Clic para navegar a través del informe

Benchmark de Ciber Riesgo Cuantificado por industria en Colombia 2024

Un estudio de KPMG Colombia

Resumen Ejecutivo

Julio 2024

Clic para navegar a través del informe

Contenido

Prefacio

Buscamos a través de nuestro enfoque, que las organizaciones puedan identificar qué controles contribuyen más a la reducción de ciertas exposiciones al riesgo cibernético y asegurar que los recursos se estén enfocando en las áreas de mayor 'rendimiento por inversión'.

En KPMG, creemos firmemente en la cuantificación del riesgo cibernético. Esta cuantificación no solo ayuda a las organizaciones a entender su exposición al riesgo, sino que también proporciona una base sólida para la toma de decisiones informadas. Con nuestra metodología, demostramos que el beneficio de la cuantificación del riesgo cibernético puede, y a menudo supera, el esfuerzo requerido.

En este documento, compartimos una instantánea de los resultados de nuestro trabajo y las capacidades de KPMG en la gestión del riesgo cibernético. Creemos que la colaboración es clave para gestionar las exposiciones a la amenaza cibernética global y alentamos a todos a participar en el desarrollo de este enfoque y a compartir sus ideas y comentarios.

En KPMG, estamos comprometidos a ayudar a las organizaciones a navegar el complejo panorama de la ciberseguridad y a gestionar eficazmente sus riesgos cibernéticos.

Jaime Vásquez

Socio Líder de Advisory

Prefacio

Muchas veces, justificar el crecimiento del gasto, pasando por la contratación de especialistas difíciles de encontrar y herramientas que cada día más van a un modelo basado en servicios cuyas condiciones contractuales son novedosas y elásticas en el tiempo, es bastante difícil o casuístico en esencia.

Nuestro enfoque de servicios siempre ha tenido como base el modelo de negocios de nuestros clientes, y cómo las tecnologías de la que se disponen apoyan y/o lo soportan, somos más de la lógica biz-first que tec-first, el tiempo nos ha dado la razón.

Entender la realidad de lo que ocurre en nuestro ecosistema tecnológico desde un punto de vista cuantificable, pone piso y límites claros a las inversiones que debemos realizar para proteger las organizaciones.

Sirva el presente acercamiento al ciber riesgo cuantificado para Colombia, como aporte a nuestros empresarios que cada día se enfrentan a un panorama con altas dosis de incertidumbre. Recordemos siempre que lo que no se mide, no se puede mejorar.

Alain Almeida

Socio Advisory

Resumen Ejecutivo

Cuantificación del Ciber Riesgo

Con el creciente panorama del ciber riesgo donde cada día aumentan los ataques y las empresas impactadas, y así mismo, los directivos piden la reducción de presupuestos en las organizaciones, la cuantificación del ciber riesgo es la clave para organizar y priorizar las inversiones en ciberseguridad, y tener retornos de inversión reflejados como reducción del ciber riesgo.

CIBER RIESGO

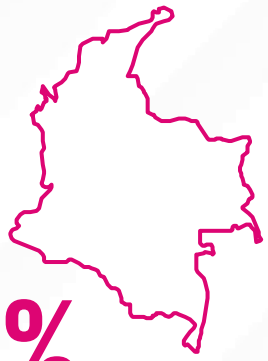
KPMG

Resumen Ejecutivo

Contextualización

83%

De ataques en LATAM los reciben otros países, acorde con el X-Force de IBM para 2024



17%

De ataques en LATAM los recibe Colombia, acorde con el X-Force de IBM para 2024

Aumento del ciber crimen y de los incidentes de ransomware

Acorde con el Microsoft Digital Defense Report 2023, Colombia ha sido uno de los países objetivo de los atacantes para para una de las 4 variantes top de ransomware.

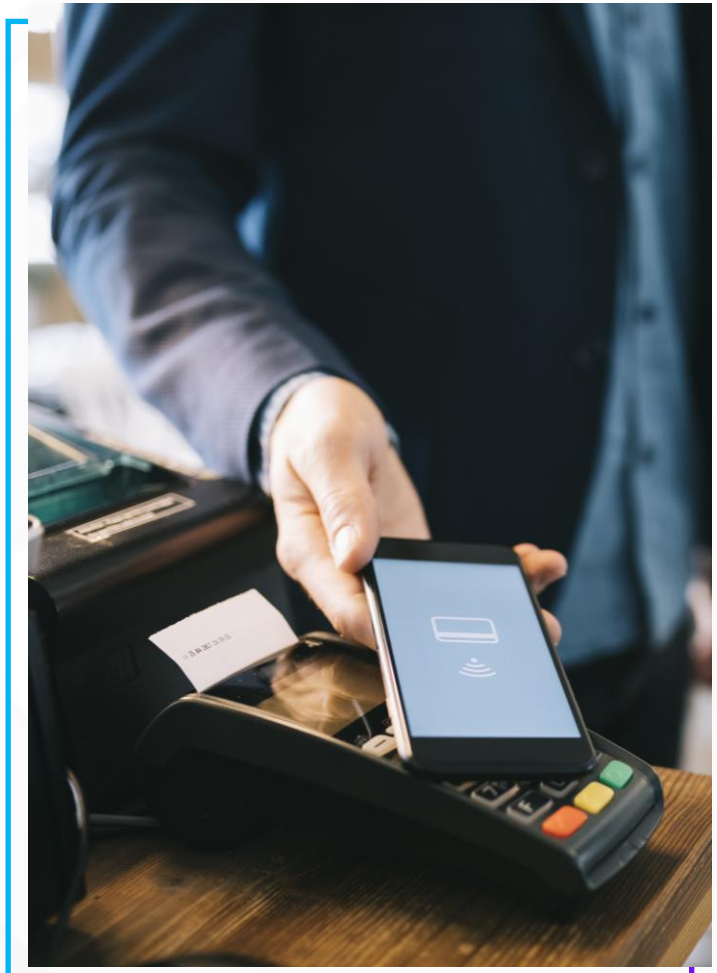
Resumen Ejecutivo

Contextualización

Impacto en datos personales

Las brechas a los datos personales siguen aumentando conforme aumentan los incidentes. Acorde con el IAPP & KPMG Privacy Study 2023

piensa que es probable que **en los siguientes 2 años un ciber ataque afecte materialmente su organización**.

