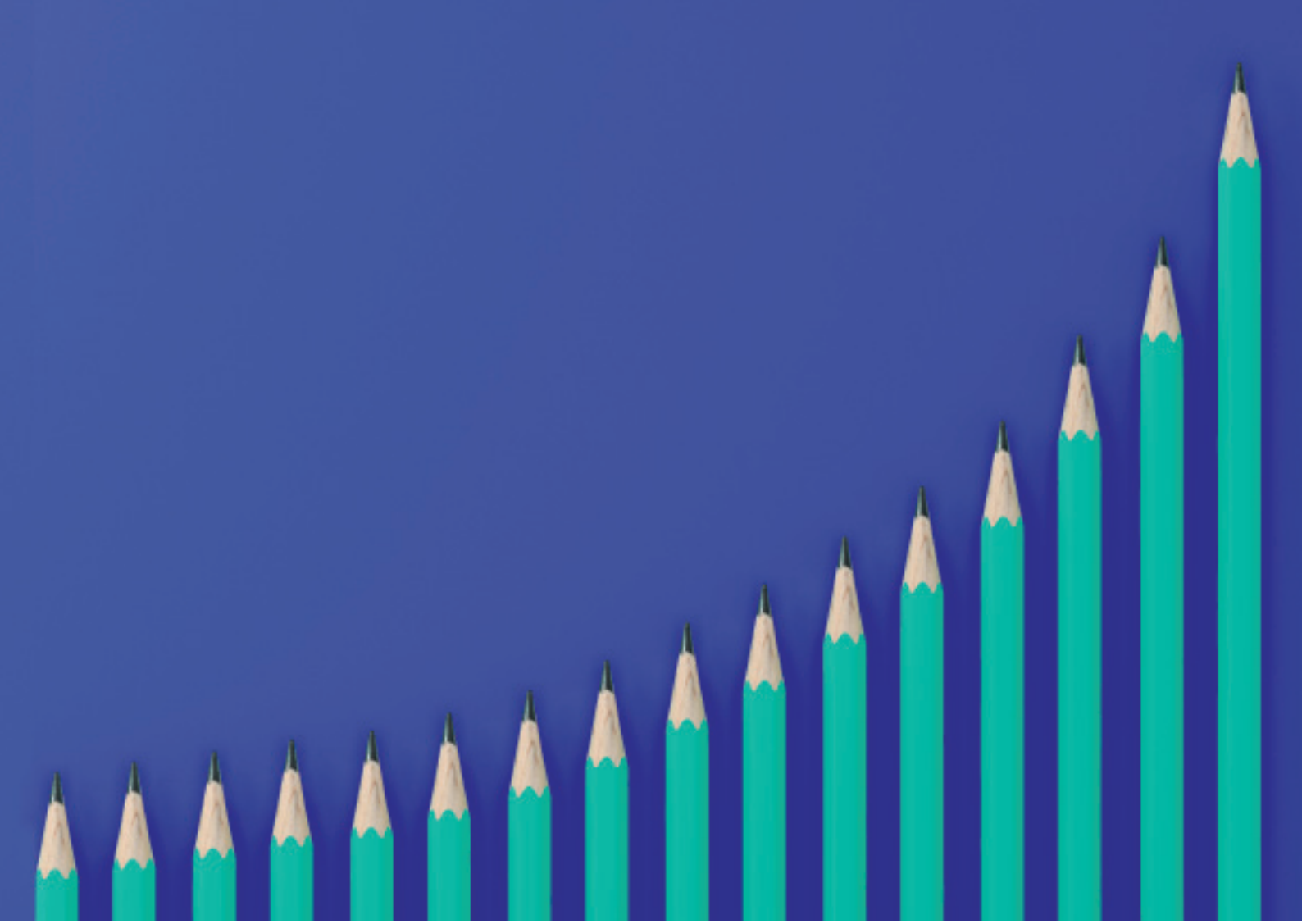


Cómo las empresas pierden dinero y ahorran costos en medio de los ciberataques

Economía de la seguridad de TI en el 2019

kaspersky BRING ON THE FUTURE

Contenido

Metodología

4,958 entrevistas

23 países

La Encuesta global de riesgos de seguridad en las TI empresariales (ITSRS) de Kaspersky es un estudio global sobre los responsables de la toma de decisiones de las TI empresariales, el cual ahora se encuentra en su noveno año. Se efectuaron un total de 4,958 entrevistas en 23 países. Se les preguntó a los encuestados sobre el estado de la seguridad en las TI de sus empresas, los tipos de amenazas a las que se enfrentan y los costos con los que tienen que lidiar mientras se recuperan de los ataques. Las regiones que se cubrieron fueron LATAM (América Latina), Europa, América del Norte, APAC (Asia-Pacífico incluido China), Japón, Rusia y META (Medio Oriente, Turquía y África).

A lo largo del informe, las empresas se denominan, ya sea PYMES (pequeñas y medianas empresas que cuentan con 50 hasta 999 empleados) o Empresas (las organizaciones que cuentan con más de 1,000 empleados). En este informe no se incluyen todos los resultados que se obtuvieron en la encuesta.

Todas las consecuencias financieras y los costos causados por los ciberataques que se mencionan en este informe están relacionados solamente con incidentes que, según los encuestados, han provocado vulnerabilidades en los datos.

Introducción

Se estima que en la primera mitad de 2019 habrá aproximadamente 4,000 violaciones de datos, poniendo en riesgo a más de 4 mil millones de usuarios.

Mientras los líderes empresariales se esfuerzan por proteger a sus empresas de futuras ciberamenazas, Kaspersky sigue trabajando para desarrollar un mundo más seguro. Esto implica comprender la forma en que las empresas y las PYMES siguen identificando las vulnerabilidades y se protegen a sí mismas contra ataques sofisticados.

Se estima que tan solo en la primera mitad del 2019 se produjeron casi 4,000 vulneraciones a los datos, lo cual representa más de cuatro mil millones de datos de usuarios en riesgo. En los últimos 12 meses, las organizaciones siguen siendo afectadas por vulneraciones a la ciberseguridad, costosas y de alto perfil. Este año, Gartner reveló que las inversiones en seguridad de las TI y el presupuesto dedicado a la infraestructura siguen creciendo. Se estima que las inversiones mundiales en TI alcancen un total de $3.74 billones en el 2019, a medida que las empresas responden a un número cada vez más grande de amenazas para sus sistemas, operaciones empresariales y financieras.

Dado que las empresas todavía son vulnerables a los ciberataques, es evidente que aún queda mucho por hacer para que puedan adaptarse a un panorama de amenazas que evoluciona rápidamente y en constante crecimiento. Mientras se esfuerzan por conseguirlo, vemos que las empresas siguen invirtiendo en sistemas y seguridad de sus TI. Con el Centro de Análisis e Intercambio de Información de Servicios Financieros advirtiendo a las empresas que deben solicitar mayores presupuestos para hacer frente a los problemas en ciberseguridad, es claro que las empresas deben reforzar sus negocios para reducir los riesgos a largo plazo y protegerse con anticipación de los ataques en el futuro.

Según nuestra investigación anual sobre la economía de la industria en la seguridad de TI, este informe muestra los resultados de las encuestas de los últimos 12 meses para resaltar la forma en que las empresas invierten su presupuesto en seguridad de las TI. También analiza cómo las empresas pierden dinero y ahorran costos en medio de los ciberataques, cómo se ven afectadas por el panorama de amenazas y la forma en que responden ante estos incidentes, tanto desde el punto de vista financiero como operativo.

