



FORRESTER®

AHORRO DE COSTES Y BENEFICIOS EMPRESARIALES IMPULSADOS POR CYBER QUANT

Estudio Total Economic Impact™ de Forrester Consulting encargado por Mastercard

JUNIO DE 2026



Índice

Resumen ejecutivo	2
El recorrido del cliente de Mastercard Cyber Quant	4
Análisis de beneficios	6
Análisis de costes	12
Resumen financiero	14
Marco metodológico TEI	15
Apéndices	17

Resumen ejecutivo

Las organizaciones se enfrentan a una presión creciente para evaluar el riesgo de ciberseguridad de forma coherente y comunicarlo en términos que la alta dirección pueda comprender y utilizar para la toma de decisiones. Sin embargo, muchas siguen dependiendo de procesos manuales y fragmentados que dificultan traducir el riesgo técnico a un impacto económico y empresarial.

Las organizaciones tienen la oportunidad de reducir el esfuerzo interno, mejorar la alineación entre los equipos de seguridad y el negocio, y respaldar decisiones de inversión tecnológica mejor fundamentadas mediante un enfoque estructurado para la evaluación del riesgo de ciberseguridad. Disponer de información cuantificada sobre el riesgo a escala corporativa transforma la evaluación del riesgo de ciberseguridad de un ejercicio puntual de cumplimiento normativo en una capacidad estratégica para la toma de decisiones.

Mastercard Cyber Quant es una plataforma de evaluación del riesgo de ciberseguridad que cuantifica el riesgo financiero y modeliza el impacto potencial sobre el negocio. Cyber Quant combina respuestas a cuestionarios, señales técnicas e inteligencia de amenazas para cuantificar el riesgo de ciberseguridad y estimar la exposición financiera potencial. La plataforma genera una puntuación global del riesgo y resultados basados en escenarios que ayudan a los equipos de seguridad a relacionar las brechas de control con el impacto empresarial, facilitando conversaciones más claras con la alta dirección y con los responsables del negocio.

Mastercard encargó a **Forrester Consulting** la realización de un estudio **Total Economic Impact™ (TEI)** para analizar el retorno potencial de la inversión (ROI) que las organizaciones pueden obtener al implantar Cyber Quant. El objetivo del estudio es proporcionar un marco de referencia que permita evaluar el impacto financiero potencial de Cyber Quant en sus organizaciones.

Resultados principales

112 % Retorno de la inversión (ROI)

255 000 USD Valor Actual Neto (VAN / NPV)

Para comprender mejor los beneficios, costes y riesgos asociados a esta inversión, Forrester entrevistó a cuatro responsables de la toma de decisiones con experiencia en el uso de Cyber Quant. A efectos de este estudio, Forrester consolidó las experiencias de los entrevistados en una única organización compuesta representativa.

Antes de implantar Cyber Quant, las organizaciones dependían de hojas de cálculo o de evaluaciones de riesgo realizadas por consultoras externas. Estos procesos consumían mucho tiempo, eran difíciles de repetir y, en muchos casos, los resultados quedaban obsoletos antes incluso de finalizar el proyecto. Como consecuencia, las organizaciones obtenían una visión inconsistente del riesgo y tenían dificultades para comunicar sus conclusiones en términos empresariales.

Tras implantar Cyber Quant, las organizaciones adoptaron un proceso de evaluación estandarizado y respaldado por la plataforma, reduciendo significativamente el esfuerzo interno, obteniendo una visión integral del riesgo empresarial y facilitando la priorización de las acciones de remediación y de las inversiones en ciberseguridad.

Principales beneficios cuantificados

- **Reducción del 50 % del tiempo necesario para realizar cada evaluación de riesgos.** La adopción de un proceso estructurado y repetible, gestionado por un equipo reducido de seguridad y respaldado por cuestionarios estandarizados y recopilación centralizada de evidencias, reduce el tiempo y el esfuerzo necesarios para realizar evaluaciones del riesgo en toda la organización.



Valor generado en tres años: 148 000 USD

- **Reducción del 55 % del esfuerzo necesario para responder a auditorías externas.** Los equipos utilizan los resultados de Cyber Quant —incluidas las evidencias, el contexto del riesgo y los criterios de priorización— para respaldar las conversaciones posteriores a las auditorías y planificar las actividades de remediación. Como resultado, el personal dedica menos tiempo a interpretar los resultados y puede centrarse en resolver los riesgos prioritarios.

