

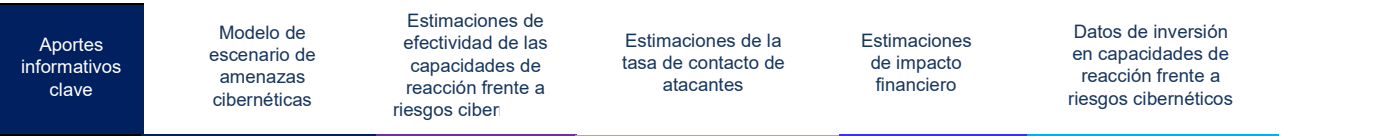


# Cyber Risk Insights [Perspectivas sobre Riesgos Cibernéticos] (CRI)

Un producto líder en el mercado para ayudarlos a tomar mejores decisiones sobre riesgos cibernéticos

## ¿Qué son los Cyber Risk Insights de KPMG (CRI)?

CRI es un producto SaaS licenciable que adopta un enfoque basado en escenarios para evaluar con mayor precisión la probabilidad y el impacto de los ciberataques. Utiliza cuadros de mando potentes e intuitivos para mostrar la información, con una sólida interfaz de usuario.



**Ejemplos de Insight**

### Priorizar los riesgos cibernéticos

CYBER SCENARIO RISK EXPOSURE

As of Sept 2023, our greatest risk exposure is from a Widespread ransomware scenario

- Widespread Ransomware: £4.6M ↑ Average ALE
- Business Email Compromise: £1.4M ↓ Average ALE
- Third Party Compromise: £1.2M ↓ Average ALE

LOSS EXCEEDANCE CURVE

75% probability of a £5M loss

40% probability of a £1M loss

### Optimizar inversión en ciberseguridad

MARCH 2023 LOSS EXPOSURES

September 2023 ALE

10th Percentile: £10M  
5th Percentile: £1.2M

Average: £20M  
Most likely ESM

90th Percentile: £30M  
95th Percentile: £2.1M

MARCH 2024 LOSS EXPOSURES

September 2024 ALE

10th Percentile: £5M  
5th Percentile: £0.12M

Average: £8M  
Most likely ESM

90th Percentile: £25M  
95th Percentile: £2.1M

CAPABILITIES	COST	CONTRIBUTION TO ALE* REDUCTION	COST/BENEFIT RATIO
Network segmentation	£550,000	£2,000,000	4.4
Incident response	£350,000	£1,000,000	2.9
Strong authentication	£475,000	£3,000,000	6.3
Anti-virus detection	£325,000	£4,000,000	12.3
Configuration management	£400,000	£2,000,000	5
<b>Total:</b>	<b>£2M</b>	<b>£12M</b>	

### Solucionar los puntos débiles de las defensas

What is the likelihood of attacker success?

Attack Vector	Initial Success	Initial Failure	Subsequent Success	Subsequent Failure
Phishing	50%	50%	20%	80%
Malware	20%	80%	10%	90%
Insider	10%	90%	5%	95%

Where do we need to invest from where we are today?

## ¿Por qué usar los Cyber Risk Insights de KPMG (CRI)?

CRI les ofrece una visión completa de las posibles pérdidas financieras en caso de ciberataque, así como de las inversiones más rentables para ayudar a mitigar esos ataques. Esto les permite tomar decisiones defendibles y basadas en datos, y puede ayudarlos a priorizar sus esfuerzos de corrección. A continuación se exponen las preguntas típicas a las que CRI ayuda a dar respuesta.

<ul style="list-style-type: none"> <li>Priorizar los riesgos cibernéticos</li> <li>Optimizar inversión en ciberseguridad</li> <li>Mejorar la comunicación</li> <li>Cumplir con la normativa</li> </ul>	<p><b>Autoridades   Directorio   CEO   CFO   COO   CIO   CRO   CISO   Negocio</b></p> <p>¿Cuál es nuestra verdadera exposición al riesgo de ciberataque (probabilidad en un año e impacto financiero potencial)? ¿Está dentro de nuestro apetito de riesgo? ¿Qué riesgos cibernéticos debemos priorizar?</p>
	<p><b>Directorio   CEO   CFO   COO   CIO   CISO   Negocio</b></p> <p>¿Qué inversiones cibernéticas reducirían el riesgo brindando una mejor relación costo/resultado? Si invertimos en XM en ciberseguridad el año que viene, ¿sería demasiado o muy poco?</p>
	<p><b>Directorio   CEO   COO   CIO   CRO   CISO   Negocio</b></p> <p>Sabemos que los cibernéticos son riesgos complejos con muchas interdependencias: ¿cómo podemos explicar de forma sencilla nuestra exposición global para tomar decisiones eficaces y bien informadas?</p>
	<p><b>Regulador   Directorio   CEO   CRO   CISO</b></p> <p>¿Cómo podemos determinar el impacto material potencial de un ataque cibernético contra mi negocio? ¿Cómo podemos comunicar el riesgo cibernético al Directorio para satisfacer los nuevos requerimientos de información sobre riesgos cibernéticos?</p>

# ¿Cómo ha ayudado CRI a nuestros clientes?

CRI ha ayudado a organizaciones de una amplia gama de sectores.

## Confianza del Directorio y reducción de riesgos **Venta al por menor**

Un compromiso histórico para alinearse con ISO27001 dio lugar a que la organización intentara arreglarlo todo, muy por encima de su capacidad de cambio. CRI permitió:

- ✓ La eliminación del 20% del alcance de los controles de ISO27001 en función del modelado de amenazas y la capacidad de simulación "Y si..." de CRI.
- ✓ Ahorro de costos de más de 500.000 libras esterlinas, al tiempo que permite tomar decisiones de priorización defendibles.
- ✓ Medición continua de la exposición al riesgo cibernético a lo largo del tiempo.