Principais resultados

Más de un tercio (38%) sienten que no son lo suficientemente conscientes de las amenazas que enfrenta su negocio

· Aumento d ela confianza: más de la mitad (el 55 %) de las empresas confían plenamente en que su red no ha sido hackeada, aunque más de un tercio (el 38%) sienten que no cuentan con información suficiente sobre las amenazas a las que se enfrentan

· Las empresas pasan por alto el peligro: solo una de cada diez (el 12 %) empresas se preocupa por las infecciones de malware, aunque es el incidente de seguridad más costoso, con costos que llegan hasta los $2.73 millones

· El poder de las personas: el 66 %, tanto de empresas como de PYMES, buscan aumentar su inversión para contratar personal especializado en TI este año

· Advertencia pero no prevención: las políticas que regulan el acceso de terceros no mejoran la protección de la empresa, en vez de ello, simplemente triplican las posibilidades de compensación

· Aproveche sus fortalezas: contar con un Centro de Operaciones de Seguridad interno reduce casi a la mitad el impacto financiero que provocan las violaciones a la seguridad de los datos empresariales, de $1.4 millones a tan solo $675 mil

· Un RPD puede ahorrarle dinero: más de un tercio (el 34 %) de las empresas que cuentan con un Responsable de la Protección de los Datos no perdieron dinero cuando sufrieron una violación a la seguridad de sus datos

Las empresas deben centrar su atención en los ataques más costosos

Cada vez más, las empresas de todos los tamaños se sienten más confiadas de que su rede está segura.

A pesar de que las empresas están incrementando sus presupuestos para la seguridad de las TI y los recursos que destinan a supervisar los incidentes por amenazas, muchas de ellas no son conscientes de que los ataques les cuestan más dinero.

Cada vez más, las empresas de cualquier tamaño sienten mayor confianza en que su red es segura. El número de empresas que dicen sentirse "100 % seguras de que su red no fue hackeada" aumentó más del 10 % desde el informe del 2016 y ha crecido un 3 % año con año. Sin embargo, a pesar de esta confianza, más de un tercio todavía sienten que no cuentan con la información o inteligencia suficiente para el tipo de amenazas a las que se enfrentan sus empresas.

Esto se refleja en los tipos de amenazas que preocupan más a nuestros encuestados y que afectan su negocio. Para las empresas, la infección de malware en los dispositivos empresariales es actualmente la forma de violación a la seguridad de los datos que representa el mayor impacto financiero, con un costo equivalente a $2.73 millones este año, a pesar de que solo un pequeño porcentaje de las empresas se sienten muy preocupadas por la infección de malware como una amenaza.

Las PYMES también ignoran cuales son los tipos de ataques más costosos. El tipo de violación a la seguridad de los datos más costoso para las empresas pequeñas son los incidentes que afectan la infraestructura de las TI alojada por terceros, los cuales suman hasta $162K. Sin embargo, las PYME solo lo clasificaron como la quinta medida más importante, y están más bien preocupadas por los problemas de protección de los datos, como la pérdida de un dispositivo físico o la pérdida de datos mediante un ataque dirigido.

Invertir en las personas, no en los sistemas

En el informe del año pasado, muchas empresas iniciaron proyectos de transformación digital para revisar sus sistemas y defenderlos de los ciberataques, en particular de las vulneraciones basadas en la nube. Sin embargo, los resultados de este año revelan que las empresas están invirtiendo cada vez más en su personal y en recursos con el fin de prepararse para más ataques y preparar a sus departamentos de TI para el futuro.

En el 2019, las empresas vieron el mayor aumento en los costos después de sufrir incidentes como consecuencia de la contratación de profesionales externos ($170 mil) y la contratación de nuevo personal ($131 mil), los cuales aumentaron 35 % y 24 % respectivamente desde el 2018. En las PYMES, los nuevos costos de contratación de personal se mantienen sin cambios en $11 mil, en comparación con la reducción de gastos en otros departamentos de todas las áreas. Sin embargo, las organizaciones se enfrentan al desafío de poder invertir en personas con experiencia para desarrollar una empresa más segura, ya que el talento no es suficiente para satisfacer las demandas del mercado.

En particular, esto da como resultado el reforzamiento de los equipos internos de TI, en vez de contratar solamente MSP externos, lo cual aporta más habilidades y experiencia internamente.

Invertir en recursos específicos, y capacitar a los expertos internamente, también es una forma en que las empresas ahorren costos a largo plazo después de que se produce un ataque en la seguridad. Como lo muestra nuestra investigación, el 34 % de todas las empresas que cuentan con un RPD (responsable de la protección de datos) especializado interno, no perdieron dinero cuando sufrieron una violación a la seguridad de los datos. Nuestro informe deja claro que esta inversión continua en personal y experiencia interna se está convirtiendo en la clave para que las empresas minimicen las pérdidas financieras y se protejan a sí mismas de incidentes futuros.

Los Centros de Operaciones de Seguridad cada vez son más importantes

Curiosamente, nuestro estudio también encontró que la consolidación de los sistemas de las TI también se traduce en ahorros cuando se produce una violación a la seguridad de los datos. Contar con un Centro de Operaciones de Seguridad interno reduce casi a la mitad el impacto financiero que causan las violaciones a la seguridad de los datos para las empresas, de $1.4 millones a solo $675 mil.

También hay ahorros superiores para las PyME que adoptan un SOC, con un impacto financiero total de una vulneración de datos de solo $106 mil para aquellas con un SOC interno, en comparación con $129 mil para las PYMES en general. Aunque este ahorro no es tan grande, sí reduce los costos un 22 %, pero este ahorro en los costos puede ser menor dado que muchas PYMES incluso utilizan un servicio externo para esta función.

Siga leyendo para obtener más información sobre los resultados del informe.

El uso inapropiado de TI conduce a la forma más frecuente de vulneración de datos

Nuestro informe del 2019 reveló que tanto las empresas como las PYME fueron las más afectadas por incidentes, como resultado del uso inapropiado de los recursos de TI por parte de los empleados (52 % empresas, 50 % PYME), seguido de la infección de malware de los dispositivos de las empresas (51 % empresas; 49 % PYME). Esto refleja que las empresas podrían considerar la posibilidad de reducir el riesgo de la vulneración de datos mediante una mayor formación para la seguridad para los datos de los empleados, con el fin de aumentar la conciencia sobre el uso seguro de las TI.