Valor generado en tres años: 320 000 USD

- **Mejores decisiones de inversión en ciberseguridad.** Cyber Quant actúa como un mecanismo de validación para las decisiones de inversión en seguridad. Mediante evaluaciones cuantificadas del riesgo e información alineada con los objetivos del negocio, las organizaciones pueden determinar si una nueva tecnología o un nuevo control reducirá realmente su nivel de riesgo. Esto permite aplazar o evitar inversiones que no aportan una reducción significativa del riesgo.

Valor generado en tres años: 14 500 USD

Beneficios no cuantificados

Además de los beneficios económicos incluidos en el estudio, los entrevistados identificaron otras ventajas relevantes:

- Una mejor comunicación entre los equipos de seguridad, la alta dirección y las áreas de negocio al traducir el riesgo técnico en impacto financiero.
- Una priorización más eficaz de los controles de seguridad teniendo en cuenta el contexto empresarial, el panorama de amenazas y la exposición real al riesgo.

Costes

El coste ajustado por riesgo durante un período de tres años corresponde principalmente al licenciamiento de la plataforma Cyber Quant.

Valor actual de la inversión: 227 000 USD

Resumen financiero

El análisis financiero realizado por Forrester concluye que una organización representativa obtiene:

- **482 000 USD** en beneficios (Valor Actual)
- **227 000 USD** en costes (Valor Actual)
- **255 000 USD** de Valor Actual Neto (VAN)
- **112 %** de retorno de la inversión
- **Período de recuperación inferior a seis meses**

"Cyber Quant nos ayuda a tomar decisiones sobre amenazas concretas y sobre posibles inversiones tecnológicas. Cuando presento el cuadro de mando a la alta dirección, comprenden claramente la necesidad de realizar determinadas inversiones. En muchas ocasiones, las mejoras no dependen únicamente de la tecnología; también implican optimizar procesos o reforzar el equipo."

Responsable de Ciberseguridad, empresa de consultoría

El recorrido del cliente de Mastercard Cyber Quant

Factores que impulsaron la inversión en Cyber Quant

Organizaciones entrevistadas

Cargo	Sector	Región	Facturación
Responsable de Seguridad de la Información	Servicios financieros	Latinoamérica	18.000 millones USD
Responsable de Ciberseguridad	Consultoría	Latinoamérica	No revelada
Responsable de Ciberseguridad	Servicios financieros	Latinoamérica	7.000 millones USD
Director de Seguridad de la Información (CISO)	Servicios financieros	EMEA	No revelada

Principales retos

Los entrevistados describieron de forma consistente un entorno previo a Cyber Quant caracterizado por evaluaciones del riesgo manuales, lentas y difíciles de traducir al lenguaje del negocio. Como consecuencia, las organizaciones tenían dificultades para mantener una visión actualizada e integral del riesgo de ciberseguridad y para comunicar claramente su impacto económico a los responsables de la toma de decisiones.

- Las evaluaciones basadas en hojas de cálculo generaban riesgo operativo y reducían la confianza en los resultados.** Los equipos de seguridad dependían principalmente de hojas de cálculo que no estaban diseñadas para gestionar evaluaciones complejas del riesgo de ciberseguridad. La introducción manual de datos provocaba problemas frecuentes de control de versiones, dificultando la consolidación de la información, la conservación del historial de evaluaciones y la confianza en los resultados, especialmente cuando aumentaban el número de participantes y de fuentes de información. Uno de los responsables de seguridad entrevistados explicó: "Había muchos desafíos: registrar toda la información, correlacionar los datos y estructurarlos para elaborar gráficos y presentaciones. En ocasiones se perdía información o alguien sobrescribía el archivo de Excel y había que recuperar una copia de seguridad. Excel simplemente no está pensado para este tipo de trabajo." Además, esta falta de estructura dificultaba asignar responsabilidades claras entre los distintos equipos que participaban en la evaluación.
- Las evaluaciones eran lentas, poco frecuentes y quedaban obsoletas rápidamente.** La mayoría de las organizaciones únicamente podía realizar una evaluación integral del riesgo cada uno o dos años. Debido al elevado esfuerzo requerido, las evaluaciones terminaban convirtiéndose en ejercicios puntuales de cumplimiento normativo, en lugar de herramientas dinámicas para gestionar el riesgo de forma continua. Varios entrevistados indicaron que una evaluación podía prolongarse durante varios meses e implicar a numerosas áreas de la organización. El CISO entrevistado comentó: "Cada dieciocho meses realizábamos una evaluación completa." Otro entrevistado señaló que una única evaluación podía requerir aproximadamente seis meses de trabajo. Un responsable de seguridad añadió: "Cuando realizábamos las evaluaciones mediante hojas de cálculo las hacíamos cada dos años y tardábamos alrededor de seis meses en disponer de todos los resultados, porque debíamos involucrar a las áreas de riesgos, asesoría jurídica y otras funciones del negocio."
- El proceso requería la participación de numerosos departamentos.** En lugar de estar dirigido por un pequeño equipo especializado, el proceso exigía entrevistas repetidas, solicitudes constantes de información y múltiples ciclos de revisión entre Tecnología, Riesgos, Asesoría Jurídica y distintas



