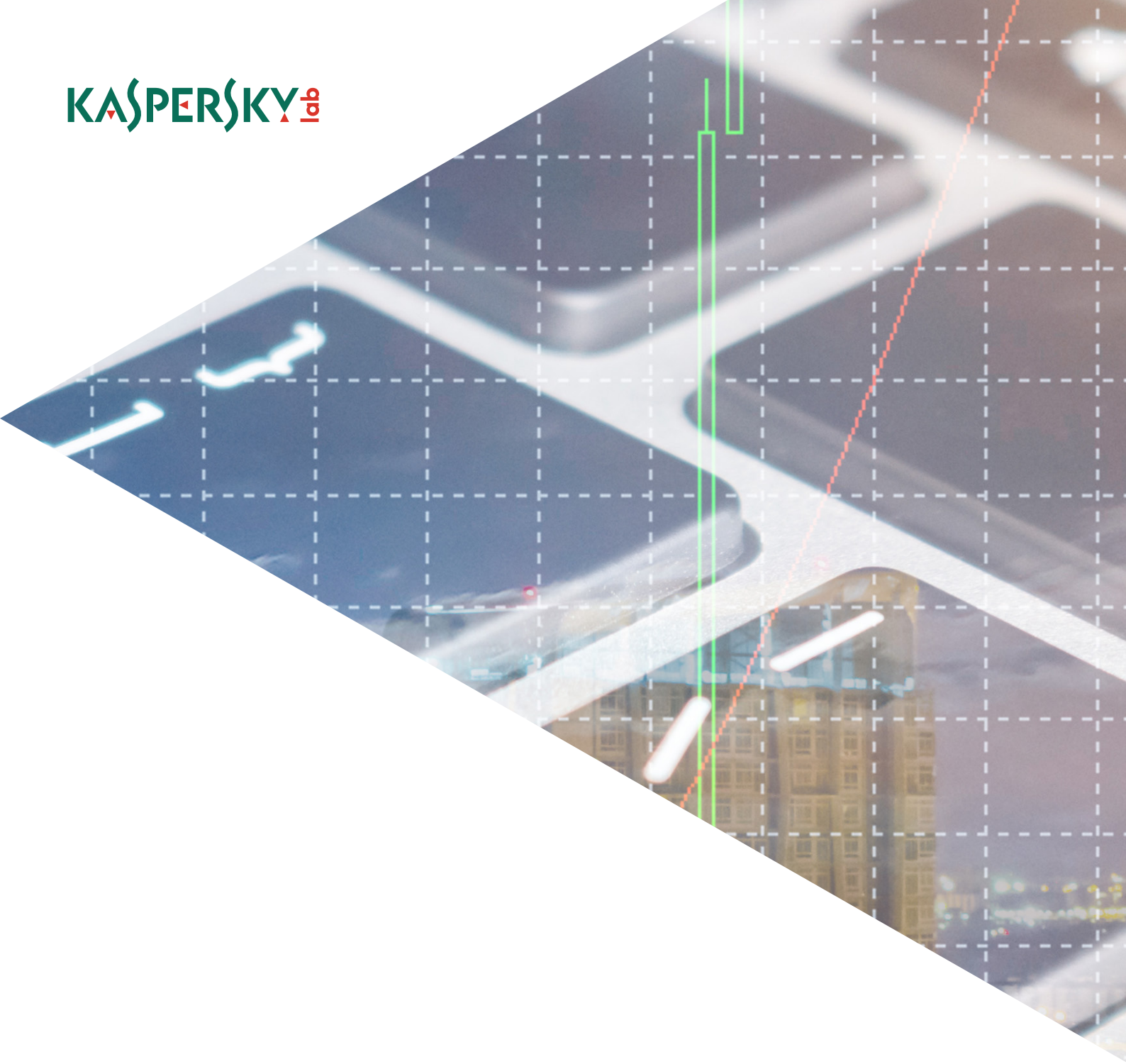


EL IMPACTO FINANCIERO DE LA SEGURIDAD DE IT EN LAS EMPRESAS EUROPEAS

Riesgos de seguridad de IT en 2016

Kaspersky Lab

TABLA DE CONTENIDOS

INTRODUCCIÓN

A medida que la información, el modo en que se genera y utiliza se digitaliza, también lo hacen los riesgos de los ciberataques. Como resultado, la ciberseguridad es ahora un tema de interés mundial que deben resolver los gobiernos, los organismos reguladores y las empresas. Por otro lado, es más importante que nunca que los recursos y el gasto de seguridad TI se sometan a un riguroso examen ya que de ellos dependerá la protección.