Los incidentes más frecuentes dirigidos a las PYMES

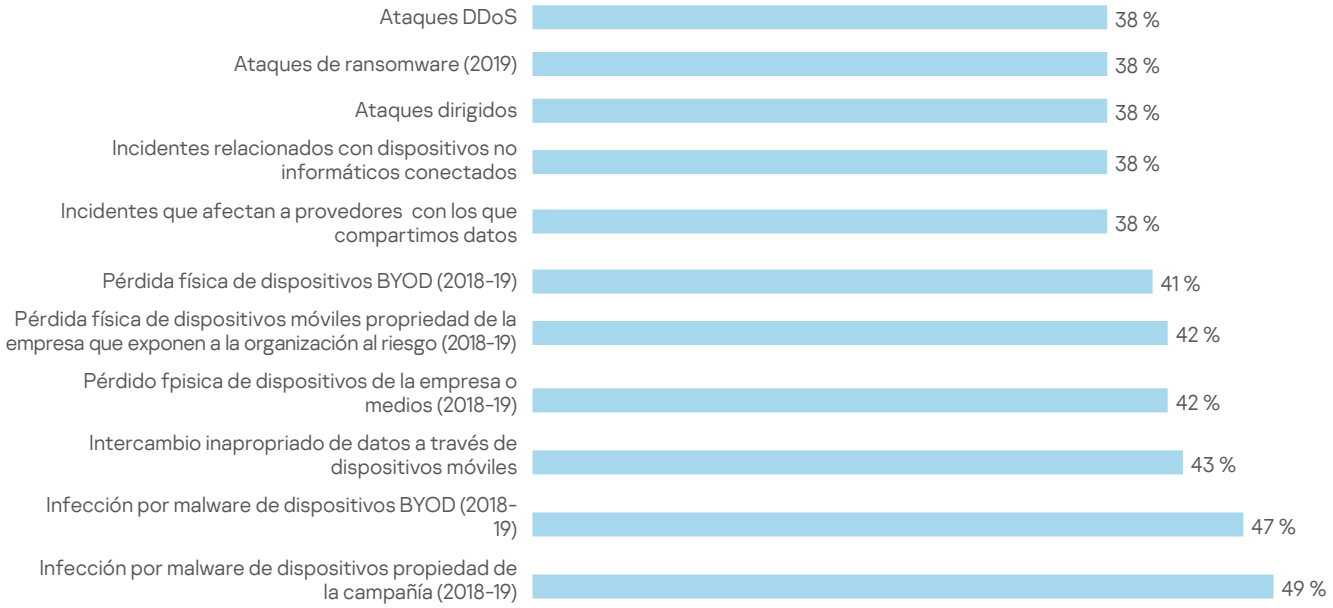


Figura 1. Los incidentes más frecuentes dirigidos a las PYMES

Incidentes mais frequentes direcionados a grandes corporações

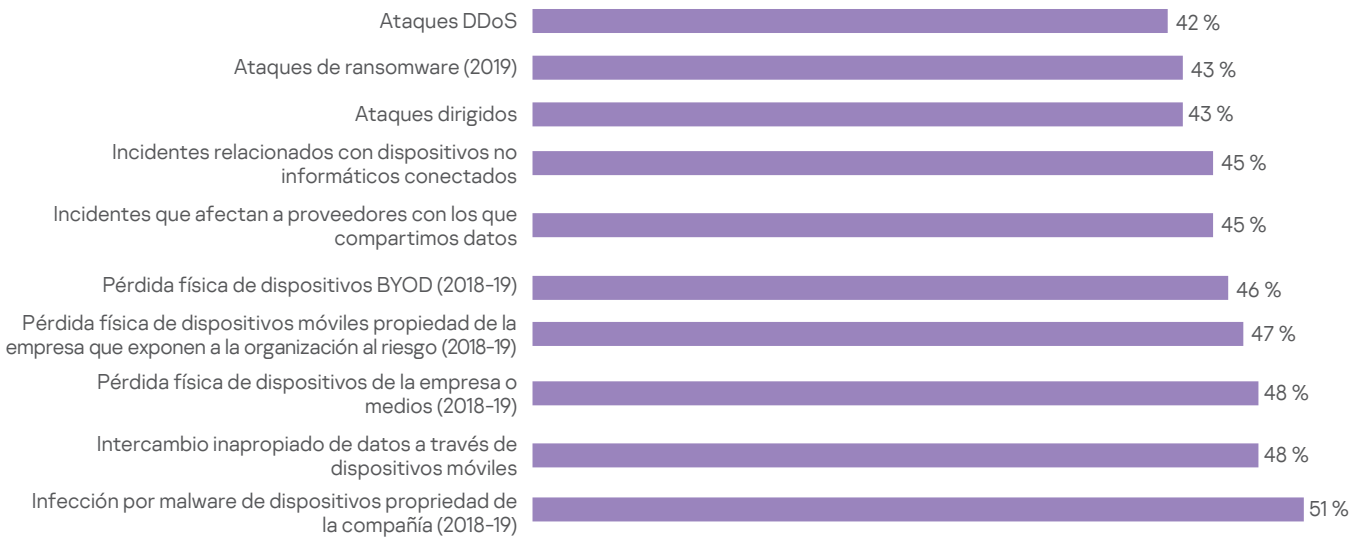


Figura 2. Los incidentes más frecuentes dirigidos a las empresas

Sorprendentemente, en el 2019 las violaciones a la seguridad de los datos más costosas para las PYMES en realidad no fueron los incidentes de seguridad más frecuentes. Este año, los tres ataques más costosos para las PYMES fueron incidentes que afectaron la infraestructura de las TI alojada por un tercero ($162 mil), ataques DDoS ($138 mil) y ataques dirigidos ($138 mil). Sin embargo, en términos de la frecuencia (Consulte la Figura 1), estos se ubican solamente en el 16.°, 12.° y 10.° lugar respectivamente en la lista de incidentes para la seguridad que se dirigen más frecuentemente a las PYMES

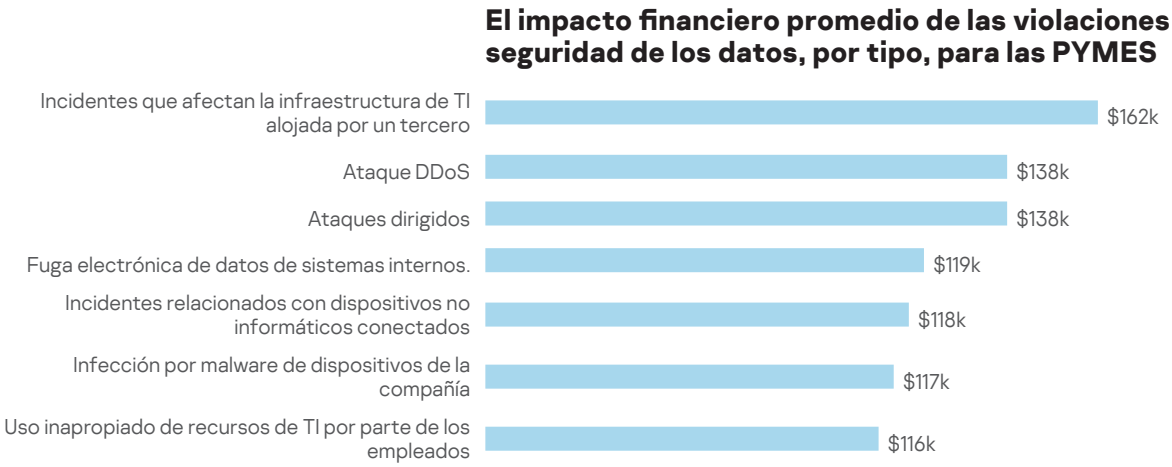


Figura 3. El impacto financiero promedio de las violaciones para la seguridad de los datos, por tipo, para las PYMES

Las empresas difieren aquí, con las tres vulneraciones de datos empresariales más costosas correspondientes a sus ataques más frecuentes: infección de malware de dispositivos propiedad de la empresa ($2.73m), incidentes que afectan a los proveedores con los que la empresa compartió datos con ($2.57 millones) y la pérdida física de dispositivos móviles propiedad de la empresa ($1.69 millones), todas se encuentran entre los seis primeros en la lista de incidentes de seguridad más frecuentes. El incidente de seguridad más costoso para las empresas en el 2019 fue la infección de malware de dispositivos propiedad de las empresas. En particular, los ataques dirigidos son solo el quinto más caro.