unidades de negocio. Esta dependencia de numerosos participantes hacía que el proceso fuese difícil de repetir y provocaba importantes interrupciones en la actividad diaria. Uno de los entrevistados indicó que una sola evaluación implicaba aproximadamente a veinte personas. El CISO explicó: "El proceso comenzaba con numerosas reuniones con los distintos responsables para revisar las configuraciones de seguridad, seguidas de la elaboración del informe y de varias rondas de revisión."

- **Las organizaciones carecían de una visión integral del riesgo.** Los enfoques tradicionales analizaban sistemas concretos, pero no ofrecían una perspectiva consolidada del riesgo a escala empresarial. Los entrevistados señalaron que normalmente obtenían mapas de calor, resultados por controles o análisis específicos de determinados sistemas, pero no una visión única del nivel de riesgo de toda la organización. Como resumió uno de los CISO entrevistados: "No disponíamos de una visión integral del riesgo en toda la organización." En muchos casos, el riesgo seguía expresándose mediante valoraciones cualitativas y no como una exposición cuantificada y agregada.
- **El riesgo de ciberseguridad no podía expresarse en términos económicos.** Otro reto importante consistía en traducir el riesgo técnico al lenguaje financiero. Los equipos de seguridad tenían dificultades para estimar pérdidas potenciales o relacionar el riesgo con el impacto sobre el negocio. Los entrevistados explicaron que otras soluciones evaluadas se centraban principalmente en medir el nivel de madurez, pero no permitían cuantificar el riesgo financiero. Uno de ellos comentó: "La otra herramienta era adecuada para medir el nivel de madurez, pero no para evaluar el riesgo. Nosotros necesitábamos cuantificar el riesgo financiero."
- **Resultaba difícil comunicar el riesgo a la alta dirección.** Los informes tradicionales estaban dirigidos principalmente a perfiles técnicos. Como consecuencia, los directivos tenían dificultades para comprender cuáles eran los riesgos prioritarios y qué impacto podían tener sobre la organización. Los entrevistados coincidieron en que el nivel de implicación de la dirección aumentó considerablemente cuando pudieron expresar el riesgo en términos económicos y operativos.
- **Las evaluaciones realizadas por consultoras externas carecían de consistencia.** Las organizaciones que dependían de evaluaciones realizadas por terceros obtenían resultados difíciles de comparar entre un año y otro. Cada consultora utilizaba metodologías, alcances y criterios distintos, limitando la capacidad para medir la evolución del riesgo. Uno de los CISO resumió la situación de la siguiente manera: "Anteriormente, cada proveedor externo utilizaba metodologías y alcances diferentes, lo que generaba resultados inconsistentes y dificultaba la comparación entre evaluaciones. Con Cyber Quant disponemos ahora de un marco metodológico y un modelo de puntuación homogéneos que nos permiten seguir la evolución del riesgo y demostrar mejoras medibles año tras año."

Objetivos de la inversión

Las organizaciones buscaban una solución capaz de:

- Implantar una alternativa estructurada y escalable a las evaluaciones manuales para reducir el tiempo y el esfuerzo.
- Obtener una visión integral del riesgo de ciberseguridad a escala empresarial.
- Cuantificar el riesgo en términos económicos para mejorar la comprensión por parte de la alta dirección y respaldar la toma de decisiones.
- Reducir la dependencia de evaluaciones realizadas por consultoras externas con metodologías poco consistentes.



"Antes de Mastercard Cyber Quant no disponíamos de una forma de cuantificar la posible pérdida de ingresos. Si un único riesgo afectaba a todos nuestros sistemas financieros, el impacto económico podía ser mucho mayor."

Responsable de Ciberseguridad — Servicios financieros

Organización compuesta

A partir de las entrevistas, Forrester desarrolló un marco **Total Economic Impact™ (TEI)** y construyó una organización compuesta representativa para elaborar el análisis financiero presentado en este estudio.

