estatal, a aproximadamente 6,9 millones de personas en el alcance posteriormente estimado.

Los datos potencialmente expuestos incluirían nombres, datos de contacto, información de pólizas y cuentas, datos de conductores y vehículos, información relacionada con siniestros,
números de permiso de conducir, Tax ID y números de la Seguridad Social. Cuando el incidente afecta a este tipo de datos y a esta escala, la exposición jurídica y financiera se multiplica de forma inmediata.

## Del incidente técnico al pleito masivo

La relevancia estratégica del caso está en la reacción jurídica casi instantánea. **Tras conocerse la violación de seguridad, distintos despachos comenzaron investigaciones dirigidas a valorar posibles demandas colectivas en representación de los afectados**, lo que confirma que, en Estados Unidos, este tipo de respuesta se ha normalizado cuando existe una filtración masiva de datos personales sensibles.

La revisión Data Breach & Privacy Class Action Review 2026, de Duane Morris, sitúa en aproximadamente 1.822 el número de acciones colectivas presentadas en 2025 en materia de privacidad de datos, con una media superior a 150 nuevas demandas al mes. El mismo análisis destaca que más del 68 % de las mociones de certificación de clase resueltas en 2025 fueron estimadas por los tribunales, un dato que explica por qué la litigación colectiva se ha convertido en una consecuencia crecientemente previsible de este tipo de incidentes.

**Desde la óptica aseguradora, esto obliga a revisar la forma en que se valora el siniestro. El coste ya no reside únicamente en el análisis forense, la contención, la notificación o la restauración operativa; incorpora, además, defensa jurídica, acuerdos, monitorización de crédito, gestión de crisis y responsabilidad agregada frente a terceros.**

*Frases importantes o para resaltar una idea, se pueden poner así*

## Evolución de las demandas colectivas

La evolución reciente de las class actions de privacidad de datos en Estados Unidos es especialmente ilustrativa, porque muestra cómo el componente litigioso se ha consolidado como una capa estable y creciente del coste total del ciberriesgo.

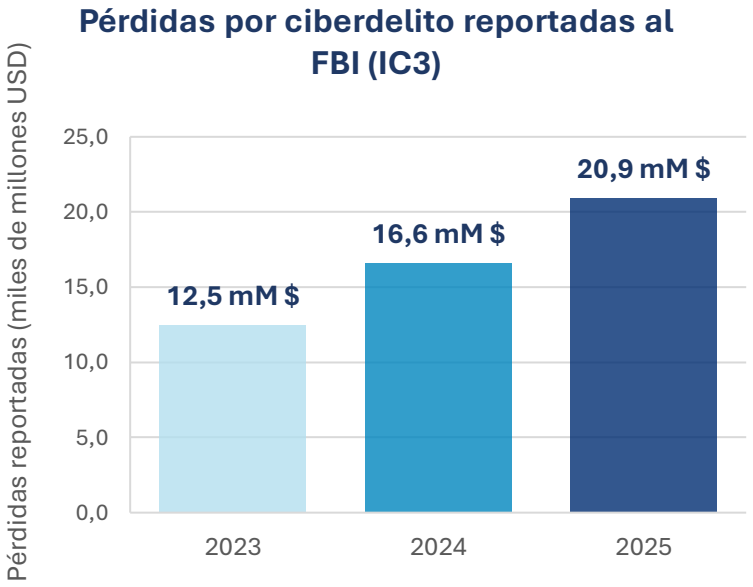



*Gráfico 2. Pérdidas por ciberdelito reportadas al FBI IC3. Fuente: FBI Internet Crime Report 2025.*

### Evolución de las demandas colectivas en privacidad de datos (EE. UU.)

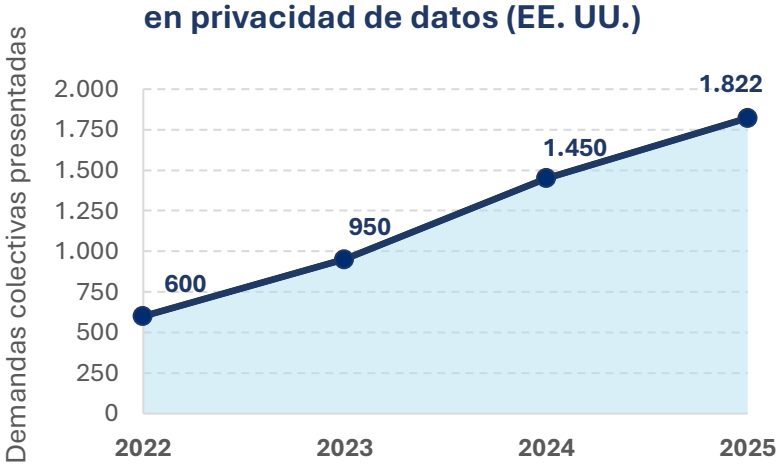



*Gráfico 1. Evolución de las demandas colectivas en privacidad de datos en EE. UU. Fuente: Duane Morris.*

## El phishing sigue dominando

El caso AssuranceAmerica tiene otra lectura esencial: **el origen del incidente no fue una técnica exótica ni una explotación sofisticada de infraestructura crítica, sino un ataque dirigido a una persona concreta mediante correo electrónico**. Ese detalle desmonta uno de los errores más habituales en muchas organizaciones: pensar que el ciberriesgo afecta sobre todo a grandes compañías tecnológicas o a objetivos geopolíticamente relevantes.