Para evaluar el estado del panorama de la seguridad en Europa y el resto del mundo, Kaspersky Lab ha colaborado con B2B International para saber si los presupuestos que se destinan a proteger a las empresas se correlacionan con las posibles pérdidas financieras provocadas por un incidente de seguridad. El estudio se ha realizado a más de 4.000 empresas de 25 países y analiza los presupuestos de seguridad TI, las actitudes y soluciones frente a las amenazas de seguridad, y el coste del robo de datos.

En lo relativo a las empresas europeas, una abrumadora mayoría (**70%**) espera aumentar su gasto en seguridad TI en los próximos tres años. Casi todas prevén un aumento de sus presupuesto de entre el **10%** y el **29%** (frente a un **35% en todo el mundo**). No obstante, ¿es suficiente la intención y la asignación de recursos para abordar las inminentes amenazas que se dirigen a las organizaciones europeas, independientemente de su tamaño?

ANÁLISIS DE LOS PRESUPUESTOS

Cuanto más dependen de la tecnología para sus operaciones, interacciones y comunicaciones diarias, las empresas requieren un mayor enfoque en seguridad TI para proteger las plataformas e infraestructuras utilizadas. Nuestro análisis indica que el factor principal del aumento de los presupuestos destinados a la seguridad es la complejidad de las infraestructuras TI, con una tercera parte de los encuestados (**35%**) que afirma que ese es el motivo principal; seguido en segundo lugar por quienes aluden a la expansión de la empresa y los nuevos negocios (**32%**).

A pesar de entender la necesidad de aumentar los presupuestos, más de un tercio de las empresas en Europa (**39%**) tiene dificultades para garantizar el gasto necesario para protegerse contra las amenazas a su seguridad. Esto es comparable a la mitad de todas las empresas a nivel mundial (**47%**). Efectivamente, al hablar de los desafíos de la implementación de medidas de seguridad TI, el **41% confirma** que es difícil demostrar a los directivos el retorno de la inversión (ROI) en seguridad.

Las empresas europeas y de todo el mundo coinciden en la necesidad de invertir en la mejora de la seguridad TI, ya que más de la mitad (56%), tanto en Europa como en todo el mundo, afirma que es mejor prevenir que curar.

Cuando se trata de la realidad de la inversión en seguridad TI, en contexto, este gasto solo representa una pequeña parte del presupuesto total de TI, y no siempre se traduce en acciones reales. En Europa, la mayoría de las empresas (**76%**) afirma que gasta menos del **20%** del presupuesto en seguridad (6**9% en el mundo)**. En términos reales, la cantidad puede ser mínima, con una de cada diez empresas europeas (**13%** en comparación con el **8%** de las empresas en todo el mundo) que gasta menos de 2.265 euros al año en todas sus medidas TI.