Perfil de la organización

La organización compuesta representa una empresa mediana que:

- Cuenta con **2.500 empleados**.
- Opera en un sector altamente regulado y con elevados requisitos de ciberseguridad.
- Gestiona operaciones regionales con múltiples entidades.
- Realiza evaluaciones tanto por entidad como a nivel regional para mantener la coherencia de los controles y de la postura de riesgo.
- Genera aproximadamente **500 millones de USD de facturación anual**.

Características de la implantación

La organización implanta Mastercard Cyber Quant para sustituir:

- Evaluaciones basadas en hojas de cálculo.
- Métodos internos de puntuación desarrollados de forma ad hoc.
- Evaluaciones puntuales realizadas por consultoras externas.

Durante el período inicial realiza su primera evaluación integral y obtiene una puntuación global del riesgo de ciberseguridad. Posteriormente mantiene una licencia **Essentials** durante los años 1, 2 y 3 para supervisar la evolución del riesgo y medir las mejoras alcanzadas.

Análisis de beneficios

Beneficios cuantificados para la organización compuesta

Beneficios totales

Beneficio	Valor Actual (3 años)
Mayor eficiencia en las evaluaciones del riesgo	148.000 USD
Mayor eficiencia en la respuesta a hallazgos de auditoría	320.000 USD
Mejores decisiones de inversión en ciberseguridad	15.000 USD
Beneficios totales (ajustados por riesgo)	482.000 USD



Mayor eficiencia en las evaluaciones del riesgo

Evidencia obtenida durante las entrevistas

Antes de implantar Cyber Quant, los entrevistados describieron la evaluación del riesgo de ciberseguridad como un proceso altamente manual que requería una coordinación considerable entre múltiples equipos y varios meses de trabajo para completarse. La mayor parte de las evaluaciones se realizaba mediante hojas de cálculo, lo que generaba dificultades relacionadas con la consolidación de la información, el control de versiones y la repetibilidad del proceso. Como consecuencia, los equipos de seguridad estaban limitados tanto en la frecuencia con la que podían evaluar el riesgo como en el alcance de dichas evaluaciones dentro de la organización.

- Tras implantar Cyber Quant, las organizaciones sustituyeron los procesos manuales y dispersos por un modelo estructurado y respaldado por la plataforma. Al centralizar la recopilación de información y estandarizar los cuestionarios de evaluación, fue posible reducir de forma significativa el trabajo manual y disminuir el número de personas implicadas. Uno de los entrevistados explicó: "Imagine que usted y yo respondemos al mismo cuestionario. Cada uno recibe su propio enlace y Cyber Quant identifica inmediatamente que usted ha respondido 'Sí' mientras que yo he respondido 'No'. Antes tenía que combinar manualmente varias hojas de cálculo para descubrir esa diferencia. Era muchísimo trabajo."
- Los entrevistados también destacaron que las evaluaciones podían realizarse con mucha mayor frecuencia. Un responsable de ciberseguridad comentó: "Si hoy realiza una evaluación y dentro de tres meses cambia el panorama de amenazas porque aparecen nuevas vulnerabilidades, Cyber Quant envía una notificación. En ese momento puede actuar inmediatamente o volver a realizar la evaluación."
- Esta capacidad permite supervisar el riesgo de manera continua en lugar de esperar uno o dos años para repetir el proceso. Gracias a este enfoque repetible, los equipos de seguridad pueden realizar evaluaciones con mayor eficiencia y con un impacto mucho menor sobre la actividad diaria.
- Un responsable de Seguridad de la Información señaló: "Hoy podemos comprobar en cuestión de minutos si el software instalado en nuestros equipos cumple con los controles que todavía debemos implantar."
- Un CISO entrevistado añadió: "Anteriormente las evaluaciones eran proyectos de gran envergadura que requerían consultores externos, numerosas reuniones y muchas horas de revisión de sistemas. Con Cyber Quant el proceso es mucho más eficiente y requiere considerablemente menos tiempo y coordinación."
- Incluso con cuestionarios cercanos a las quinientas preguntas, los entrevistados consideraron que el proceso seguía siendo sencillo de completar gracias a la estructura de la plataforma. Además de reducir el esfuerzo operativo, Cyber Quant permitió disponer de una visión verdaderamente integral del riesgo empresarial. Como explicó uno de los entrevistados: "Antes cada evaluación cubría únicamente una parte de nuestro entorno tecnológico. Ahora disponemos de una visión completa de todos nuestros sistemas y de una puntuación global del riesgo que nos permite medir objetivamente nuestra evolución con el paso del tiempo."