En realidad, **cuanto más común es el vector de ataque, mayor es la probabilidad de que cualquier organización resulte afectada**. Empresas medianas, corredores, mediadores, despachos profesionales, MGAs, proveedores de servicios y aseguradoras comparten una misma fragilidad: el factor humano y la dependencia operativa del correo electrónico y de las credenciales internas.

*Cuanto más común es el vector de ataque, mayor es la probabilidad de que cualquier organización resulte afectada*

## La dimensión económica del riesgo

La presión financiera del ciberdelito sigue creciendo a escala agregada. Las publicaciones que recogen el Internet Crime Report 2025 del FBI sitúan las pérdidas reportadas en casi 21.000 millones de dólares durante 2025, confirmando un nuevo máximo y reforzando la idea de que el fenómeno ya debe tratarse como un riesgo sistémico y no como una sucesión de eventos aislados.

A esa visión macro se añade el coste medio de una filtración individual. El informe Cost of a Data Breach 2025 de IBM sitúa el coste medio global en aproximadamente 4,44 millones de dólares, una cifra suficientemente elevada por sí misma, pero todavía incompleta si no se añade el componente de litigación, reputación y responsabilidad frente a terceros.

## España y las acciones colectivas

La lección para España no consiste en extrapolar mecánicamente el sistema procesal estadounidense, pero sí en asumir que la lógica del riesgo avanza en una dirección parecida: mayor sensibilidad regulatoria, mayor protección del afectado, mayor capacidad de agregación de reclamaciones y un mayor escrutinio sobre el tratamiento de datos personales.

En este contexto, **una violación de seguridad relevante no compromete únicamente la seguridad de la información, sino también el gobierno corporativo, la diligencia del órgano de administración, la suficiencia del marco de compliance y la adecuación del programa asegurador**.

### Coste medio global de una violación de seguridad de datos

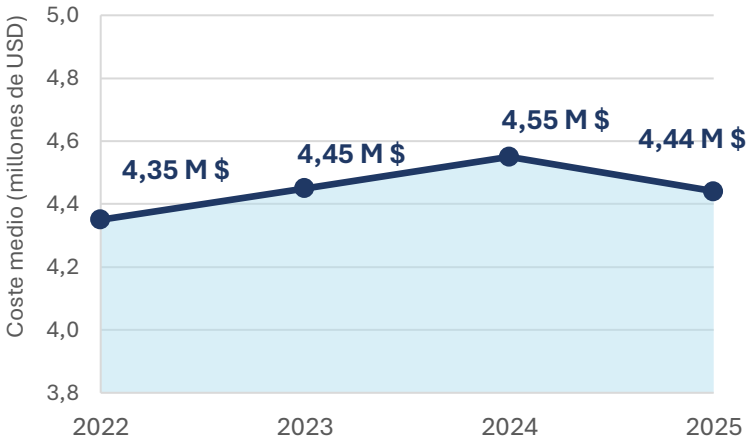



*Gráfico 3. Coste medio global de una violación de seguridad de datos. Fuente: IBM Cost of a Data Breach Report 2025.*

*La pregunta correcta ya no es si existe una póliza, sino si la estructura de cobertura es realmente suficiente.*

**La pregunta correcta ya no es si existe una póliza, sino si la estructura de cobertura es realmente suficiente** en cuanto a límites, alcance, servicios de respuesta y coordinación con otras líneas, como RC o D&O.

## Mensaje para el mercado

Para muchas empresas que aún consideran el ciberriesgo como una cobertura secundaria o prescindible, el caso envía una señal inequívoca: **un solo correo fraudulento puede desembocar en una fuga masiva de datos, un proceso de notificación a millones de afectados, investigaciones regulatorias, exposición reputacional y reclamaciones colectivas de gran escala.**

## Indicadores clave

| Indicador | Dato relevante |
|---|---|
| ➢ Personas afectadas estimadas (caso AssuranceAmerica) | **6,9 millones** |
| ➢ Demandas colectivas de privacidad de datos en EE. UU. (2025) | **1.822 acciones** |
| ➢ Tasa de certificación de clase estimada (2025) | **> 68 % de las mociones resueltas** |
| ➢ Pérdidas por ciberdelito reportadas al FBI (2025) | **20.900 M $** |
| ➢ Coste medio global de una violación de seguridad de datos | **4,44 M $** |

Por eso, **el ciberriesgo debe dejar de tratarse como una garantía complementaria reservada a grandes grupos tecnológicos**. Hoy forma parte del mapa central de riesgos de cualquier organización que custodie datos personales, opere con redes comerciales amplias o dependa críticamente del correo electrónico, de los accesos remotos y de los sistemas internos compartidos.

**Casimiro Rey**

*Director de Empresas y Negocio Internacional*
*Miembro del Comité de Dirección*
*Grupo Galilea S.L. (Söderberg & Partners)*