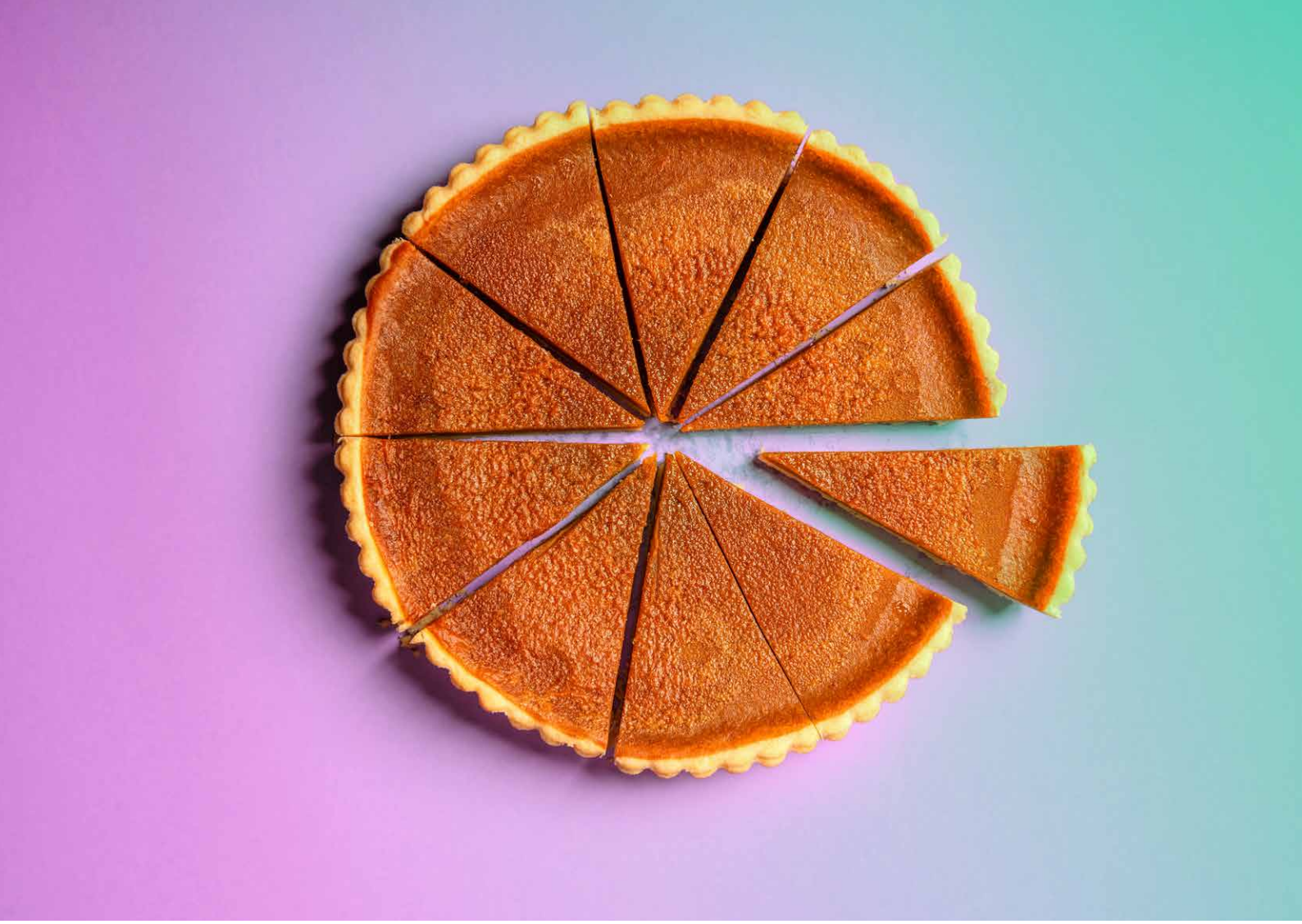


Ajuste de las inversiones: Modificación de los presupuestos de TI con el cambio en las prioridades sobre la seguridad

Economía en la seguridad de las TI en el 2020: Resumen ejecutivo

kaspersky BRING ON THE FUTURE

Obtenga más información en kaspersky.com

Contenido

Introducción

El riesgo contra la recompensa es una línea muy fina cualquier empresa debe seguir. Pero ya no más cuando se trata de la seguridad de su personal y de los valiosos datos que contiene.