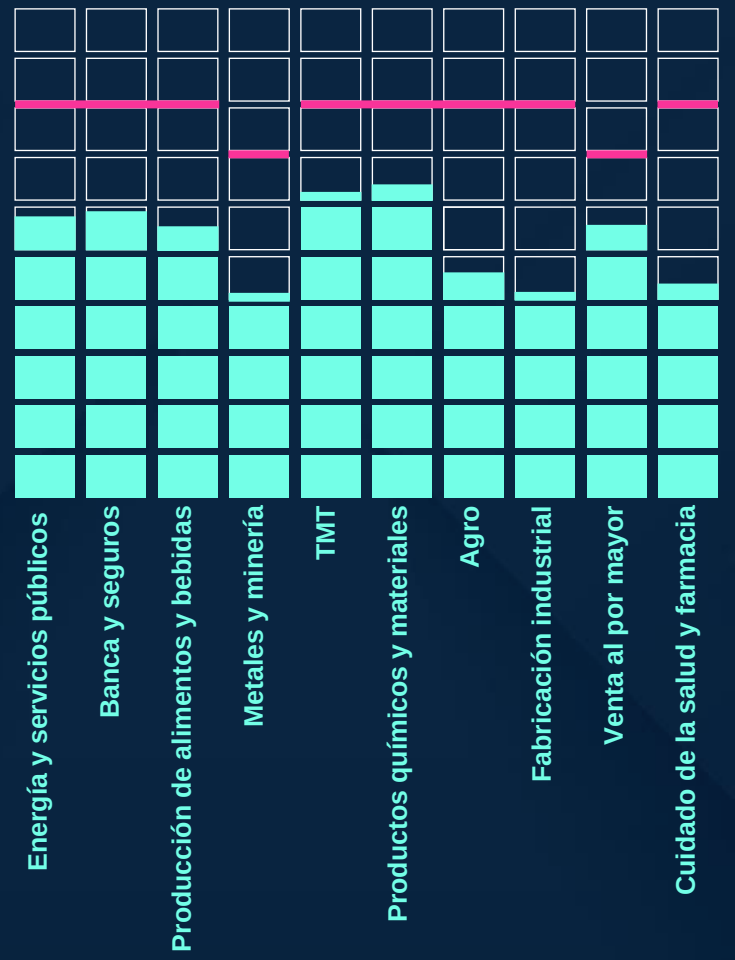


Resumen Ejecutivo

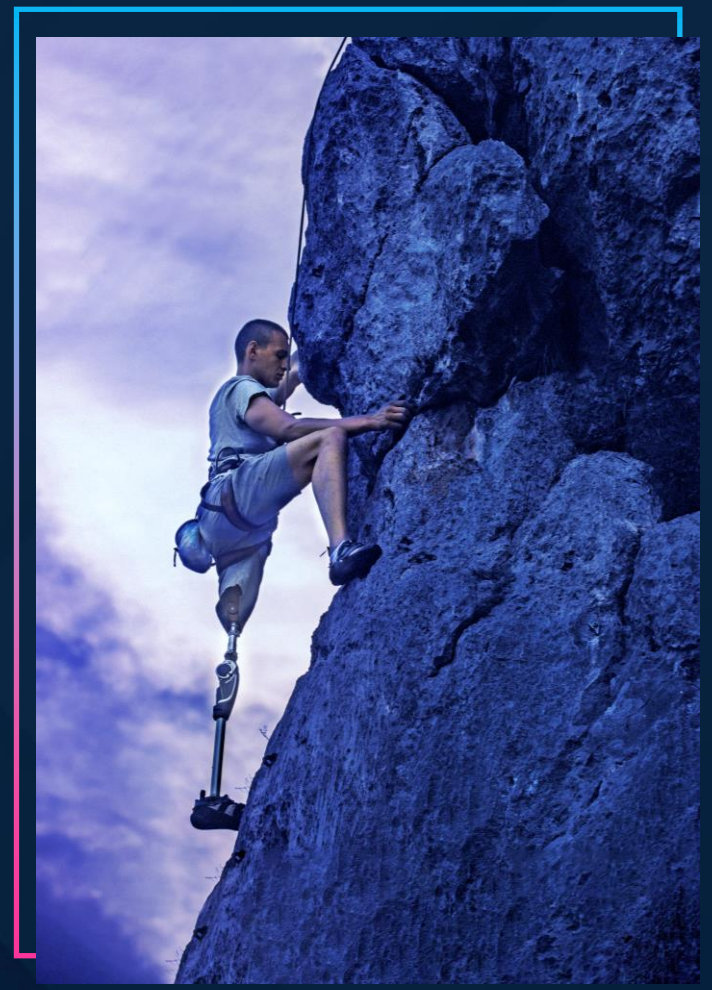
Contextualización

Madurez promedio por industria es baja, lo que incrementa el ciberriesgo.

Acorde con el **Benchmark de KPMG,** la madurez promedio de las industrias evaluadas es menor a 3.5 de 5, lo cual indica posibles ausencias de controles o debilidades en controles existentes.



Nivel mínimo recomendado por KPMG



Resumen Ejecutivo

Los enfoques y metodologías actuales para modelar y cuantificar el ciber riesgo pueden resultar confusas y difíciles de aterrizar a la realidad de las organizaciones. En los servicios que hemos prestado a nuestros clientes **en Colombia, hemos identificado que la cuantificación del ciber riesgo no es una práctica habitual en las organizaciones**, más bien la tendencia en las organizaciones actualmente es a medir su nivel de madurez y establecer metas para alcanzar un determinado nivel de madurez objetivo.

Si bien esto es muy importante hoy en día para tener un indicador sobre el estado de la ciberseguridad, la medición de un nivel de madurez por si sola, sin combinarse con la identificación y análisis de los riesgos, no aporta a la estrategia de ciberseguridad de la organización, sino que más bien estresa los presupuestos de ciberseguridad, buscando **inversiones más altas, que no siempre están justificadas y que tampoco en muchos casos pueden ser recuperadas con una disminución real y cuantificada del ciber riesgo**.

Resumen Ejecutivo

CIBERSEGURIDAD

La gestión del ciber riesgo, utilizando una metodología de gestión de riesgo cuantificado, **ayuda a los responsables de ciberseguridad, la alta dirección y la junta directiva en la toma de decisiones**, también **ayuda a comprender el verdadero nivel de exposición al ciber riesgo**, apoya el análisis sobre cómo contribuyen los controles de ciberseguridad actuales a la reducción del ciber riesgo, y así mismo, contribuye a asegurar que los recursos económicos se estén usando en las áreas que generen mayor rentabilidad (mayor reducción del ciber riesgo).

Acorde con lo que indicamos en nuestro informe de *Consideraciones de Ciberseguridad para el 2024*[(1)], **la gestión del ciber riesgo ayuda a la empresa a alinear la ciberseguridad con la resiliencia organizacional**, la cual es vital para mantener las competencias operativas de la empresa, proteger la confianza de los clientes y reducir el impacto de futuros ataques.

(1) Consideraciones de Ciberseguridad 2024 KPMG

Resumen Ejecutivo

KPMG ha desarrollado una metodología para el cálculo cuantificado del ciber riesgo, la cual tiene un enfoque basado en escenarios, y que permite evaluar con mayor precisión la probabilidad y el impacto de los ciber ataques.