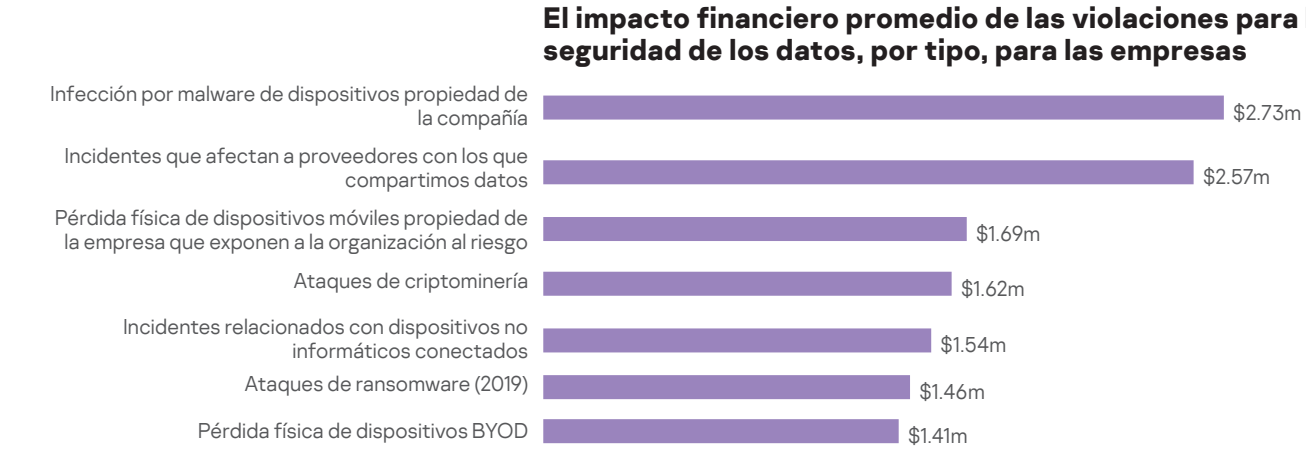


Figura 4. El impacto financiero promedio de las violaciones para la seguridad de los datos, por tipo, para las empresas

Sin embargo, cuando se trata de los incidentes que preocupan a las empresas, estas están más preocupadas por la pérdida de datos como resultado de un ataque dirigido (23%) en comparación con los virus y el malware (13 %). Del mismo modo, los ataques dirigidos son la principal preocupación de las PYMES (23 %), y la tercera forma más costosa de vulneración de datos para las PYME, en $138 mil.

Este año, el 47% de las PYMES y el 51 % de las empresas coincidieron en que cada vez es más difícil distinguir entre los ataques contra la seguridad generales o dirigidos. Esto provoca que sea más difícil para ellas detectar un incidente entre el "gris ruido" o evaluar los posibles daños que causó el incidente, lo cual probablemente es uno de los motivos por los que se están volviendo susceptibles al aumento en los niveles de amenazas por malware, tanto moderadas como avanzadas.

En general, el costo de las vulneraciones de los datos para las empresas aumentó, y el impacto financiero de su vulneración de datos promedio ha alcanzado $1.41 millones, y hasta $1.23 millones del año previo. Las mayores aumentos en los costos provienen de un crecimiento en la contratación de expertos externos para asegurar una vulneración ($170 mil), y del costo global en las pérdidas de las empresas ($163 mil). A este costo se añade la necesidad de una RP adicional para reparar el daño de la marca después de una vulneración ($161 mil).

En comparación, el costo total de las vulneraciones de datos para las PYME fue de $108 mil, esto se reduce desde $120 mil en el 2018 , con menos gastos en compensaciones ($5 mil), perdidas empresariales ($13 mil) y software e infraestructura ($13 mil).

1 La disminución del costo de las vulneraciones de datos para las PYME también estaría influida por el cambio en la muestra de la encuesta en el 2019. El cambio en la estructura de la muestra en algunos sectores verticales puede introducir necesidades específicas de los sectores verticales.

Las empresas pagan por las personas, las relaciones públicas y las oportunidades empresariales perdidas

Cuando una empresa, ya sea una empresa o una PYME, sufre un ataque contra la seguridad, el aumento de sus costos empresariales se debe a una serie de factores, entre los que se incluyen las sanciones y multas, el aumento de las primas de seguros, los nuevos programas informáticos y la capacitación. Sin embargo, de acuerdo con nuestra investigación, la experiencia externa y el poder de las personas son los motores clave para el aumento de los costos empresariales como resultado de un ciberataque en el 2019.

Desglose del impacto financiero promedio de una violación a la seguridad de los datos para las empresas

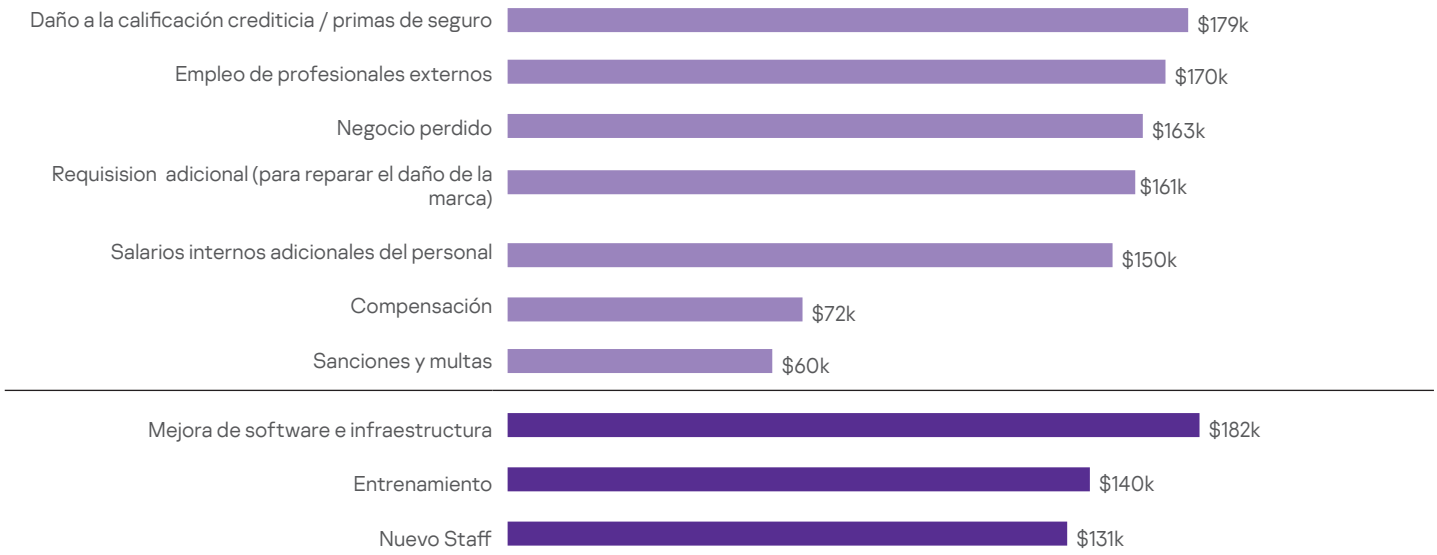


Figura 5. Desglose del impacto financiero promedio de una violación a la seguridad de los datos para las empresas

Desglose del impacto financiero promedio de una violación a la seguridad de los datos para las PYME