Dado que el 2020 ha sido un año de enormes cambios e incertidumbre para todas las empresas, grandes y pequeñas, nunca había sido más importante para los líderes empresariales revisar las prioridades de seguridad de la TI y garantizar que los procedimientos y los presupuestos se ajusten, para generar prosperidad y crecimiento en el futuro. Investigaciones recientes de Gartner apoyan esta tendencia y predicen que el 75% de los directores generales serán personalmente responsables de los incidentes de ciberseguridad física para el 2024.

En la última década, gracias a la investigación en curso de Kaspersky sobre la economía en la seguridad de la TI, hemos visto un gran cambio en las prioridades cuando se trata de proteger a las empresas, junto con enormes avances en las soluciones de ciberseguridad, inteligencia y educación. Pero, ¿qué impacto tuvo el aumento de la dependencia de la tecnología y la colaboración en línea para los gastos y las perspectivas actuales en seguridad solo en el último año?

En este primer informe, que pertenece a una serie de varios, se analiza la economía de la seguridad de la TI, se profundiza en los principales hallazgos que generó la investigación en este año y se prepara el escenario para los costos, desafíos y los cambios que afectan a los responsables de tomar decisiones de seguridad de la TI en la actualidad. Curiosamente, el tamaño de los presupuestos de seguridad de TI sigue siendo bastante plano, en comparación con los datos del 2019, pero su proporción dentro del gasto total en TI está aumentando. Esto sugiere una posición elevada para las medidas de ciberseguridad en torno a la mesa donde se toman las decisiones cuando se trata de mantener en línea los sistemas de misión crítica, y proteger a las personas y los datos.

Metodología

La encuesta acerca de los Riesgos de Seguridad de TI Corporativa (ITSRS) de Kaspersky está ahora en su décimo año.

En junio del 2020 se entrevistó a un total de 5,266 personas encargadas de tomar decisiones empresariales sobre la TI en 31 países. Se le preguntó a los encuestados sobre el estado de la seguridad de TI en 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.

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.

Tenga en cuenta que aunque se hicieron todos los esfuerzos posibles para que los resultados sean comparables de un año al otro, la investigación ha sido objeto de algunas revisiones durante el 2020, lo cual significa que no todos los resultados son directamente comparables. El público objetivo sigue siendo el mismo, pero se revisaron las preguntas de selección para identificar de manera más confiable a las personas que poseen la experiencia y los conocimientos más relevantes. Esto aumentó significativamente la proporción de encuestados que tienes funciones de especialistas en TI y en seguridad de la TI, de un 33% en el 2019 a un 62% en el 2020.

Además, aunque el alcance del estudio se ha mantenido a nivel mundial, en el 2019 se incluyeron menos países (en particular, China estuvo ausente). La investigación del 2020 presenta una base más amplia de países (a partir del 2018 y 2017), y también se agregaron Polonia y Kazajistán a la lista.