Esta metodología **responde a preguntas como ¿Dónde debo invertir? ¿Cuál es el costo-beneficio de esta inversión? ¿Cuál es la exposición al riesgo de mi organización? ¿Cuáles defensas debo mejorar?**

Resumen Ejecutivo

Este primer estudio de ciber riesgo cuantificado en Colombia, el cual ha sido realizado por KPMG Colombia, permite a nuestros clientes y potenciales clientes, tener una visión general de lo que podría costarles un ciber ataque en su industria.

13.684

Compañías incluidas en el estudio

Se analizó la información de 2.022 de 10 industrias diferentes, para tener un panorama más cercano a la realidad de ciberriesgo del país.

10

¿Por qué realizar un estudio de ciber riesgo cuantificado en Colombia?

Este estudio permite a las organizaciones tener una referencia del posible impacto económico que podrían tener por un ciber ataque con un valor de referencia para su industria, y que tanto Juntas Directivas como Comités Directivos tomen conciencia y definan acciones preventivas para reducir el posible impacto.

Felipe Silgado
Director Cyber Security Services
KPMG Colombia

KPMG

Resumen Ejecutivo

¿Cómo se desarrolló el estudio?

La información recolectada por KPMG para el estudio muestra el Top 10 de industrias en Colombia que generaron **mayor INGRESO OPERATIVO durante 2.022**.

$135.447

Millones de pesos colombianos. Ingreso operativo promedio en 2.022 de todas las industrias del estudio.

Gráfico 1 – *INGRESO OPERATIVO PROMEDIO POR INDUSTRIA 2.022.*
Valores en millones de pesos colombianos.

Resumen Ejecutivo

¿Cómo se desarrolló el estudio?

Para cada una de estas industrias, se tomaron tamaños de muestra representativos.

13.684

Empresas incluidas en el estudio

10

Industrias incluidas en el estudio

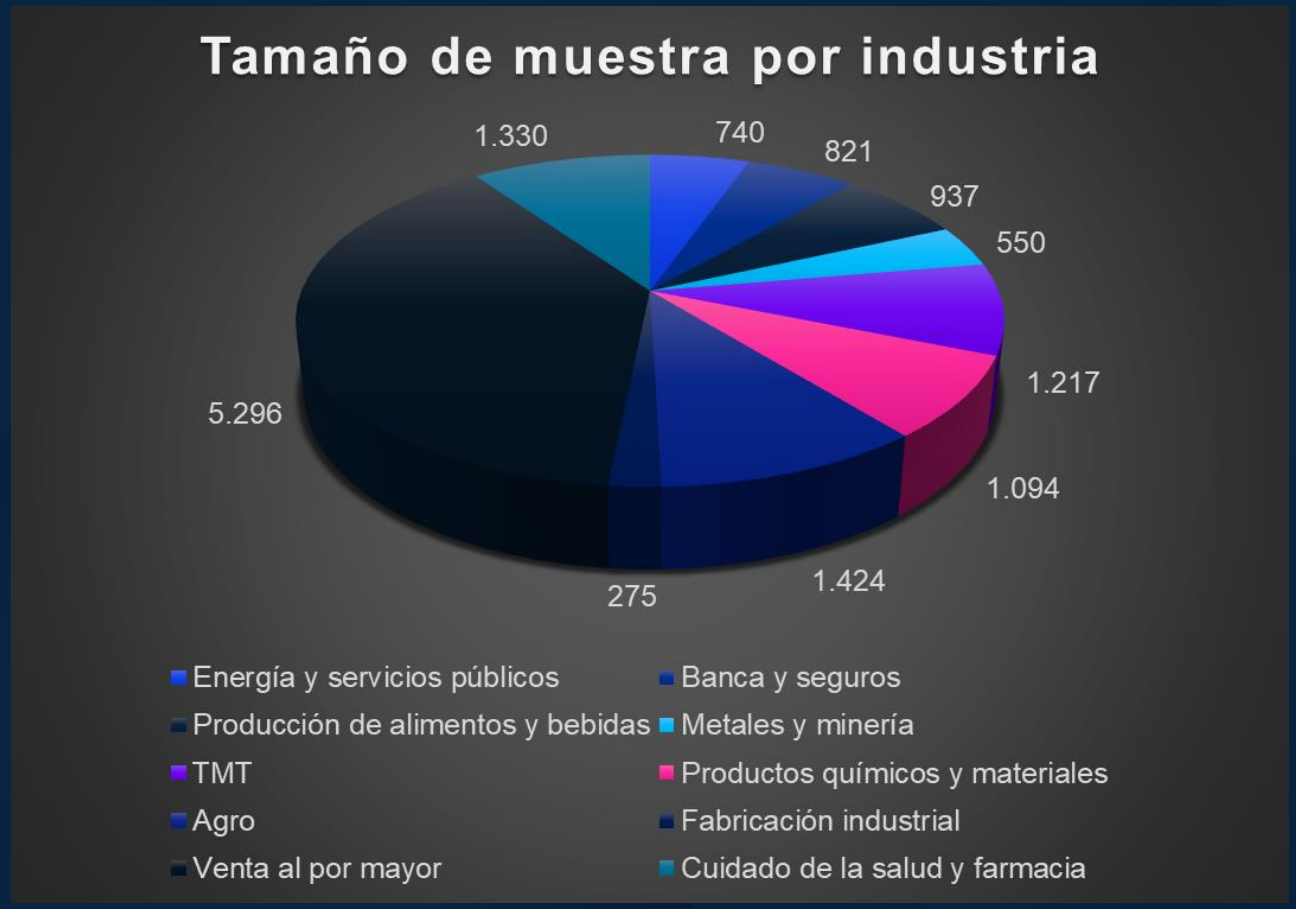


Gráfico 2 –Cantidad de empresas incluidas en el estudio por industria

Resumen Ejecutivo

¿Cómo se desarrolló el estudio?