Modelo financiero y supuestos

A partir de las entrevistas, Forrester establece los siguientes supuestos para la organización compuesta:

- Antes de implantar Cyber Quant, cada evaluación requería aproximadamente **1.000 horas de trabajo**.
- Con Cyber Quant, el tiempo necesario para completar una evaluación se reduce en un **50 %**.
- El coste horario totalmente imputable del personal encargado de realizar las evaluaciones es de **62,50 USD por hora**.



Factores de riesgo

El beneficio obtenido variará entre organizaciones en función de:

- El número de evaluaciones realizadas antes de implantar Cyber Quant.
- Los recursos asignados al proceso.
- El alcance de las evaluaciones.
- El nivel de madurez del programa de gestión del riesgo.
- El grado de familiaridad de los equipos con la plataforma.

Para reflejar esta variabilidad, Forrester aplica un ajuste por riesgo del **5 %**, obteniendo un **Valor Actual de 148.000 USD** durante un período de tres años.

Resultados

Reducción del tiempo necesario para realizar una evaluación del riesgo 50 %

Concepto	Valor
Beneficio anual	59.375 USD
Beneficio total (3 años)	178.125 USD
Valor Actual	147.657 USD

"Hay numerosos casos en los que utilizamos Cyber Quant como referencia para cumplir con distintos requisitos regulatorios. Resultaría imposible realizar seis o siete evaluaciones independientes durante el año. En su lugar, realizamos una única evaluación anual con Cyber Quant y esa evaluación nos sirve de apoyo para prácticamente todas nuestras obligaciones de cumplimiento."

Responsable de Seguridad de la Información — Servicios financieros

Mayor eficiencia en la respuesta a los hallazgos de auditoría

Además de mejorar la eficiencia de las evaluaciones del riesgo, los entrevistados describieron un beneficio adicional: Cyber Quant redujo significativamente el esfuerzo necesario para responder a los hallazgos derivados de auditorías externas.

Antes de utilizar Cyber Quant, los equipos documentaban los hallazgos en informes estáticos o en hojas de cálculo, obligando al personal de seguridad a reconstruir manualmente la evidencia, relacionar controles y justificar decisiones durante cada proceso de seguimiento.

Con Cyber Quant, las organizaciones comenzaron a reutilizar los resultados estructurados generados por la plataforma, empleándolos como soporte para auditorías, revisiones internas y actividades de remediación. En lugar de volver a recopilar información para cada auditoría, los equipos podían apoyarse en la evidencia ya disponible dentro de la plataforma.

Como consecuencia:

- Se redujo considerablemente el tiempo dedicado a localizar documentación.
- Disminuyó el esfuerzo necesario para validar decisiones previamente adoptadas.
- Los especialistas pudieron concentrarse en ejecutar las acciones de remediación, en lugar de reconstruir la evidencia necesaria para cada auditoría.

Un CISO entrevistado resumió este beneficio de la siguiente manera:

"Cyber Quant ofrece una excelente capacidad para gestionar y visualizar la información. Después de cada evaluación genera una presentación clara de las puntuaciones de riesgo, los actores de amenaza y los vectores de ataque, facilitando enormemente la comunicación con la dirección y con el consejo de administración."

Los entrevistados también señalaron que la claridad de los resultados redujo significativamente las conversaciones repetitivas entre las distintas áreas implicadas en los procesos de remediación.

Como explicó un responsable de ciberseguridad:

"Ahora mi equipo puede dedicar su tiempo a desarrollar proyectos para nuestros clientes, en lugar de invertirlo en proyectos internos. Eso nos permite aumentar los ingresos, mejorar los márgenes y generar nuevas oportunidades para el equipo."

Evidencia obtenida durante las entrevistas

Antes de implantar Cyber Quant, las organizaciones tomaban decisiones de inversión en ciberseguridad sin disponer de un mecanismo consistente que permitiera validar si dichas inversiones reducirían realmente el riesgo empresarial.

Con frecuencia, las decisiones estaban impulsadas por requisitos regulatorios, recomendaciones de buenas prácticas o necesidades puntuales de determinadas áreas, más que por una comprensión cuantificada del nivel de riesgo global de la organización.

Como consecuencia, existía el riesgo de invertir en tecnologías cuyo impacto real sobre la reducción del riesgo era limitado.