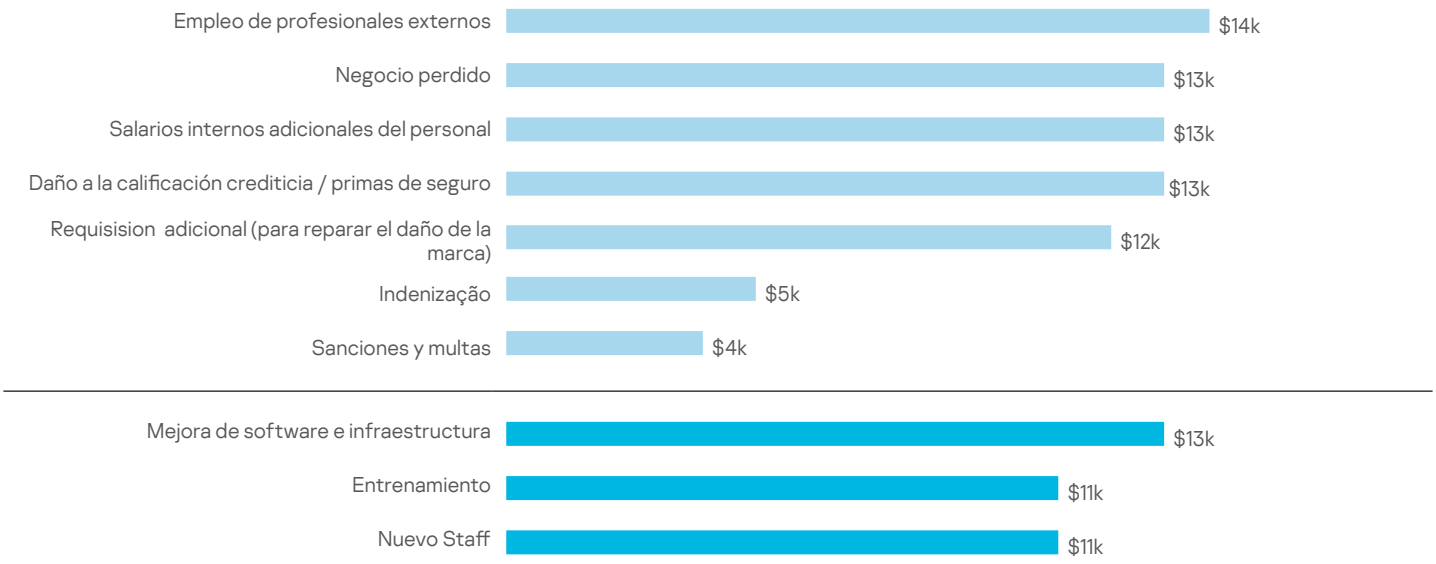


Figura 6. Desglose del impacto financiero promedio de una violación a la seguridad de los datos para las PYME

Para las empresas, el aumento entre años más significativo de los costos debido a la vulneración de datos se debe a la contratación de profesionales externos ($170 mil) y a la contratación de personal nuevo ($131 mil), que han aumentado 35 % y 24 %, respectivamente, desde el 2018.

Impacto financiero promedio de una violación a la seguridad de los datos para las empresas

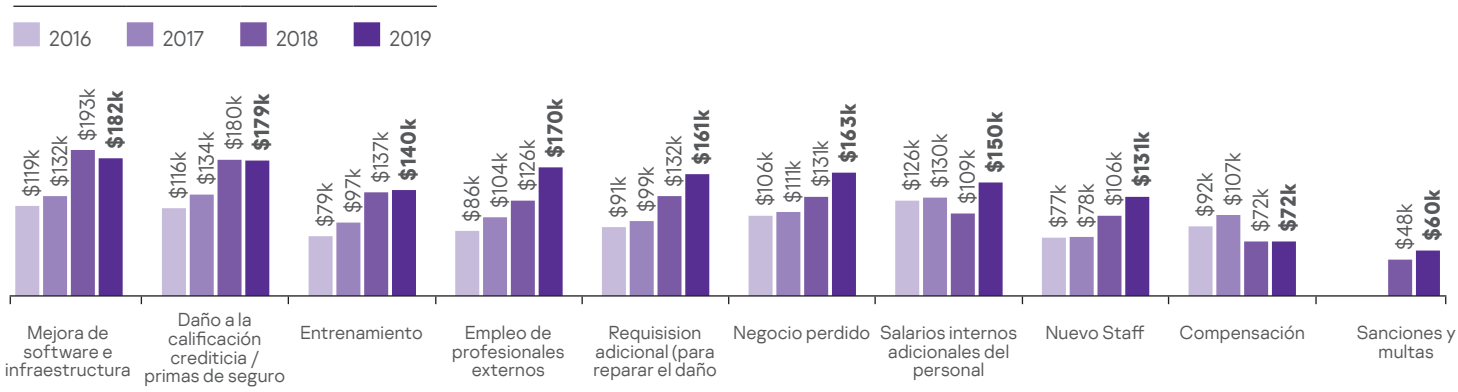


Figura 7. Impacto financiero promedio de una violación a la seguridad de los datos para las empresas

Mientras tanto, en el caso de las PYME, sus niveles generales de gastos relacionados con las amenazas están disminuyendo. Sin embargo, el gasto en personal nuevo se mantiene sin cambios $11 mil, lo cual demuestra que las PYME siguen invirtiendo en experiencia de los equipos para desarrollar un mayor grado de preparación en materia de seguridad.

Impacto financiero promedio de una violación a la seguridad de los datos para las PyMEs

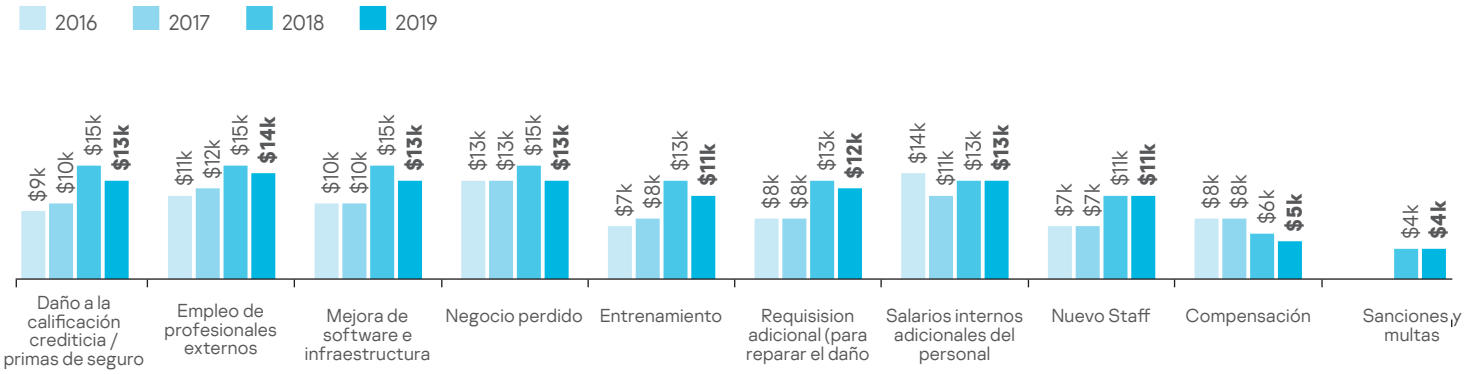


Figura 8. Impacto financiero promedio de una violación a la seguridad de los datos para las PyMEs

La pérdida de empresas nuevas o existentes también es un punto de costos notable para las empresas de todo tipo que sufren un incidente. Este año, la infección de malware encabezó la lista de las infracciones financieras más costosas para las empresas, mientras que las PYME fueron las más afectadas financieramente por los ataques dirigidos. En ambos casos, los mayores costos para cada industria procedían de la pérdida empresarial como resultado del ataque, lo que representaba $331 mil de la pérdida de ingresos de las empresas afectadas por una infección de malware, y $22 mil para PYMES que han sufrido un ataque selectivo.

Escándalos de RP e incidentes de amenazas: Con los escándalos de vulneración de datos corporativos que aparecen con mayor frecuencia en los titulares, el público es cada vez más consciente de los incidentes relacionados con la seguridad de sus datos. Esto puede conducir a una falta de confianza interna y pública en las empresas, lo cual obliga a que las empresas inviertan en relaciones públicas y administración de crisis para restablecer la confianza de los clientes en su marca. Nuestra encuesta reveló que el 31 % de las PYME y el 36 % de las empresas experimentaron problemas relacionados con las relaciones públicas en el 2019 debido a las vulneraciones de los datos, lo cual tuvo como resultado un impacto financiero adicional.

Cada vez más empresas están introduciendo políticas de acceso de terceros, utilizándolas para mitigar los riesgos de incidentes de seguridad, pero ¿realmente estas políticas hacen que las vulneraciones de datos sean menos probables? De acuerdo con nuestra investigación, 79 % de las empresas y 75 % de las PYMES pusieron en marcha políticas especiales para regular el acceso de los proveedores a sus datos.