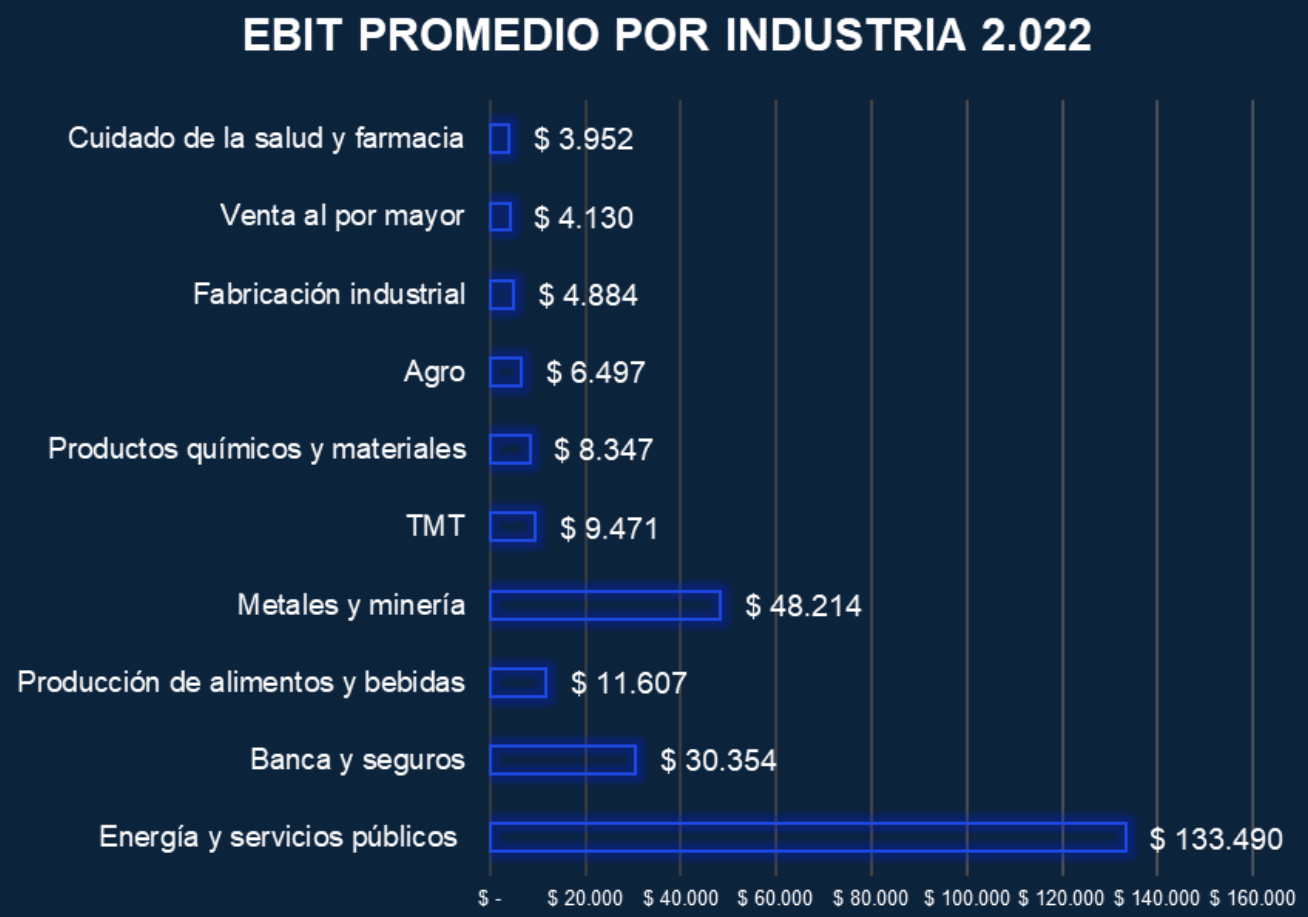


Gráfico 3 – EBIT PROMEDIO POR INDUSTRIA 2.022. Valores en millones de pesos colombianos.

También se recolectó información del **EBIT promedio durante 2.022 para las 10 industrias** que generan mayor ingreso operativo en Colombia.

$26.095

Millones de pesos colombianos.
EBIT promedio en 2.022 de todas las industrias del estudio.

¿Cómo se desarrolló el estudio?

Enero 2024

Iniciamos a recolectar la información de las empresas y el Benchmark de KPMG de madurez en Ciberseguridad.

Febrero 2024

Definimos las variables y parámetros para realizar las simulaciones a partir de los impactos primarios (p.e. pérdidas de ingresos) y secundarios (p.e. impacto en la reputación).

Objetivo del estudio

Identificar el valor promedio del potencial de pérdida económica en pesos colombianos, para el top 10 de industrias en Colombia por mayor ingreso operativo generado en 2.022, debido a la ocurrencia de un ciber ataque, y compararlo versus el ingreso operativo promedio y el EBIT promedio de cada industria, para definir un nivel de riesgo de materialidad por industria.

Resumen Ejecutivo

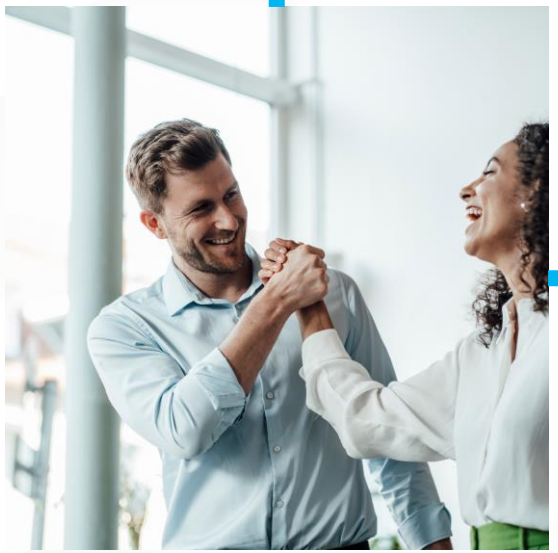
¿Cómo se desarrolló el estudio?

Marzo 2024

Iniciamos las simulaciones piloto del estudio para validar los parámetros y operación del modelo. Se realizaron 50.000 simulaciones con modelo de Montecarlo.

Abril 2024

Consolidamos el primer resultado del estudio en un resumen ejecutivo. Este resumen lo compartimos a los Chief Information Security Officers de clientes que han trabajado con KPMG, para tener su feedback, ajustar el estudio y el modelo.



Mayo y Junio 2024

Finalizamos el cálculo del ciber riesgo cuantificado por industria, consolidamos la información y calculamos el riesgo de materialidad por industria.
Solicitamos feedback a varios CISOs e hicimos algunos ajustes.

Resumen Ejecutivo

¿Cómo se desarrolló el estudio?

Me parece que el informe está muy bien logrado, tiene una muestra bastante significativa segmenta por industrias y evalúa escenarios con criterios y datos claves para el cálculo de probabilidad e impacto de un ciber incidente. Aporta claramente a tener una visión del segmento al cual pertenecemos, pero más allá, es una provocación para evaluar de forma individual el ciber riesgo cuantificado de nuestra organización.