Tras implantar Cyber Quant, las organizaciones comenzaron a utilizar la plataforma como un mecanismo de validación para determinar si las inversiones tecnológicas previstas estaban realmente alineadas con su perfil de riesgo.

En lugar de adquirir automáticamente nuevas herramientas, los equipos de seguridad utilizaban Cyber Quant para responder a preguntas como:

- ¿Los controles actuales ya reducen suficientemente este riesgo?



- ¿Esta inversión tendrá un impacto significativo sobre nuestra exposición?
- ¿Existen otras iniciativas con una mayor prioridad?

Uno de los responsables de Seguridad de la Información comentó:

"Para nosotros es fundamental que cualquier tecnología que estemos evaluando esté respaldada por los resultados obtenidos con Cyber Quant."

El entrevistado explicó que una de las soluciones evaluadas finalmente no fue adquirida porque el análisis realizado mediante Cyber Quant demostró que apenas aportaría una reducción adicional del riesgo.

Mayor confianza en las decisiones de inversión

Los entrevistados coincidieron en que la plataforma no solo ayuda a decidir **qué adquirir**, sino también **cuándo no es necesario invertir**.

Al vincular las inversiones tecnológicas con evaluaciones cuantificadas del riesgo, las organizaciones reducen la probabilidad de destinar presupuesto a herramientas cuyo impacto sobre la postura de seguridad sería limitado.

Cyber Quant también ayuda a mantener el foco en aquellos controles que resultan más relevantes para el contexto regulatorio, geográfico y empresarial de cada organización.

Modelo financiero y supuestos

Forrester asume que la organización compuesta evita aproximadamente: **20.000 USD**

en inversiones tecnológicas durante el primer año gracias a la validación proporcionada por Cyber Quant.

Ajuste por riesgo

Dado que este beneficio puede variar en función de la estrategia tecnológica de cada organización, Forrester aplica un ajuste por riesgo del **20 %**.

Como resultado:

Valor Actual (3 años): 14.545 USD

Beneficio económico

Concepto	Valor
Inversión tecnológica evitada (Año 1)	20.000 USD
Beneficio ajustado	16.000 USD
Valor Actual	14.545 USD

"Ahora existe una mayor alineación entre los distintos países de nuestra región porque todos podemos comprobar que contamos con los mismos controles. En apenas unos clics podemos visualizar los controles implantados, el nivel de exposición, el riesgo y muchos otros indicadores."

Responsable de Seguridad de la Información — Servicios financieros

Beneficios no cuantificados

Además de los beneficios económicos incluidos en el modelo financiero, los entrevistados identificaron diversas ventajas estratégicas que aportan un valor significativo, aunque no fueron cuantificadas dentro del estudio.

Mejor comunicación con la alta dirección y las áreas de negocio

Antes de implantar Cyber Quant, los equipos de seguridad encontraban dificultades para comunicar el riesgo de ciberseguridad fuera del ámbito estrictamente técnico.

Aunque las evaluaciones generaban informes detallados, estos rara vez ofrecían una narrativa empresarial que permitiera a la alta dirección comprender rápidamente el impacto de los riesgos y tomar decisiones fundamentadas.

Tras adoptar Cyber Quant, las organizaciones observaron una mejora significativa en la comunicación con la dirección.

La capacidad de expresar el riesgo en términos económicos permitió cerrar la brecha existente entre el lenguaje técnico y las prioridades empresariales.

En lugar de debatir vulnerabilidades individuales, las conversaciones comenzaron a centrarse en el impacto potencial sobre la organización y en las actuaciones con mayor valor para el negocio.

Como consecuencia:

- aumentó la alineación entre seguridad y negocio;
- disminuyó el tiempo necesario para justificar prioridades;
- se agilizó la toma de decisiones.

Priorización más eficaz de los controles de seguridad

Los entrevistados también describieron un cambio importante en la forma de priorizar las actividades de remediación.

Antes de Cyber Quant resultaba complicado determinar qué acciones producirían la mayor reducción del riesgo.

Con Cyber Quant, las organizaciones pueden evaluar el riesgo considerando simultáneamente:

- el contexto empresarial;
- la exposición regional;
- el panorama de amenazas;
- el impacto económico.

Esto permite distinguir claramente entre riesgos de alto impacto y riesgos de menor relevancia, destinando los recursos allí donde generan un mayor valor para la organización.

Uno de los entrevistados resumió este beneficio del siguiente modo:

"Alineamos Cyber Quant con los riesgos específicos de nuestra región y de nuestro negocio para determinar qué controles debemos implementar."