¿Los terceros están sujetos a las políticas de seguridad de TI?

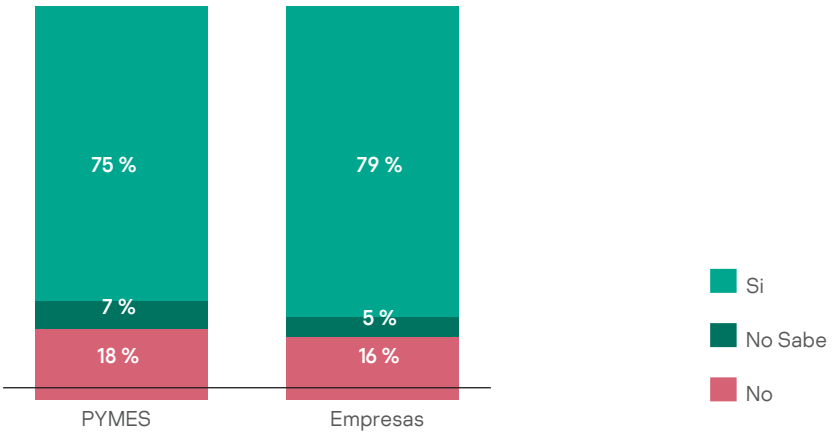


Figura 9. ¿Los terceros están sujetos a las políticas de seguridad de TI?

Figura 10. Políticas de acceso de terceros y vulneraciones de datos para las PYME

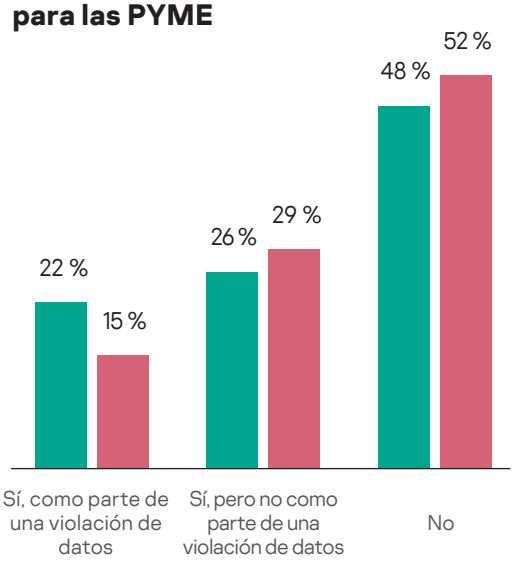


Figura 10. Políticas de acceso de terceros y vulneraciones de datos para las PYME

Figura 11. Políticas de acceso de terceros y vulneraciones de datos para empresas

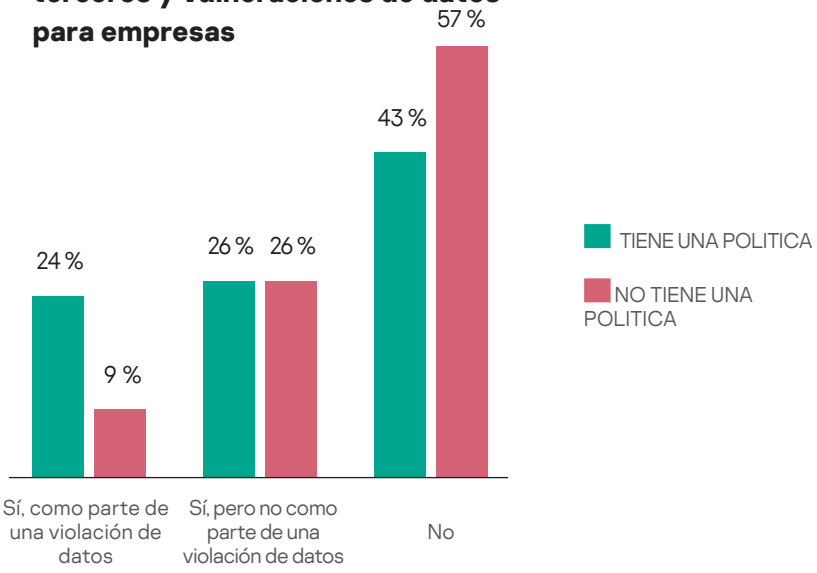


Figura 11. Políticas de acceso de terceros y vulneraciones de datos para empresas

Si bien las Figuras 10 y 11 anteriores revelan que estas políticas no han hecho que estos incidentes sean menos frecuentes, aumentaron la probabilidad de que una empresa reciba una compensación tras una vulneración de datos que involucre a un tercero. Tal como se muestra en la Figura 12 siguiente, el 71% de las empresas que cuentan con una política de terceros informaron que recibieron compensaciones en el 2019, en comparación con solo el 22% de las empresas que no contaban con una política similar.

Políticas de acceso de terceros y infracciónes de datos para pymes

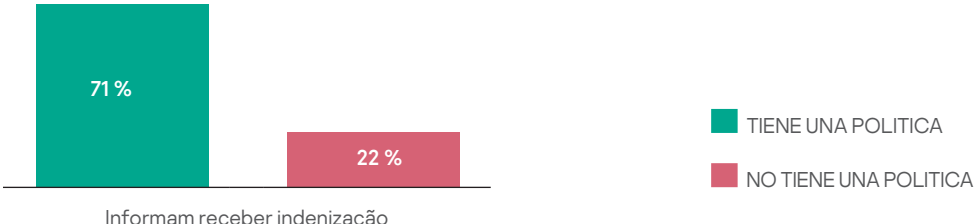
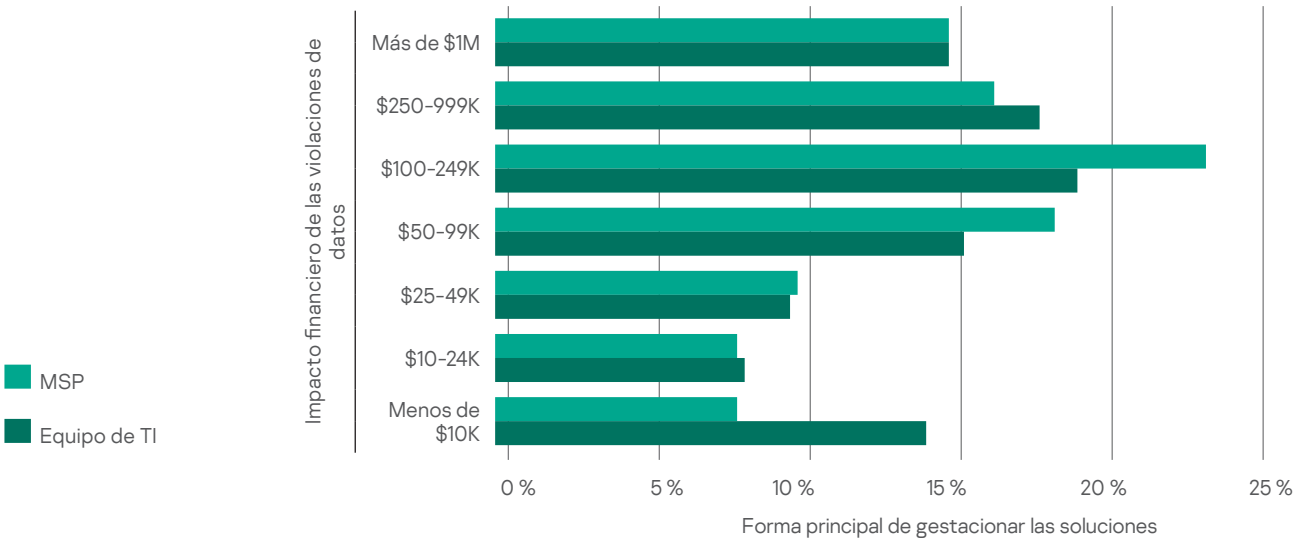


Figura 12. Políticas de acceso de terceros y compensación para empresas

Cuando se enfrentan a los crecientes costos de la seguridad de TI, muchas empresas consideran que la externalización de sus equipos de TI puede ayudarles a ahorrar dinero. Sin embargo, los proveedores de servicios de ciberseguridad descuidados o poco calificados pueden aumentar la factura de una empresa en caso de incidente. De todas las empresas que experimentaron una vulneración de datos con un impacto financiero de entre $100 mil y $249 mil, 23 % fueron empresas que utilizan un MSP subcontratado por motivos de seguridad, mientras que solo el 19 % eran empresas con personal de TI interno.