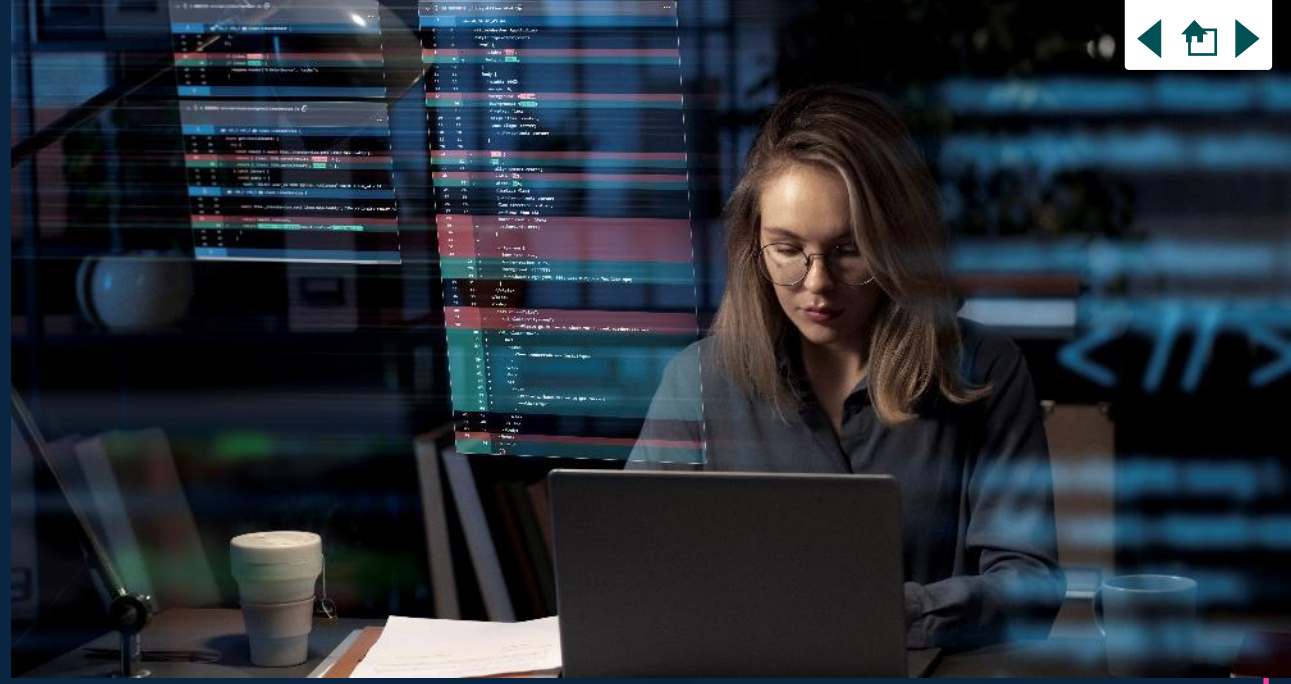
CISO de uno de los bancos más grandes en Colombia.

Julio 2024

Lanzamiento del estudio al mercado.

Resumen Ejecutivo

Resultados del estudio



El resultado del estudio muestra que el **potencial impacto económico promedio**, agrupando todas las industrias evaluadas, debido a un ciber ataque, es de:

$1.093,7

Millones de pesos colombianos por cada ciberataque

Para las empresas con niveles de madurez bajos, este valor de pérdida económica es potencialmente superior, por lo cual, cada organización debe evaluar su propia madurez y el impacto del ciber riesgo para determinar su propio potencial de pérdida.

Nota: El resultado de este estudio debe tomarse como una guía general.

Resumen Ejecutivo

Resultados del estudio

El impacto de la **pérdida sobre el EBIT promedio** agrupando todas las industrias es del

%↓ 4,2%

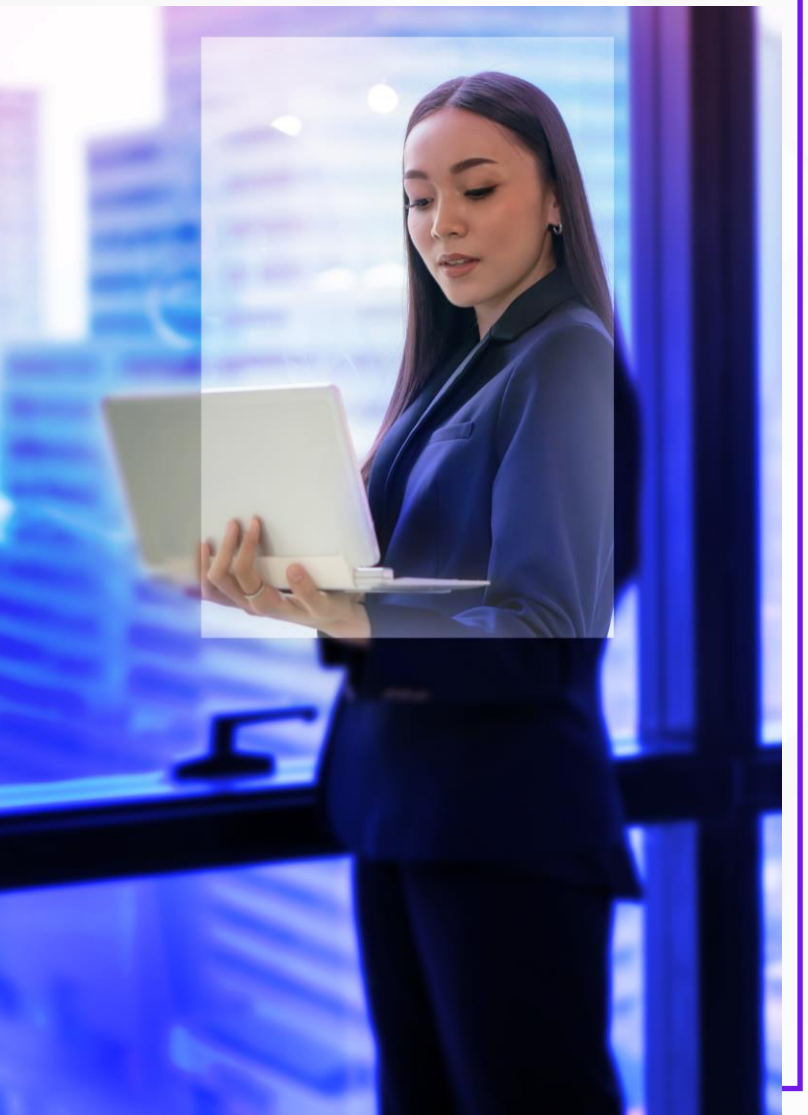
El Riesgo de materialidad promedio agrupando todas las industrias es: Medio

Porcentaje > 6% del EBIT
Porcentaje > 3% y < 6% del EBIT
Porcentaje < 3% del EBIT

Nota: El resultado de este estudio debe tomarse como una guía general.

