

# Cyber Risk Insights

Un producto líder de mercado que ayuda a tomar mejores decisiones sobre los riesgos en ciberseguridad

## ¿Qué es KPMG Cyber Risk Insights (CRI)?

CRI es un producto SaaS que adopta un enfoque basado en escenarios para evaluar con mayor precisión la probabilidad y el impacto de los ciberataques. Utiliza cuadros de mando y ofrece métricas potentes e intuitivas para definir modelos basados en la cuantificación del riesgo.

Inputs clave

Modelado de escenarios de ciber amenazas

Estimaciones de la efectividad de ciber capacidades

Estimaciones de "contact rates" de ataques

Estimaciones de impacto financiero

Datos de inversiones de ciberseguridad

### Priorización de riesgos de ciber

### Optimizar el gasto de ciber

CAPABILITIES	COST	CONTRIBUTION TO ALE REDUCTION	COST-BENEFIT RATIO
Network segmentation	£450,000	£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>	

### Corregir debilidades en las medidas de protección

### Identificar mejoras óptimas futuras

## ¿Por qué usar la herramienta KPMG CRI?

CRI brinda una visión integral de las posibles pérdidas financieras en caso de un ataque en ciberseguridad, así como las mejores inversiones para ayudar a mitigar esos ataques. Esto permite tomar decisiones defendibles y basadas en datos ayudando a priorizar los esfuerzos de remediación. Las preguntas típicas que CRI ayuda a responder se encuentran a continuación:

Priorizar riesgos	<div style="display: flex; justify-content: space-between; border-bottom: 1px solid #ccc; margin-bottom: 5px;"> <span style="background-color: #003366; color: white; padding: 2px 5px;">Regulador</span> <span style="background-color: #003366; color: white; padding: 2px 5px;">Dirección</span> <span style="background-color: #003366; color: white; padding: 2px 5px;">CEO</span> <span style="background-color: #003366; color: white; padding: 2px 5px;">CFO</span> <span style="background-color: #003366; color: white; padding: 2px 5px;">COO</span> <span style="background-color: #003366; color: white; padding: 2px 5px;">CIO</span> <span style="background-color: #003366; color: white; padding: 2px 5px;">CRO</span> <span style="background-color: #003366; color: white; padding: 2px 5px;">CISO</span> <span style="background-color: #003366; color: white; padding: 2px 5px;">Negocio</span> </div> <p>¿Cuál es la exposición al riesgo (probabilidad en un año e impacto financiero potencial de sufrir un ciberataque)? ¿Está dentro de nuestro apetito de riesgo? ¿Qué riesgos ciber de deberían priorizar?</p>
Optimizar el gasto ciber	<div style="display: flex; justify-content: space-between; border-bottom: 1px solid #ccc; margin-bottom: 5px;"> <span style="background-color: #003366; color: white; padding: 2px 5px;">Dirección</span> <span style="background-color: #003366; color: white; padding: 2px 5px;">CEO</span> <span style="background-color: #003366; color: white; padding: 2px 5px;">CFO</span> <span style="background-color: #003366; color: white; padding: 2px 5px;">COO</span> <span style="background-color: #003366; color: white; padding: 2px 5px;">CIO</span> <span style="background-color: #003366; color: white; padding: 2px 5px;">CISO</span> <span style="background-color: #003366; color: white; padding: 2px 5px;">Negocio</span> </div> <p>¿Qué inversiones ciber ofrecerían la mejor reducción del riesgo? Si se invierten X millones en ciber el próximo año, ¿qué beneficio aportará a la empresa?</p>
Mejorar la comunicación	<div style="display: flex; justify-content: space-between; border-bottom: 1px solid #ccc; margin-bottom: 5px;"> <span style="background-color: #003366; color: white; padding: 2px 5px;">Dirección</span> <span style="background-color: #003366; color: white; padding: 2px 5px;">CEO</span> <span style="background-color: #003366; color: white; padding: 2px 5px;">COO</span> <span style="background-color: #003366; color: white; padding: 2px 5px;">CIO</span> <span style="background-color: #003366; color: white; padding: 2px 5px;">CRO</span> <span style="background-color: #003366; color: white; padding: 2px 5px;">CISO</span> <span style="background-color: #003366; color: white; padding: 2px 5px;">Negocio</span> </div> <p>Teniendo en cuenta que en ciber se pueden detectar diferentes tipologías de riesgos, con muchas interdependencias: ¿cómo se puede explicar la exposición global de forma sencilla?</p>
Cumplir con las regulaciones	<div style="display: flex; justify-content: space-between; border-bottom: 1px solid #ccc; margin-bottom: 5px;"> <span style="background-color: #003366; color: white; padding: 2px 5px;">Regulador</span> <span style="background-color: #003366; color: white; padding: 2px 5px;">Dirección</span> <span style="background-color: #003366; color: white; padding: 2px 5px;">CEO</span> <span style="background-color: #003366; color: white; padding: 2px 5px;">CRO</span> <span style="background-color: #003366; color: white; padding: 2px 5px;">CISO</span> </div> <p>¿Cómo se puede determinar el impacto "material" de un ciberataque en la empresa? ¿Cómo se puede comunicar el riesgo ciber a la junta directiva para cumplir con los nuevos requisitos?</p>

# ¿Cómo ha ayudado CRI a nuestros clientes?

CRI ha ayudado a organizaciones en una amplia gama de industrias.