Impacto financiero total por las violaciones a la seguridad de los datos: subcontratación vs administración interna de la seguridad en TI



La consolidación conduce a ahorros: Las empresas que cuentan con RPD y SOC minimizan los costos por una vulneración

Las empresas con un responsable de la protección de datos (RPD) especializado tienen menos probabilidades de sufrir pérdidas financieras. El 34 % de las empresas con un RPD no vieron una pérdida de ingresos tras su ataque, en comparación con el 20 % de las empresas que no tienen esta función. Pero, por supuesto, aunque puede ayudar a reducir las pérdidas, tener esta función dedicada no proporcionará protección contra las vulneraciones de datos.

Para las empresas, disponer de un centro de operaciones de seguridad interno puede ayudar a reducir significativamente el costo de las vulneraciones de datos. En el 2019, esta cifra era de solo $675 mil para las empresas del SOC, frente a una media de $1.41 mill para las empresas en general.

Sin embargo, el simple hecho de nombrar al equipo de seguridad actual de su empresa como SOC no tiene el mismo efecto: nuestra encuesta mostró que si un SOC lleva a cabo funciones generales de seguridad de TI, no afecta el impacto financiero de una vulneración de datos. Se necesita capacitación, experiencia y sistemas dedicados para ver este ahorro de costos después de sufrir una vulneración.

¿Cómo están cambiando los presupuestos de seguridad de TI?

De acuerdo con Gartner, el gasto global en seguridad de las empresas está en aumento. Esto se confirma en la encuesta de este año, en la que el gasto de las PYMES alcanza los $267 mil en comparación con $256 mil en el 2018. Esto es aún más pronunciado en las empresas en las que su presupuesto de seguridad se ha duplicado, alcanzando $18.9 mill, en comparación con $8.9 mill el año pasado. Se espera que esta cifra aumente 11 % más en los próximos tres años.

La proporción del presupuesto de TI de las empresas asignada a la seguridad de TI

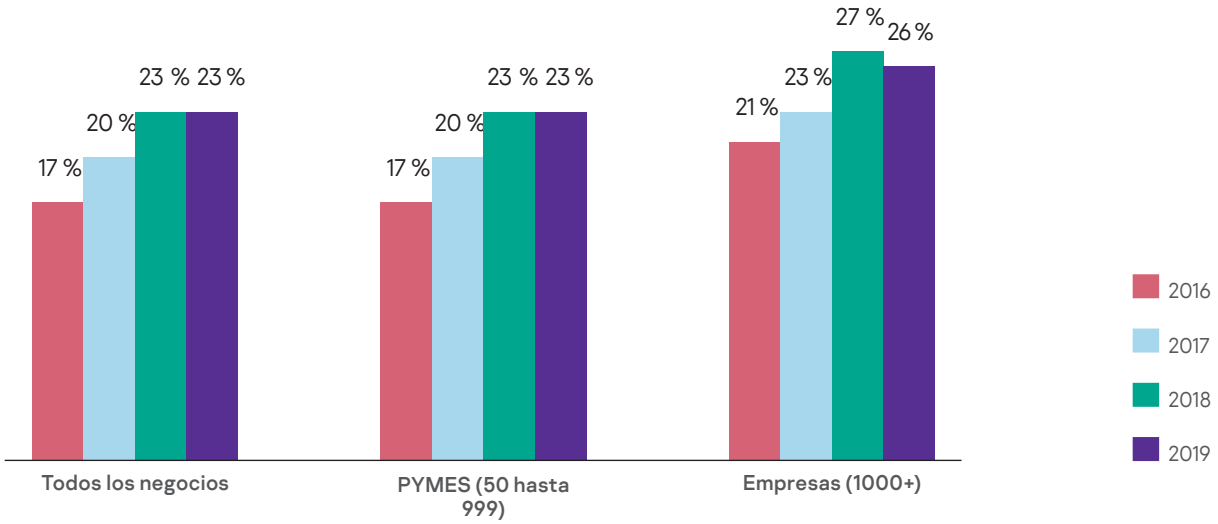


Figura 14. La proporción del presupuesto de TI de las empresas asignada a la seguridad de TI

A pesar de este aumento, los presupuestos de seguridad de TI no están absorbiendo un mayor porcentaje de los presupuestos de TI más amplios de las empresas. Este año, la proporción general de la seguridad de TI como porcentaje del gasto total en TI se ha mantenido incluso en las PYME con una tasa de crecimiento constante del 23 % en ambos años 2018 y 2019, e incluso ha disminuido ligeramente en el caso de las empresas, con un a 27 % del presupuesto total en el 2018 al 26 % en 2019.

Esto podría explicarse por las grandes inversiones que se realizaron en años anteriores. Varias vulneraciones de datos grandes, como la vulneración en la base de datos de la tarjeta de crédito Capital One, que reveló 106 millones datos de clientes, o el incidente de Facebook en el cual se vieron cientos de millones de registros de usuarios expuestos en un servidor en la nube de Amazon, el despliegue de RGDP y las transformaciones digitales en todos los sentidos catalizaron grandes inversiones en ciberseguridad empresarial en los últimos años. Ahora parece que las empresas han alcanzado un umbral relativamente estable de alrededor del 25 % y podrían estar empezar a reevaluar los beneficios de estas inversiones anteriores antes de seguir mejorando su ciberseguridad.