Resumen Ejecutivo

Resultados del estudio



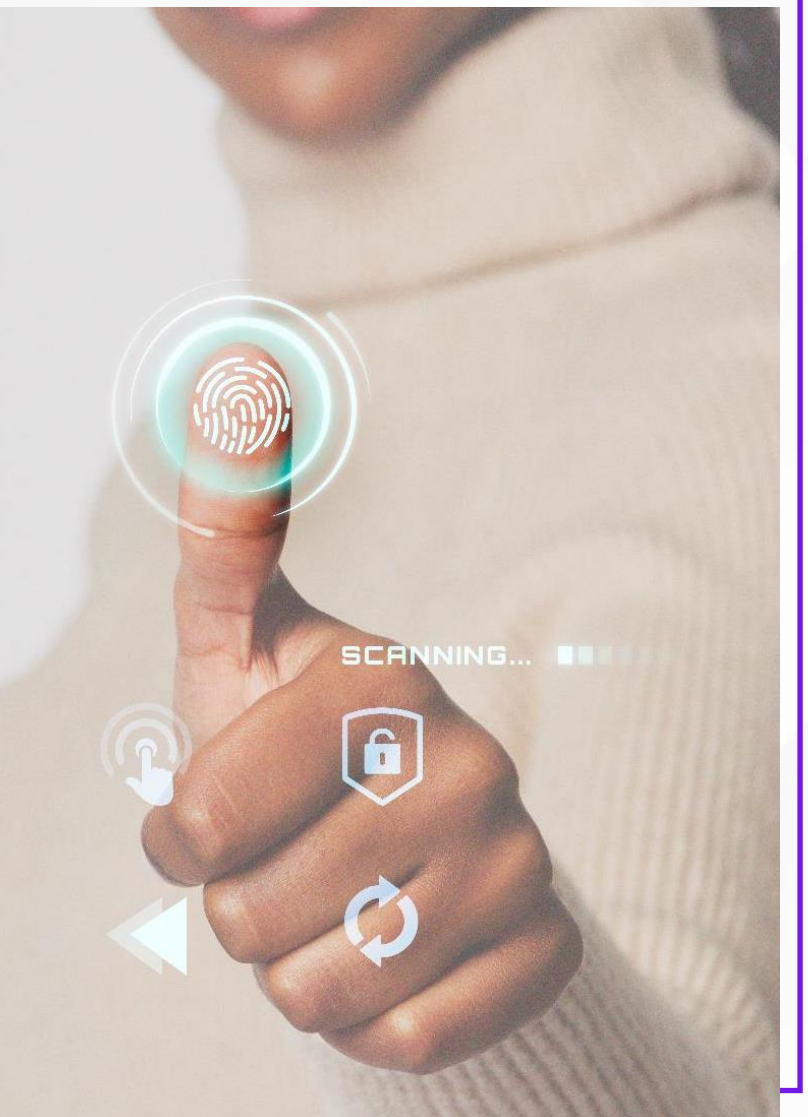
Resultados del estudio por industria

	Pérdida potencial	Riesgo de materialidad
Energía y servicios públicos	$1.916,8MM ↑	Low – High
Banca y seguros	$1.213,4MM ↑	Low – High
Producción de alimentos y bebidas	$1.451,1MM ↑	Low – High
Metales y minería	$1.130,5MM ↑	Low – High
TMT	$790,5MM ↓	Low – High

Menor al promedio de todas las industrias ↓ Mayor al promedio de todas las industrias ↑

Resumen Ejecutivo

Resultados del estudio



Resultados del estudio por industria

	Pérdida potencial	Riesgo de materialidad
Productos químicos y materiales	$1.147,1MM ↑	Low – High
Agro	$754,6MM ↓	Low – High
Fabricación industrial	$1.007MM ↓	Low – High
Venta al por mayor	$714,7MM ↓	Low – High
Cuidado de la salud y farmacia	$811,1MM ↓	Low – High

Menor al promedio de todas las industrias ↓ Mayor al promedio de todas las industrias ↑

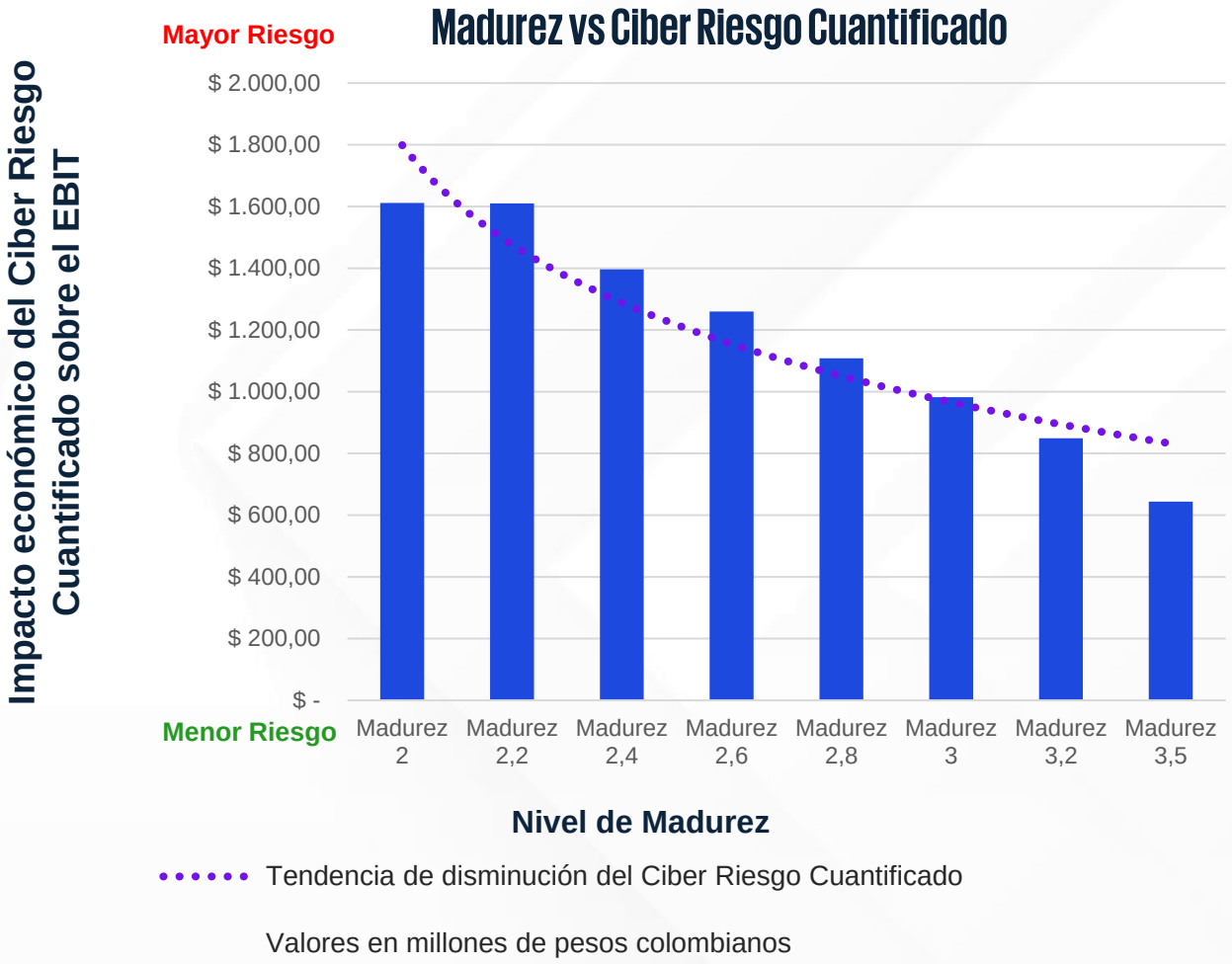
Resumen Ejecutivo

Resultados del estudio

El resultado del estudio también muestra que es necesario para las organizaciones tener un nivel de madurez más alto que el promedio actual de industria para evitar que las pérdidas potenciales por un ciber incidente lleguen a ser materiales.