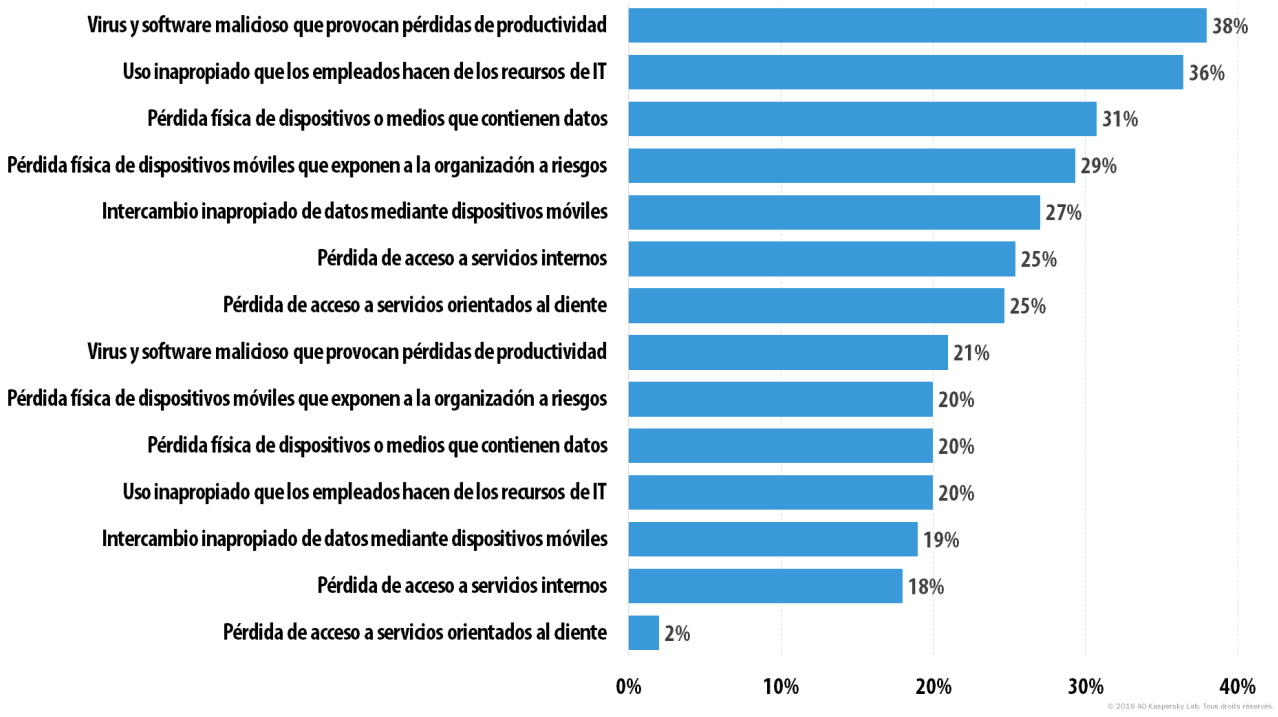
Muchas empresas europeas consideran que su seguridad depende en gran medida de la labor de sus empleados. Así, casi dos tercios de los encuestados (**64%**) prevé que, en los próximos tres años, la empresa contrate nuevos expertos en seguridad. Aunque esa cifra sea ligeramente inferior a la media mundial (**68%**), la mitad de las empresas europeas (**47%**frente al **54%** mundial) espera que aumente el gasto en contratación y el pago de salarios de sus expertos en seguridad TI.

IMPORTANCIA DE LOS COSTES

Al ponderar sus presupuestos, la mayoría de las empresas son conscientes de que los costes reales de un incidente de seguridad o un robo de datos pueden ser enormes si se tienen en cuenta el impacto en la reputación y las consecuencias financieras.

El estudio muestra que el **47%** de las empresas europeas (frente al **52%** mundial) presupone que su seguridad TI se verá comprometida en algún momento. Es más, en los últimos 12 meses, el **32%** de las empresas (frente al **38%** mundial) afima haber sufrido pérdidas de productividad por ataques con virus y software malicioso; mientras que el **30%** ha tenido problemas por el uso inapropiado que los empleados hacen de los recursos TI (**36% a nivel**mundial).

Tipos de eventos de seguridad ocurridos en los últimos 12 meses (media del total de empresas por tipo de ataque)



Frente al verdadero coste financiero de estos tipos de incidentes, solo cabe destacar la importancia de estar preparado y contar con presupuestos que sean eficaces. Nuestro estudio reveló que más del **84%** de las empresas europeas (en comparación con el **82% a nivel** mundial) han sufrido entre uno y cinco incidentes de exposición, filtración o pérdida de datos en los últimos 12 meses.