Dónde invierten las PYMES y las empresas su presupuesto de TI

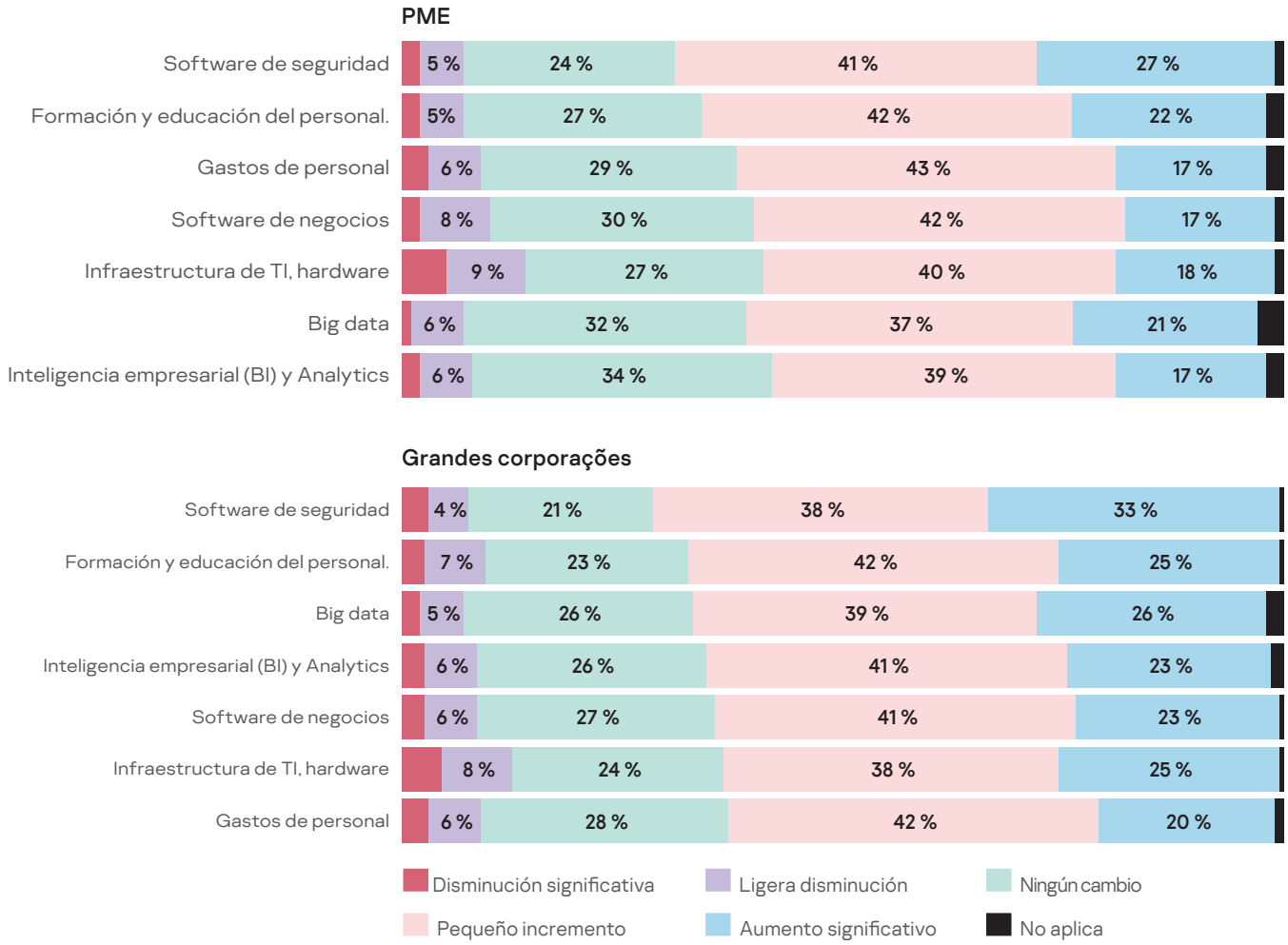


Figura 15. Dónde invierten las PYMES y las empresas su presupuesto de TI

Cuando se trata de invertir para el futuro, las empresas utilizan principalmente su presupuesto de TI para aumentar sus inversiones en formación y educación del personal de software de ciberseguridad. Como se muestra en la Figura 15, el 33 % de las empresas y el 27 % de las PYMES han visto un aumento significativo en las inversiones para software de seguridad. Tanto las empresas como las PYME también han realizado importantes inversiones en programas de grandes bases de datos (26 % empresas, 21% PYME) y la capacitación y educación del personal (25 % empresas, 22% PYME).

La participación de los ejecutivos de nivel C conduce a un aumento de los presupuestos de ciberseguridad

En las empresas donde los ejecutivos de nivel C están muy involucrados en el proceso de toma de decisiones de TI, el presupuesto medio de seguridad de TI supera los $5 mill, tanto para las empresas como para las PYME. Esto es en comparación con un presupuesto promedio de $10 mil a $12 mil en empresas donde la dirección ejecutiva solo participa parcialmente.

Gasto en seguridad de TI y participación en el nivel C

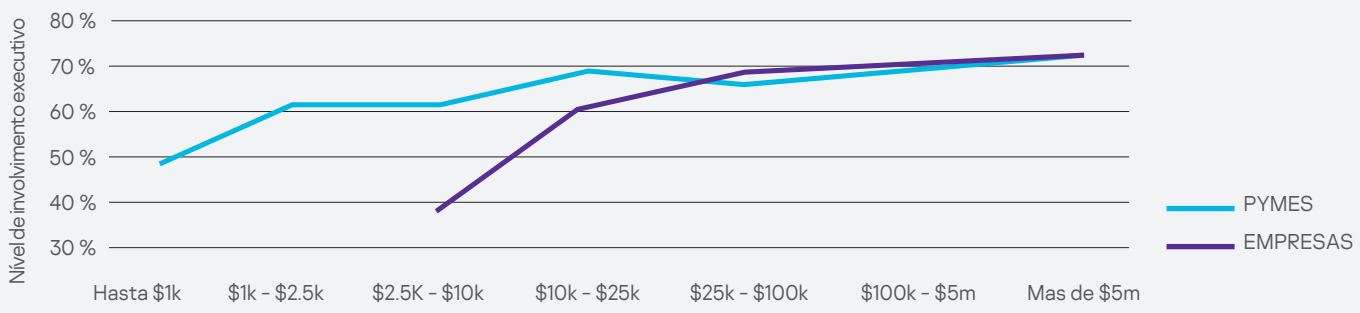


Figura 16. Gasto en seguridad de TI y participación en el nivel C

Conclusión

Es escencial que las empresas continuén invirtiendo y reconsiderando sus procesos de seguridad de TI para que estén un paso por delante de las tasas de crescimiento de los ataques cibernéticos y limiten las pérdidas financieras incurridas.

Nuestro informe destaca que cuando una empresa invierte en personal, recursos y procesos, está en mejores condiciones de hacer frente a los resultados y pérdidas financieras de los incidentes de ciberseguridad.

Las empresas que instalaron un DPO experto, incorporando un SOC interno, o que han introducido una regulación para terceros que tienen acceso a los datos de la empresa, ven una disminución de las pérdidas financieras, o la capacidad de recuperar algunos costos, después de una vulneración de los datos.

Cada vez más, los líderes empresariales también están involucrandose en el proceso de toma de decisiones de seguridad de TI. Esto se traduce en mayores presupuestos para la seguridad de TI y una mayor preparación para la administración de incidentes. Por lo tanto, tanto para las PYME como para las empresas que buscan una mayor inversión en sus actividades de ciberseguridad, es fundamental contar con el interés del nivel ejecutivo.

Sin embargo, no todas las empresas están tan preparadas como deberían para la amenaza de un ataque. En general, la percepción general entre las empresas es que el número de amenazas en sus redes está disminuyendo, a pesar de que los incidentes de todo tipo siguen aumentando en el 2019. Dado que solo una de cada diez (el 12%) empresas está preocupada por las infecciones de malware, a pesar de que se trata del incidente de seguridad más costoso, está claro que las empresas deben ser más conscientes de cuánto les están costando estos ataques a su empresa, independientemente de la frecuencia.

Del mismo modo, el porcentaje del presupuesto dedicado a la seguridad de TI se mantuvo estático en comparación con el año pasado, lo que posiblemente demuestra que la inversión en seguridad de TI comenzó a estancarse mientras las empresas consideran su próximo enfoque. Dando el riesgo continuo de ataques, en vez de esperar, las empresas y las PYME deberían seguir invirtiendo en su futuro ahora para que estén preparadas para la siguiente generación de incidentes de seguridad. Es vital que las empresas sigan invirtiendo y replanteando sus procesos de seguridad de TI para estar un paso por delante de las crecientes tasas de ciberataques y para limitar las pérdidas financieras en las que puedan incurrir.

Es evidente que para muchas empresas, cuando se trata de protegerse de las amenazas de la ciberseguridad, resulta difícil conseguir la experiencia adecuada. Por eso, ya sea de manera interna o externa mediante un proveedor, dar prioridad e invertir en conocimientos de ciberseguridad es esencial para mantenerse seguro.

Noticias sobre amenazas cibernéticas: www.securelist.com
Noticias sobre seguridad de TI: business.kaspersky.com/

kaspersky BRING ON THE FUTURE

www.kaspersky.com