Resultados principales

Costo de las vulneraciones de los datos

$101,000 para las PYMES

$1.09 millones para las empresas

Presupuesto de seguridad de TI

$275,000 para las PYMES

$14 Millones para las empresas

- El costo promedio de las vulneraciones de datos disminuyó a $101,000 dólares para las PYMES y $1.09 millones de dólares para las empresas en el 2020, en comparación con $108,000 y $1.41 millones de dólares, respectivamente, en el 2019
- La proporción de la seguridad de la TI en los presupuestos generales de TI aumentó del 23% en el 2019 al 26% en el 2020, en el caso de las PYMES, y del 26% en el 2019 al 29% en el 2020 en el caso de las empresas
- Esto a pesar de la disminución del gasto generado de $4.9 millones de dólares para las empresas (de $18.9 millones de dólares en el 2019 a $14 millones de dólares en el 2020) y un ligero aumento de $8,000 dólares en el gasto para las PYMES (de $267,000 dólares en el 2019 a $275,000 dólares en el 2020)
- Hace tres años, un tercio de los responsables de la toma de decisiones (el 33% de las PYMES y el 35% de las empresas) admitió que tardaban varios meses en detectar una vulneración de los datos. En el 2020, eso se redujo drásticamente a solo el 13% de las empresas
- Los principales desafíos que preocupan a los equipos de seguridad de TI este año son muy específicos: los ataques de phishing a los clientes (50% de las PYMES y 48% de las empresas) y los ataques a las filiales (44% de las PYMES y 42% de las empresas)
- Los principales controladores para la reducción del gasto en seguridad de TI incluyen un tercio (32%) de los altos directivos de las empresas, quienes no ven razón para invertir tanto en el futuro, y el 29% de las PYMES que recortan los gastos generales de la empresa y optimizan sus presupuestos

El costo variable de las vulneraciones de datos

Uno de los principales controladores y motivadores para gastar en seguridad de TI es principalmente el costo para la empresa, si no se trata de usted, y ocurre cuando hay una vulneración de los datos. Hay muchos ejemplos de empresas que ponen en riesgo a sus clientes y su propia reputación cuando sufren de una vulneración de los datos.

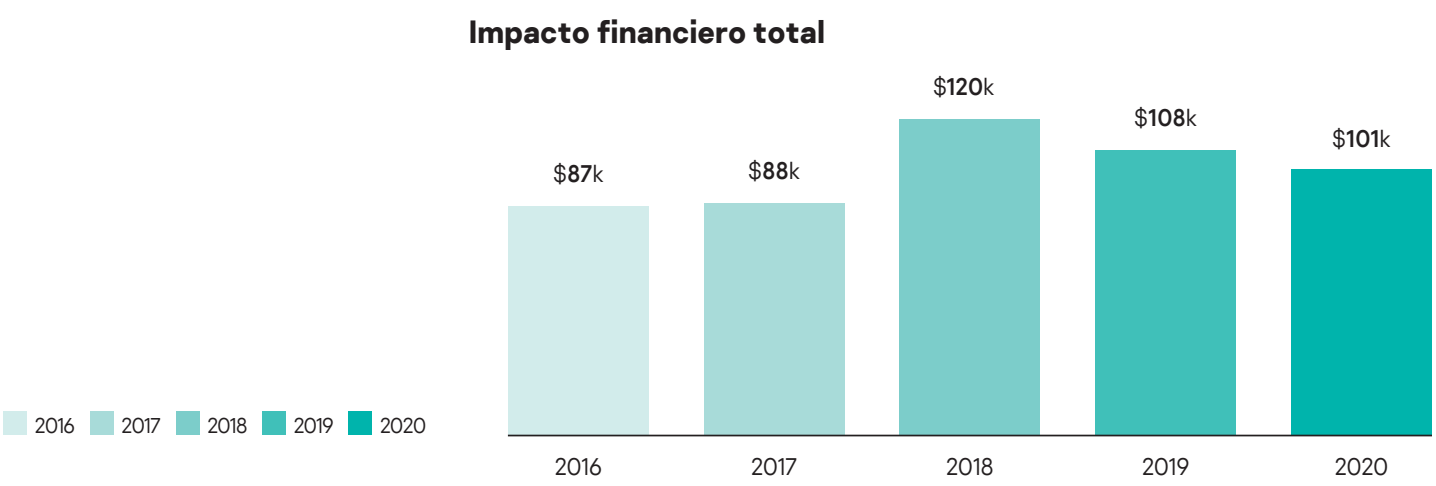
El hackeo que ocurrió en mayo del 2020 tuvo como objetivo a Blackbaud, uno de los mayores proveedores de software de administración de la educación, recaudación de fondos y administración financiera del mundo, el cual afectó a más de 10 universidades en el Reino Unido, Estados Unidos y Canadá, a las que les robaron datos de estudiantes y exalumnos después de que los hackers atacaran a un proveedor de computación en la nube. La cadena hotelera Marriot fue de nuevo objeto de una vulneración de la seguridad en marzo del 2020, en la cual se revelaron los datos de más de 5.2 millones de huéspedes del hotel, que obtuvieron los hackers en el transcurso de un mes antes de que se descubriera la vulneración.