## Confianza en la junta directiva y reducción de riesgos

Energía

Un CISO necesitaba defender ante la junta directiva la estrategia y programa de inversión ciber definidos. CRI permitió:

- ✓ Identificar los controles prioritarios para la inversión sobre la base de un sólido análisis de costes y beneficios
- ✓ Reducir anualmente la exposición al riesgo ciber. Seguimiento de los beneficios de las iniciativas
- ✓ Realizar evaluaciones y elaborar un estudio de viabilidad basado en un análisis cuantitativo

## Priorización y optimización de recursos

Seguro

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

- ✓ Reducir el 20% de los controles ISO27001 basándose en la capacidad de modelización de amenazas y simulación hipotética de CRI.
- ✓ Ahorrar más de 500k €, al tiempo que se tomaron decisiones defendibles sobre prioridades.
- ✓ Medición continua de la exposición al riesgo ciber a lo largo del tiempo

## Gestión de la exposición de la entidad

Capital Privado

Se solicitaron un conjunto de evaluaciones de riesgos en ciberseguridad y planes de acción asociados en más de 20 empresas. CRI Permitió:

- ✓ Que cada empresa comprendiera su exposición al riesgo en ciber, en términos financieros
- ✓ Que cada empresa priorizara sus inversiones en ciber en función de las amenazas específicas para su negocio
- ✓ El cambio a una metodología de evaluación de madurez (1-5), dando a los líderes de la organización una mayor confianza en la seguridad de su capital

# ¿Cómo puede ayudarte el CRI?

CRI proporciona las herramientas para:



## Presentaciones defendibles ante la junta directiva

El enfoque lógico y transparente de CRI ayuda a comunicar el riesgo de ciberseguridad ante la junta directiva, demostrando los beneficios empresariales de las capacidades ciber y presentando casos de inversión convincentes.



## Realizar evaluaciones sistemáticas, coherentes y basadas en datos

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



## Cuantificar la probabilidad y el impacto

Modelos que cuantifican de manera eficaz la probabilidad de que se produzcan situaciones de riesgo ciber así como las pérdidas financieras potenciales.



## Orientar el gasto objetivo para reducir la exposición

Los modelos gráficos que proporciona la herramienta permiten ver dónde contribuyen más las capacidades a la reducción del riesgo de ciberseguridad.



## Ayudar a optimizar las inversiones

Determinar la cartera de inversión más óptima para ayudar a alcanzar los objetivos establecidos.



## Evalúa las inversiones

Estimar el período de recuperación de una inversión o cartera de inversiones, basándose en un análisis de costo-beneficio del gasto en comparación con la reducción esperada de las pérdidas.

## Contacta con nosotros

Contáctenos para analizar las necesidades de su organización o para concertar una demostración de nuestro producto Cyber Risk Insights



**Javier Aznar**  
Socio, Technology Risk.  
Ciberseguridad y Privacidad  
[jaznar@kpmg.es](mailto:jaznar@kpmg.es)



**Juan Ignacio Ríos**  
Director, Technology Risk  
[juanignaciorios@kpmg.es](mailto:juanignaciorios@kpmg.es)



**Daniel Sánchez-C.**  
S. Manager, Technology Risk  
[danielpolo@kpmg.es](mailto:danielpolo@kpmg.es)

### Equipo desarrollo producto

**Martin Tyley**  
CRI Global Lead Partner  
[Martin.Tyley@kpmg.co.uk](mailto:Martin.Tyley@kpmg.co.uk)

**James Hanbury**  
CRI Global Lead Director  
[James.Hanbury@kpmg.co.uk](mailto:James.Hanbury@kpmg.co.uk)

**Jack Whitaker**  
CRI Global Product Lead  
[Jack.Whitaker@kpmg.co.uk](mailto:Jack.Whitaker@kpmg.co.uk)

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 aquí contenida es de carácter general y no pretende abordar las circunstancias de ningún individuo o entidad en particular. Aunque nos esforzamos por proporcionar información exacta y oportuna, no puede garantizarse que dicha información sea exacta en la fecha en que se recibe o que siga siéndolo en el futuro. Nadie debe actuar sobre la base de dicha información sin el asesoramiento profesional adecuado tras un examen exhaustivo de la situación concreta.

© 2024 KPMG Asesores S.L., sociedad española de responsabilidad limitada y firma miembro de la organización global de KPMG de firmas miembro independientes afiliadas a KPMG International Limited, sociedad inglesa limitada por garantía. Todos los derechos reservados.

KPMG hace referencia a la organización global o a una o más de las firmas miembro de KPMG International Limited ("KPMG International"), cada una de las cuales es una entidad jurídica independiente. KPMG International Limited es una sociedad inglesa privada limitada por garantía y no presta servicios a clientes. Para más información sobre nuestra estructura, visite [home.kpmg/governance](https://home.kpmg/governance).

El nombre y el logotipo de KPMG son marcas comerciales utilizadas bajo licencia por las firmas miembro independientes de la organización global KPMG.A lo largo 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 es una entidad jurídica independiente.