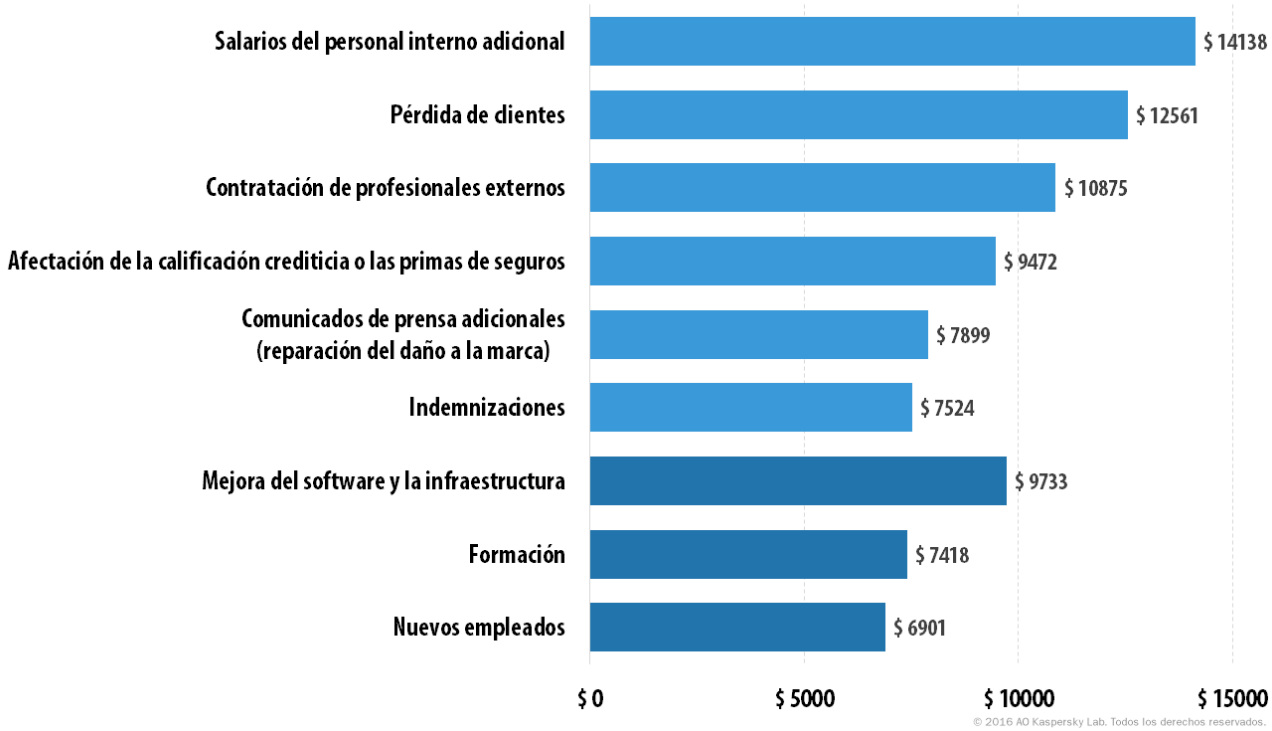
Como resultado de esa clase de incidentes, el **10%** de las empresas europeas perdió acceso a información crítica durante una semana (en comparación con una de cada diez empresas en todo el mundo) y el **15%** sufrió interrupciones que les impidieron realizar transacciones comerciales durante más de siete días. Descubrir que se ha producido un robo de datos tampoco es fácil y una de cada diez empresas (**10%**) podria tardar hasta un año. Esta falta de visibilidad y preparación que la mayoría ve como una consecuencia inevitable del panorama tecnológico que vivimos puede tener repercusiones financieras inimaginables.

Si se considera este tema en contexto, el impacto financiero de un solo vector de ataque y robo de datos se calcula aproximadamente en **77.372 euros** para las pymes a nivel mundial y en **770.252 euros** para las grandes empresas. En este cálculo, la reasignacióndel tiempo del personal de TI representa el mayor coste adicional, tanto para las pymes como para las grandes empresas.