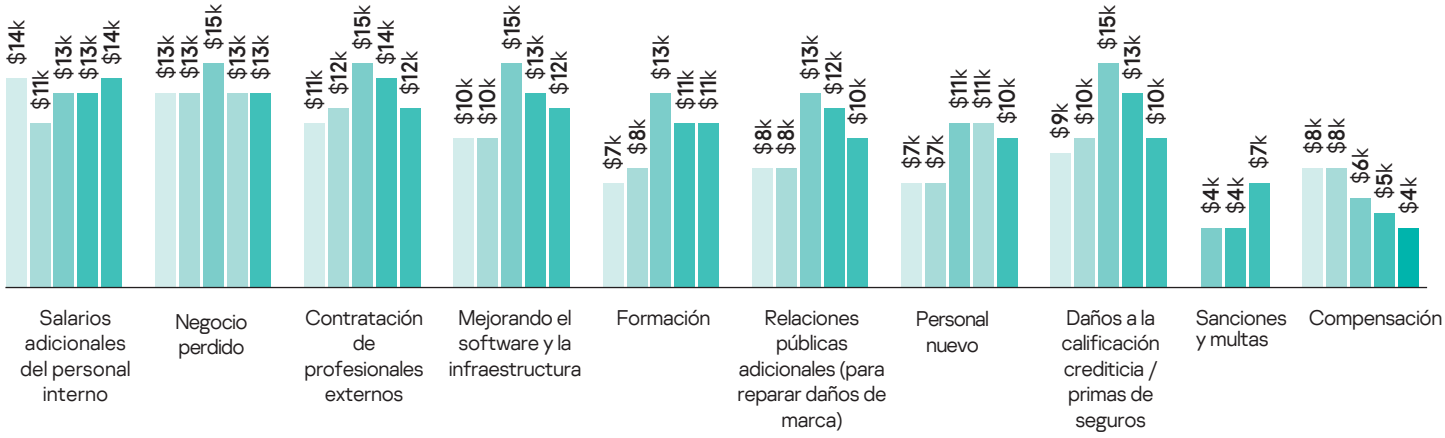
Además de tener un efecto perjudicial en la confianza del consumidor y de empañar su reputación, estas empresas y muchas otras como ellas sufrieron enormes costos e implicaciones financieras asociadas a una vulneración de seguridad que hicieron aún más difícil recuperarse, especialmente para pequeñas empresas con presupuestos más pequeños y recursos limitados.

La buena noticia es que en nuestra investigación se determinó que los costos de una vulneración de los datos están disminuyendo, tanto para las PYMES como para las empresas, aunque el impacto financiero sigue aumentando en el sector de los servicios financieros, tal vez debido a la naturaleza altamente regulada del sector y a un alcance más amplio en las consecuencias del incumplimiento.