Con valores de madurez superiores a **3.3 de 5,** el riesgo empieza a disminuir y el potencial de pérdida también, llegando a niveles donde no sería material (<3% del EBIT).

Sin embargo, para evitar un impacto económico alto, se deben fortalecer los controles que ayudan a mitigar el impacto.



Resumen Ejecutivo

Resultados del estudio

Acorde con la información de KPMG, los escenarios de ciber riesgo que representan mayor impacto económico para las organizaciones de todas las industrias evaluadas son los siguientes:

Ransomware

Ataque en el cual se realiza secuestro de datos, afectación del servicio y exfiltración de la información confidencial/privada.

Brecha de datos interna

Ataque de exfiltración de información desde un interno (empleado o tercero), exfiltrando información confidencial / privada de la organización.

Compromiso de Servicios Web

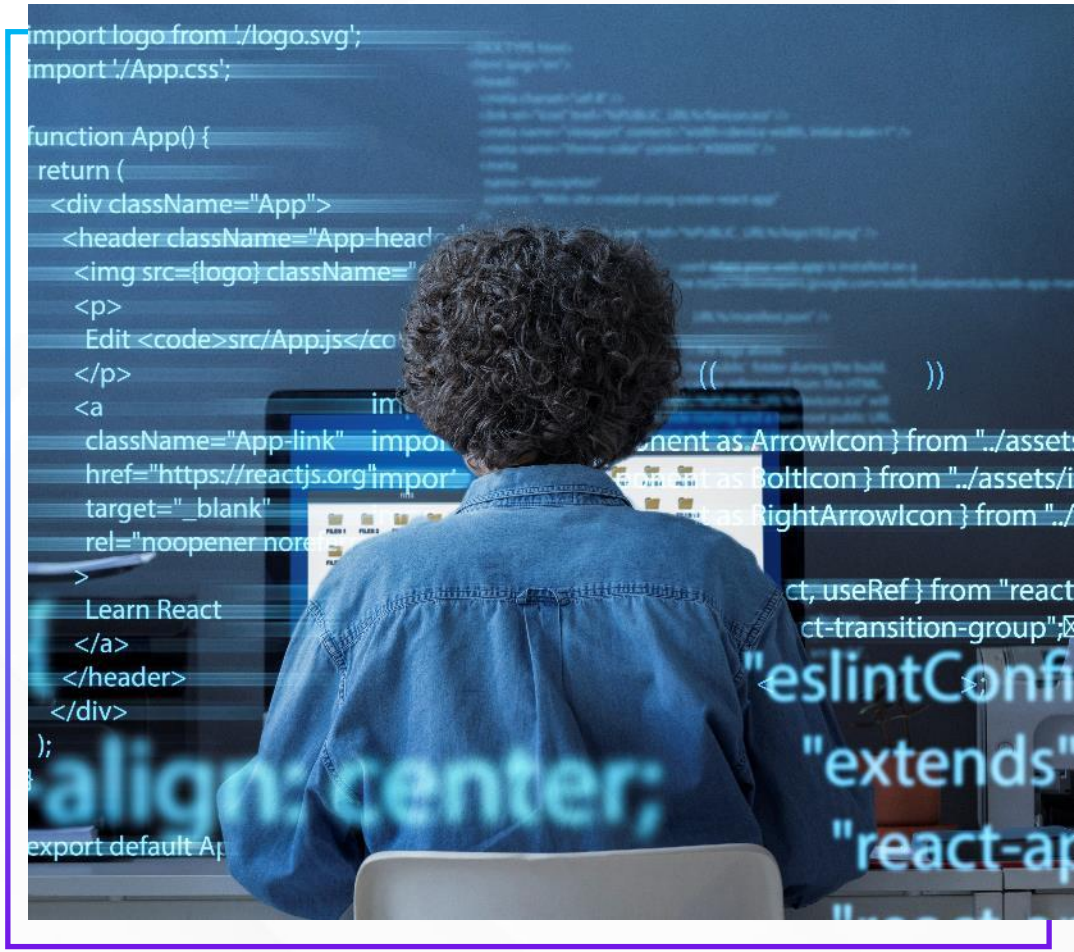
Ataque en el cual se compromete un servicio web público, permitiendo la exfiltración de información confidencial/privada de la aplicación.

Compromiso de Terceros

Ataque en el cual se compromete la seguridad de un tercero, y a través de este, se logra atacar a la organización.

Ataque BEC

Ataque en el cual se compromete la cuenta de un alto ejecutivo llevando a lograr la autorización de un pago grande fuera de la organización.



Resumen Ejecutivo

¿Cómo puedo reducir el impacto de un ciber incidente en mi organización?

01

Mida su nivel actual de madurez en ciberseguridad

establezca un nivel objetivo acorde con la criticidad de la industria y su apetito de riesgo, y defina un plan para llegar a ese objetivo. Realice mediciones anuales para validar que su nivel de madurez cumple con el objetivo planteado. Evalúe la madurez de los controles que ayudan a reducir el impacto de un ciber incidente.

02

Realice evaluaciones de ciber riesgo cuantificado

para identificar cuáles escenarios de ciber incidentes podrían tener mayor impacto en su organización, y establezca un plan de tratamiento para reducir la probabilidad y el impacto de estos escenarios. Recuerde que si cotiza en NYSE, la SEC definió en 2023 nuevas reglas que hacen que este ejercicio sea obligatorio.

03

Realice ejercicios de respuesta de ciber incidentes

que le permitan identificar qué tan preparado está para afrontar diferentes escenarios de posibles incidentes en su industria. Acorde con los resultados, actualice sus planes de respuesta de incidentes y de continuidad del negocio.