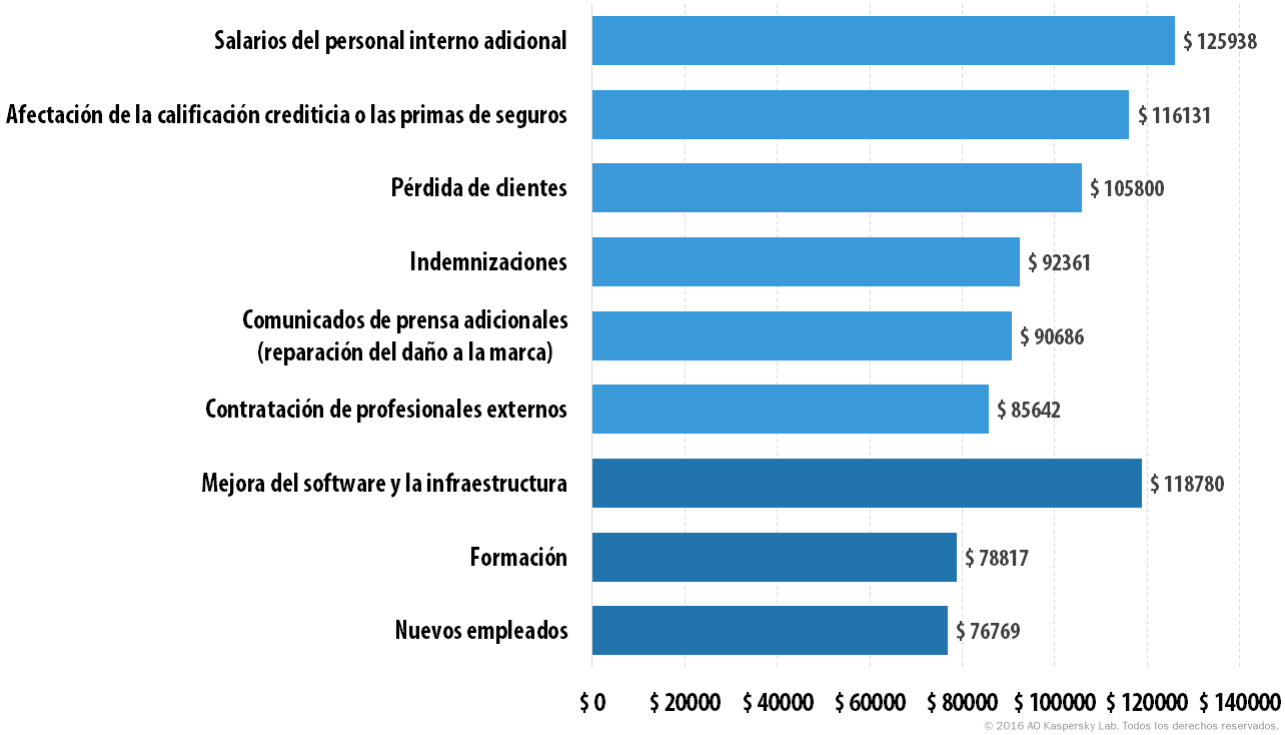
La investigación realizada sirvió para determinar hasta qué punto están ajustados los presupuestos y por qué hay poco margen para el error en la asignación de recursos a la seguridad. Para ello, se realizó una comparación de la media anual del gasto en seguridad TI en las pymes y en las grandes empresas con las pérdidas previstas de un solo ataque. Si tenemos en cuenta el gasto habitual de **193.000 euros** que las pymes invierten en seguridad y lo comparamos con el coste de un ataque (**77.372 euros**), las medidas de seguridad de las pymes solo necesitan evitar **dos ataques y medio** para ahorrarse elevadas cantidades, por no mencionar los daños a su reputación.

Desglose del impacto financiero por un incidente de robo de datos

Pymes



Grandes empresas



CONCLUSIÓN

El impacto financiero de los ciberataques debe analizarse en el contexto de los recursos que se implementan para combatirlos. Las empresas europeas reconocen la necesidad de mejorar la seguridad TI para hacer frente a estos ataques cada vez más frecuentes. El **26%** considera que la respuesta es añadir más personal y recursos de seguridad TI en los próximos 12 meses; mientras que el **36%** afirma que lo que se necesita es software de seguridad más avanzado. No obstante, los presupuestos no siempre respaldan estas medidas.

La clave para reducir el impacto es adoptar un enfoque holístico de seguridad de IT, en lugar de depender solo de la tecnología de detección. Para reducir los riesgos y obtener un retorno real sobre cualquier inversión en seguridad de IT, ya sea para contratar personal o adquirir software, la formación y la inteligencia constituyen un aspecto crucial. Después de todo, ser prevenido vale por dos, con lo que las organizaciones podrán reducir sus riesgos al ir más allá de la prevención y centrarse en la recuperación y mitigación de riesgos.