Flexibilidad

Forrester destaca que el valor de la flexibilidad dependerá de la situación particular de cada organización.



Los entrevistados identificaron diversas oportunidades futuras que podrían incrementar aún más el valor obtenido mediante Cyber Quant.

Incrementar la frecuencia de las evaluaciones

Al eliminar la dependencia de procesos largos y manuales, las organizaciones pueden realizar evaluaciones con mayor frecuencia sin incrementar proporcionalmente el esfuerzo necesario.

Uno de los responsables de ciberseguridad explicó:

"Si necesito comprobar cómo ha evolucionado nuestra postura de ciberseguridad, simplemente realizo una nueva evaluación y comparo ambos resultados. Normalmente realizamos dos o tres evaluaciones al año."

Esto permite transformar la evaluación del riesgo en un proceso continuo de mejora, en lugar de un ejercicio periódico de cumplimiento.

Forrester señala que este beneficio potencial no se cuantificó dentro del modelo financiero, ya que dependerá de las características de cada proyecto.

Valor aportado por los partners

Servicios profesionales basados en Cyber Quant

Dos de las cuatro organizaciones entrevistadas utilizan Cyber Quant como plataforma principal para prestar servicios de evaluación del riesgo de ciberseguridad y consultoría especializada a sus propios clientes.

La plataforma les permite realizar evaluaciones alineadas con distintos marcos regulatorios y estándares del sector.

Aunque los entrevistados no cuantificaron el ahorro económico para sus clientes, sí destacaron mejoras significativas en:

- la consistencia de las evaluaciones;
- la claridad de los resultados;
- la capacidad para convertir los hallazgos en planes de actuación concretos.

Como consecuencia, Cyber Quant no solo genera valor para las organizaciones que lo implantan internamente, sino también para aquellas que ofrecen servicios de consultoría y gestión del riesgo apoyándose en la plataforma.

Análisis de costes

Costes cuantificados para la organización compuesta

Costes totales

Concepto	Valor Actual (3 años)
Costes de licencias	227.340 USD
Costes totales (ajustados por riesgo)	227.340 USD

Costes de licencias

Evidencia obtenida durante las entrevistas

Los entrevistados indicaron que utilizan Cyber Quant una o varias veces al año y que renuevan la licencia de la plataforma de forma continuada. Cyber Quant pasó a integrarse en el ciclo habitual de evaluación del riesgo de sus organizaciones.

En lugar de tratarse de un proyecto puntual, la plataforma se convirtió en un componente permanente del programa de gestión del riesgo de ciberseguridad.

Modelo financiero y supuestos

A partir de las entrevistas, Forrester establece los siguientes supuestos para la organización compuesta:

- La organización realiza una inversión inicial de **30.000 USD** para la primera evaluación.
- Posteriormente mantiene una licencia **Cyber Quant Essentials** con un coste anual de **75.000 USD** durante los años 1, 2 y 3.

El coste real dependerá de las necesidades de cada organización, de la combinación de productos contratados y del modelo de licenciamiento acordado con Mastercard.

Factores de riesgo

Forrester aclara que los importes incluidos en este estudio tienen únicamente fines de modelización económica.

No representan precios de catálogo ni reflejan necesariamente las tarifas abonadas por todas las organizaciones.

Para reflejar esta variabilidad, Forrester aplica un ajuste por riesgo del **5 %**, obteniendo un **Valor Actual de 227.340 USD** durante tres años.

Resumen económico de los costes

Concepto	Valor
Servicios iniciales de evaluación	30.000 USD
Licencia anual Essentials	75.000 USD
Coste ajustado (3 años)	267.750 USD
Valor Actual	227.340 USD



Resumen financiero

Indicadores consolidados (ajustados por riesgo)

El análisis financiero elaborado por Forrester concluye que una organización representativa obtiene los siguientes resultados durante un período de tres años.

Indicador	Resultado
Beneficios (Valor Actual)	482.260 USD
Costes (Valor Actual)	227.340 USD
Beneficio neto (Valor Actual)	254.920 USD
Retorno de la inversión (ROI)	112 %
Período de recuperación	Inferior a seis meses

Flujo de caja

Durante el primer año, los beneficios obtenidos superan ampliamente la inversión inicial realizada en la plataforma.

A partir de ese momento, la organización continúa generando beneficios recurrentes derivados de:

- una mayor eficiencia operativa;
- una reducción del esfuerzo dedicado a responder a auditorías;
- decisiones de inversión en ciberseguridad mejor fundamentadas.