La gestión integral y diligente del riesgo de ciberataque en una organización requiere un enfoque holístico por parte del CISO moderno. Este enfoque debe considerar insumos como el nivel de madurez en ciberseguridad, las capacidades disponibles (humanas, técnicas y de procesos), así como también el impacto económico y operacional frente a una posible materialización del riesgo. De esta forma, el CISO puede generar de manera efectiva un programa de ciberseguridad alineado a las expectativas de la alta dirección y que responda a las necesidades reales y retos actuales de la organización.

Alejandro Ramírez
CISO de Grupo Keralty en Colombia

Resumen Ejecutivo

¿Cómo puedo reducir el impacto de un ciber incidente en mi organización?

04

Incremente las campañas de sensibilización en ciberseguridad

personalizándolas para los escenarios de ciber incidentes más probables que apliquen a su organización, y evalúe a los participantes para validar su aprendizaje. Se recomienda aumentar la frecuencia, e incluir a los terceros con los que tenga relación su organización.

05

Adquiera un servicio de respuesta de ciber incidentes

por demanda o prepagado, que le permita tener una reacción rápida ante un incidente y contenerlo oportunamente, lo que permitirá reducir el impacto en la organización y restablecer su operación en un menor tiempo.

06

Analice la posibilidad de tomar una póliza de ciber riesgo

Revise ofertas de póliza de ciber riesgo, que cubran los escenarios de riesgo que mayor impacto le traigan a su organización y que permitan reducir el impacto de un incidente de ciberseguridad. Valide el costo beneficio entre el riesgo cuantificado calculado vs. el costo de la póliza para tomar una decisión.

En un contexto extremadamente dinámico en cuanto a las amenazas y tecnologías emergentes, contar con metodologías cuantitativas de riesgos es primordial para priorizar las acciones en la estrategia de ciberseguridad.

Richard García Rondón
CISO de GeoPark

¿Cómo puede ayudarlo KPMG?

Nuestra capacidad global de Cyber

Creando juntos un mundo digital de confianza

La misión de KPMG Cyber es ayudar a nuestros clientes a mejorar su postura y capacidades de ciberseguridad **ahora y para el futuro**. Tanto si está entrando en un nuevo mercado, lanzando productos y servicios, o interactuando con los clientes de una nueva manera, KPMG puede ayudarle a anticiparse al mañana, moverse más rápido y obtener una ventaja con tecnología segura y de confianza.

350+
Ciber socios dedicados

9,300+
Ciber profesionales

145+
Países que proveen Servicios de Ciber

6,000+
Clientes globales

30+
Alianzas líderes en la industria

45,000+
Consultores globales en tecnología y riesgos

Respaldados por nuestra promesa al cliente

Ofrecemos los resultados que importan. Colaboramos con usted y con nuestros socios aliados

Aprovechamos la tecnología. Soluciones digitales que proporcionan una vía directa hacia la transformación sostenible.

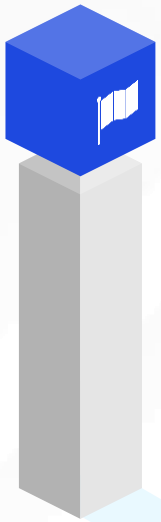
Sabemos cómo funciona su negocio. Nos basamos en nuestros modelos del sector para acelerar su progreso.

Sabemos cómo hacer las cosas. Metodologías de entrega y herramientas probadas para impulsar sus resultados.

Estamos a su lado en todo momento. Le ayudamos a sacar el máximo partido de la mejora continua y la innovación permanente.

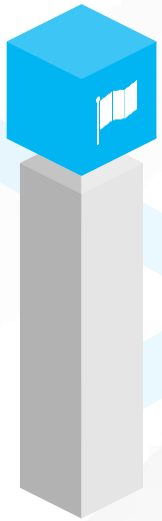
¿Cómo puede ayudarlo KPMG?

Servicios alineados a reducir el impacto de un ciber incidente en su organización



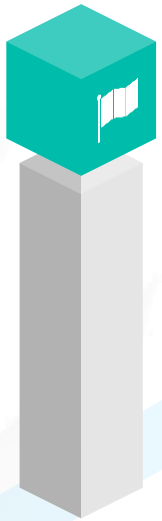
Cyber Maturity Assessment

El diagnóstico de madurez en ciberseguridad - Cyber Maturity Assessment (CMA) es un servicio único de KPMG diseñado para proveer una vista holística de las capacidades en seguridad de la información de una organización.



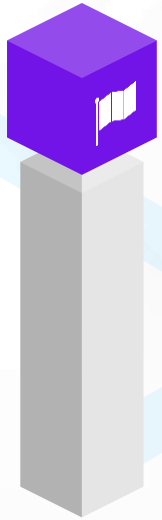
Cyber Risk Quantification

El servicio de Cuantificación de Riesgos de Ciberseguridad de KPMG permite evaluar de manera cuantitativa los riesgos a través de modelamiento de escenarios, y así mismo, definir las necesidades de inversión y mejoramiento de los controles.



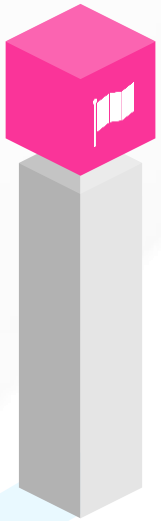
Cyber Incident Response Exercise

KPMG realiza un ejercicio teórico de simulación de ataque de ciberseguridad, en el cual evalúa los procesos de respuesta del cliente, y entrega recomendaciones de mejora y mejores prácticas.



Cyber Security Awareness

El enfoque de concientización de KPMG se enfoca en modificar el comportamiento de los usuarios, definiendo la visión deseada, midiendo el estado actual, estableciendo un programada de mejora, y midiendo de nuevo el estado final de conciencia de los usuarios.



Cyber Incident Response Services

KPMG apoya a las organizaciones al momento de sufrir un ciber incidente, y realiza análisis forenses, identificación de la causa del incidente, apoyo en la mitigación del impacto, y respalda consultas internas, legales, judiciales, o de terceros.

Agradecimientos

KPMG Colombia agradece a las siguientes personas por su apoyo y aportes en el desarrollo del presente estudio:

- Alejandro Ramirez, CISO de Grupo Keralty en Colombia.
- Richard García Rondón , CISO de GeoPark.
- Jorge Mario Barrantes Alvarez, CISO Viamericas.
- Enoc Rubio, Director de Tecnología, Grupo Empresarial Puerto de Barranquilla.
- Al CISO de uno de los bancos más grandes en Colombia.

Contáctenos

Jaime Vásquez
Socio Líder Advisory
javasquez@kpmg.com

Alain Almeida
Socio Advisory
abalmeida@kpmg.com

Felipe Silgado
Director Cyber Security Services
fsilgado@kpmg.com

colombia@kpmg.com.co
home.kpmg/co
T:+57 (1) 618 8000

KPMG Colombia

KPMG_CO