



# Disparidad de incentivos

Los ciberdelincuentes aprovechan las fuerzas del mercado para aventajar a los defensores.

## Las tres dimensiones de la disparidad

La disparidad entre la ciberdelincuencia y la respuesta es de una gran complejidad. Se produce a distintos niveles: entre los agresores y los defensores, entre la estrategia y la implementación, y entre los directivos y los operadores de las empresas.

Atacantes



### Ágiles y rápidos

Los incentivos de los agresores se basan en un mercado fluido y descentralizado, lo que contribuye a que sean ágiles y se adapten rápidamente.

Defensores



### Limitados por los trámites burocráticos

Los defensores se enfrentan a los trámites burocráticos y a las decisiones impuestas desde arriba.

frente a

Estrategia



90 %

Más del 90 % de las empresas cuentan con una estrategia de ciberseguridad.

Implementación



Menos del 50 %

Menos de la mitad de las empresas han implementado completamente sus estrategias.

frente a

Directivos



### Diferente evaluación del éxito

Los directivos que diseñan las ciberestrategias no miden el éxito de la misma forma que los encargados de su puesta en práctica.

Operadores



### Eficacia limitada

Los responsables de poner las estrategias en práctica están sujetos a las imposiciones de los directivos.

frente a

## La disparidad

Aunque el riesgo para la ciberseguridad es más preocupante que nunca para las empresas, hay discrepancias en la gestión de riesgos, los incentivos del equipo, así como inherentes al modus operandi de los agresores frente a la forma de proceder de los defensores.



76 %

El 76 % de los encuestados sitúa ahora a la ciberseguridad como uno de los tres principales factores riesgos.



54 %

El 54 % de los directivos encuestados están más preocupados por el impacto en la reputación de la empresa que por los efectos reales de un incidente de seguridad.



83 %

El 83 % de los encuestados siguen comunicando daños debidos a ataques a la ciberseguridad.



5 veces más

Los operadores son 5 veces más propensos a indicar que no existen incentivos para la ciberseguridad.



Ideas/dinero

Los ciberdelincuentes de más alto nivel roban ideas, mientras que los de los niveles más básicos persiguen el dinero.



51 %

Solo el 51 % de los especialistas en TI consultados en Rusia habían encontrado un puesto de trabajo en un sector tecnológico legal.



42 %

Los ciberdelincuentes aprovechan hasta un 42 % de las vulnerabilidades antes de 30 días de haberse divulgado.

## Lecciones del mercado de la ciberdelincuencia

El mercado de la ciberdelincuencia frente al mercado de la protección



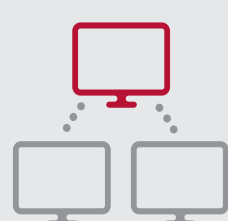
### Incremento de la transparencia

Ampliar el intercambio de información recorta costos para la aplicación de la ciberdelincuencia, ayuda a difundir noticias de la duplicación. Además, ayuda a difundir noticias sobre nuevas tecnologías y prácticas que aportan mejoras significativas para la seguridad.



### Equiparación de los incentivos

Para equiparar los incentivos de los directivos con los de los operadores, se deben ofrecer compensaciones y bonificaciones a los empleados y administradores que consiguen buenos resultados en seguridad.



### Aprovechamiento de las fuerzas del mercado

La externalización y los contratos abiertos reducen los costos, aumentan la competitividad y promueven la difusión de mejores prácticas innovadoras.



### Reducción de las barreras de acceso

Contar con una reserva de expertos más amplia, con jóvenes y especialistas en TIC extranjeros que a menudo terminan formando parte de la ciberdelincuencia, ayuda a las empresas cubrir las vacantes de ciberprofesionales y aprovecha el talento existente en el mercado de la ciberdelincuencia.



### Uso de divulgación pública

Responder con más celeridad a la divulgación de vulnerabilidades mediante una mejor aplicación de parches y una sustitución más rápida de los sistemas obsoletos contribuye a incrementar la seguridad y eleva los costos para los agresores.

Póngase a su nivel. Aprenda de los ciberdelincuentes. **Adáptese y triunfe.**

Visite [www.mcafee.com/misaligned](http://www.mcafee.com/misaligned) para ver el informe completo.