Como resultado, la inversión alcanza su punto de equilibrio antes de transcurridos seis meses.



Nota importante

Los resultados financieros presentados en este estudio pueden utilizarse como referencia para calcular el retorno de la inversión (ROI), el Valor Actual Neto (VAN) y el período de recuperación para organizaciones con características similares.

Forrester ha utilizado una tasa anual de descuento del **10 %** para todos los cálculos financieros.

Todos los beneficios y costes se ajustaron mediante factores de riesgo con el fin de reflejar escenarios empresariales más realistas.

Los valores actuales y los valores actuales netos se calcularon descontando los flujos de caja futuros correspondientes a cada ejercicio.

Debido al redondeo de determinadas cifras, algunos totales pueden presentar ligeras diferencias respecto a la suma exacta de sus componentes.

Marco metodológico TEI

A partir de la información recopilada durante las entrevistas, Forrester desarrolló un marco **Total Economic Impact™ (TEI)** para ayudar a las organizaciones a evaluar el impacto económico potencial de invertir en Mastercard Cyber Quant.

El objetivo del marco TEI es identificar los beneficios, los costes, la flexibilidad y los riesgos que influyen en una decisión de inversión tecnológica.

Para ello, Forrester siguió un proceso compuesto por varias fases.

Investigación previa

Entrevistas con especialistas de Mastercard y analistas de Forrester para recopilar información relativa a Cyber Quant.

Entrevistas con clientes

Forrester entrevistó a cuatro responsables de organizaciones usuarias de Cyber Quant con el fin de recopilar información sobre beneficios, costes y riesgos.

Organización compuesta

Las experiencias de los entrevistados se consolidaron en una organización representativa utilizada como base para el análisis financiero.

Modelo financiero

Se desarrolló un modelo económico basado en la metodología TEI y posteriormente se ajustó mediante factores de riesgo para reflejar la incertidumbre inherente a toda previsión financiera.

Estudio de caso

El análisis considera cuatro elementos fundamentales:

- Beneficios
- Costes
- Flexibilidad



- Riesgos

La metodología TEI ofrece una visión completa del impacto económico de una inversión tecnológica y facilita la comunicación de dicho valor a la alta dirección.

Glosario

Beneficios

Valor económico que una solución aporta a la organización.

Costes

Todas las inversiones necesarias para implantar y operar la solución.

Flexibilidad

Valor estratégico que puede obtenerse mediante inversiones futuras realizadas sobre una plataforma ya implantada.

Riesgo

Nivel de incertidumbre asociado tanto a los beneficios como a los costes estimados.

La metodología TEI incorpora esta incertidumbre mediante distribuciones triangulares.

Valor Actual (VA)

Valor presente de los beneficios o costes futuros descontados mediante una tasa de interés.

Valor Actual Neto (VAN)

Valor actual de los flujos netos de efectivo futuros.

Un VAN positivo suele indicar que la inversión genera valor económico.

Retorno de la inversión (ROI)

Indicador que expresa el rendimiento esperado de una inversión.

Se calcula dividiendo los beneficios netos entre los costes.

Tasa de descuento

Tipo de interés utilizado para reflejar el valor temporal del dinero en el análisis financiero.

Las organizaciones suelen emplear tasas comprendidas entre el 8 % y el 16 %.

Período de recuperación

Tiempo necesario para que los beneficios acumulados iguallen la inversión inicial realizada.



Apéndices

Apéndice A – Metodología Total Economic Impact™

Total Economic Impact™ (TEI) es una metodología desarrollada por Forrester Research para ayudar a las organizaciones a evaluar el impacto económico de sus inversiones tecnológicas.

Su objetivo es facilitar la demostración del valor empresarial de las iniciativas tecnológicas tanto ante la alta dirección como ante otros responsables de la toma de decisiones.

Apéndice B – Notas finales

Divulgaciones

Los lectores deben tener en cuenta que:

- Este estudio fue encargado por Mastercard y elaborado por Forrester Consulting.
- No debe utilizarse como un análisis comparativo frente a la competencia.
- Forrester no garantiza que todas las organizaciones obtengan los mismos resultados.
- Cada organización debe utilizar sus propios datos para evaluar la conveniencia de invertir en Cyber Quant.
- Mastercard revisó el documento y realizó comentarios, pero Forrester mantuvo el control editorial sobre el contenido y las conclusiones del estudio.
- Mastercard proporcionó los nombres de los clientes entrevistados, pero no participó en las entrevistas realizadas por Forrester.