## Priorización de una hoja de ruta cibernética **Seguros**

Un CISO estaba siendo cuestionado por el Directorio sobre los beneficios del programa de inversión cibernética y se le pidió que redujera el gasto. CRI permitió:

- ✓ Identificación de los controles prioritarios para la inversión sobre la base de un sólido análisis de costos y beneficios.
- ✓ Reducción anual demostrable de la exposición al riesgo cibernético vinculada al seguimiento de los beneficios de las iniciativas de cambio.
- ✓ Evaluaciones detalladas de las unidades de negocio individuales tras la evaluación de todo el Grupo.

## Justificación de la inversión en **petróleo y gas**

Se necesitaba un caso empresarial para justificar la inversión en una costosa herramienta de detección de amenazas de tecnología operativa. CRI permitió:

- ✓ Un análisis costo-beneficio de la reducción estimada de la exposición a pérdidas cibernéticas debidas a la implantación de la herramienta.
- ✓ La preparación de un caso de negocio para el Director Financiero basado en un análisis cuantitativo.
- ✓ La toma de una decisión de inversión sólida.

## Gestión de la exposición en una cartera de capital riesgo

Se requirieron evaluaciones de riesgos cibernéticos y planes de corrección en más de 20 empresas de cartera. CRI permitió:

- ✓ Que cada sociedad de cartera comprenda su exposición al riesgo cibernético en términos financieros.
- ✓ Que cada empresa de la cartera priorice sus inversiones cibernéticas en función de las amenazas específicas para su negocio.
- ✓ La sustitución de su metodología de evaluación de madurez 1-5, dando a los líderes mayor confianza en la seguridad de su cartera.

Algunos o todos los servicios aquí descritos pueden no estar permitidos para los clientes de auditoría de KPMG y sus filiales o entidades relacionadas.

[home.kpmg/uk/en/CRI](https://home.kpmg/uk/en/CRI)

La información presentada en este documento es de naturaleza general y no tiene por finalidad abordar las circunstancias de ninguna persona o entidad en particular. Aunque procuramos brindar información precisa y oportuna, no es posible garantizar que dicha información lo sea en el momento en que se recibe o siga siéndolo en el futuro. No se deben tomar medidas en base a dicha información sin el debido asesoramiento profesional después de un estudio detallado de la situación en particular.

© 2023 KPMG, una sociedad argentina y firma miembro de la red de firmas miembro independientes de KPMG afiliadas a KPMG International Limited, una entidad privada inglesa limitada por garantía que no presta servicios a clientes. Derechos reservados.

KPMG se refiere a la organización global o a una o más de las firmas miembro de KPMG International Limited ("KPMG International"), cada una de las cuales constituye una entidad legal separada. KPMG International Limited es una compañía inglesa de capitales privados, limitada por garantía y no presta servicios a clientes. Para más información sobre nuestra estructura, visite [home.kpmg/governance](https://home.kpmg/governance).

# ¿Cómo los puede ayudar CRI?

CRI los dota de las herramientas necesarias para:

A los fines de este documento, "nosotros", "KPMG", "nos" y "nuestro" se refieren a la organización global o a una o más de las firmas miembro de KPMG International Limited ("KPMG International"), cada una de las cuales constituye una entidad legal separada.

### Presentar el caso ante el Directorio

El enfoque lógico y transparente de CRI los ayuda a comunicar el riesgo cibernético a las partes interesadas de alto nivel, demostrar los beneficios empresariales de las capacidades cibernéticas y presentar casos de inversión convincentes.



### Realizar evaluaciones sistemáticas, coherentes y basadas en datos

CRI agiliza y simplifica la adopción de técnicas cuantitativas y mejora la objetividad de las evaluaciones de riesgos al producir resultados coherentes y basados en datos.

### Cuantificar la probabilidad y el impacto

Accedan a nuestros modelos probados y contrastados, que cuantifican la probabilidad de que se produzcan escenarios de ciberriesgo, la posibilidad de que los atacantes tengan éxito a través de las capas de defensa y las pérdidas financieras potenciales.



### Apuntar a la inversión para reducir la exposición

Los modelos gráficos de escenarios de riesgo les permiten ver dónde contribuyen sus capacidades cibernéticas a la reducción del riesgo en todos los niveles de defensa y qué áreas se beneficiarían más de la inversión.



### Ayudar a optimizar las inversiones

Determinamos la cartera óptima de inversiones en ciber capacidades, para ayudarlos a conseguir un gran rendimiento de la inversión en reducción de riesgos.



### Probar las inversiones

Estimamos el periodo de amortización de una inversión o cartera de inversiones, basándonos en un análisis costo-beneficio del gasto comparado con la reducción esperada de las pérdidas cibernéticas.

Comuníquense con nosotros para hablar de las necesidades de su organización o para concertar una demostración de nuestro producto Cyber Risk Insights.

## Contáctenos:

**Martin Tyley**  
Socio Líder Global  
[Martin.Tyley@kpmg.co.uk](mailto:Martin.Tyley@kpmg.co.uk)

**James Hanbury**  
Socio Líder Global  
[James.Hanbury@kpmg.co.uk](mailto:James.Hanbury@kpmg.co.uk)

**Jack Whitaker**  
Líder de Producto Global  
[Jack.Whitaker@kpmg.co.uk](mailto:Jack.Whitaker@kpmg.co.uk)