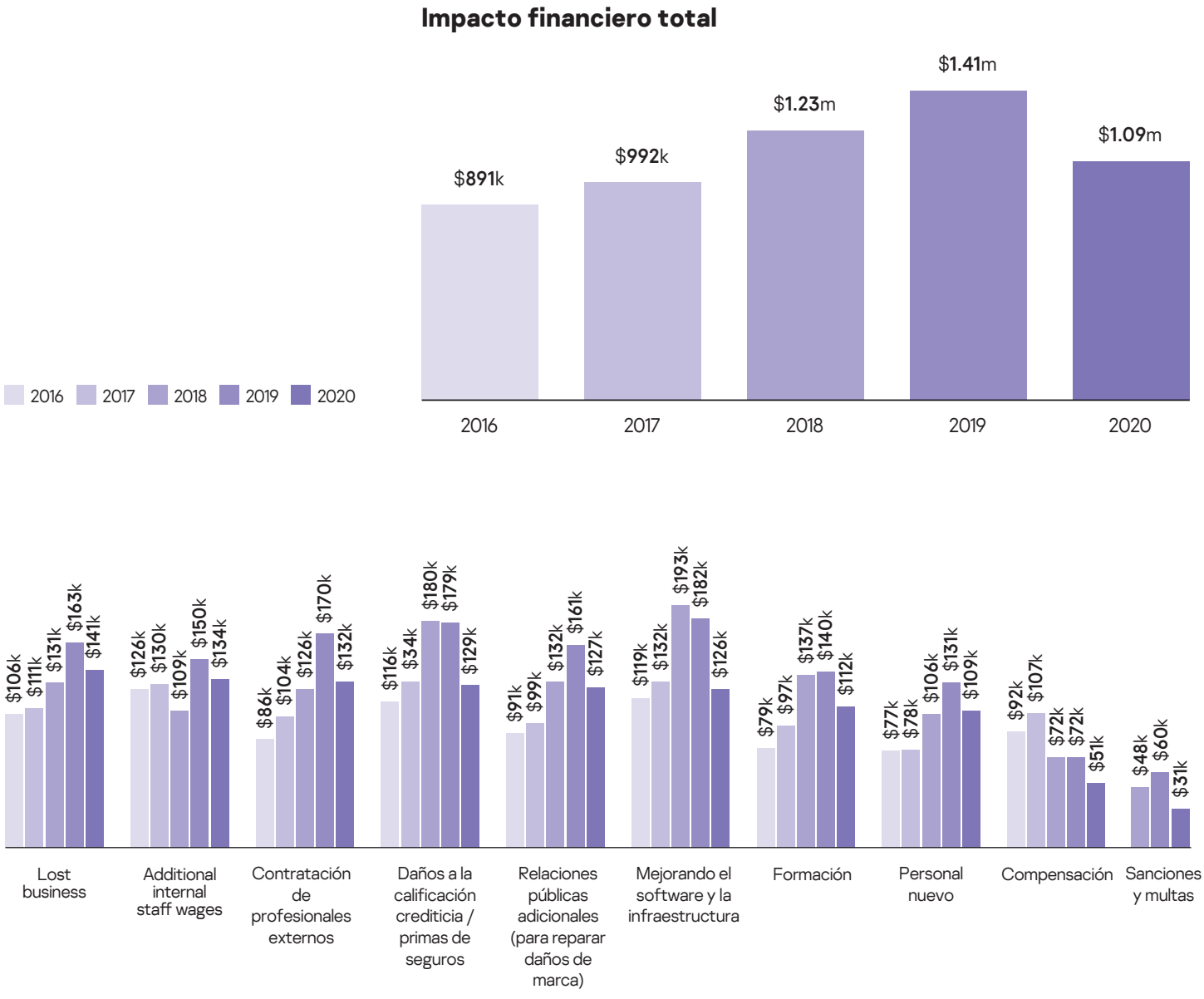
El impacto financiero promedio de una vulneración de los datos para las PYMES que han sufrido al menos una, es de $101,000 dólares (en comparación con $108,000 dólares en el 2019), y para las empresas asciende a $1.09 millones de dólares (en comparación con $1.41 millones de dólares en el 2019). Los tres principales costos que componen esta cifra general para todas las empresas se traducen como salarios adicionales del personal interno, pérdida de negocios y la necesidad de emplear profesionales externos para solucionar una vulneración de datos en cuanto ocurra.

Gráfica 1: Impacto financiero total promedio de una vulneración de datos para las PYMES





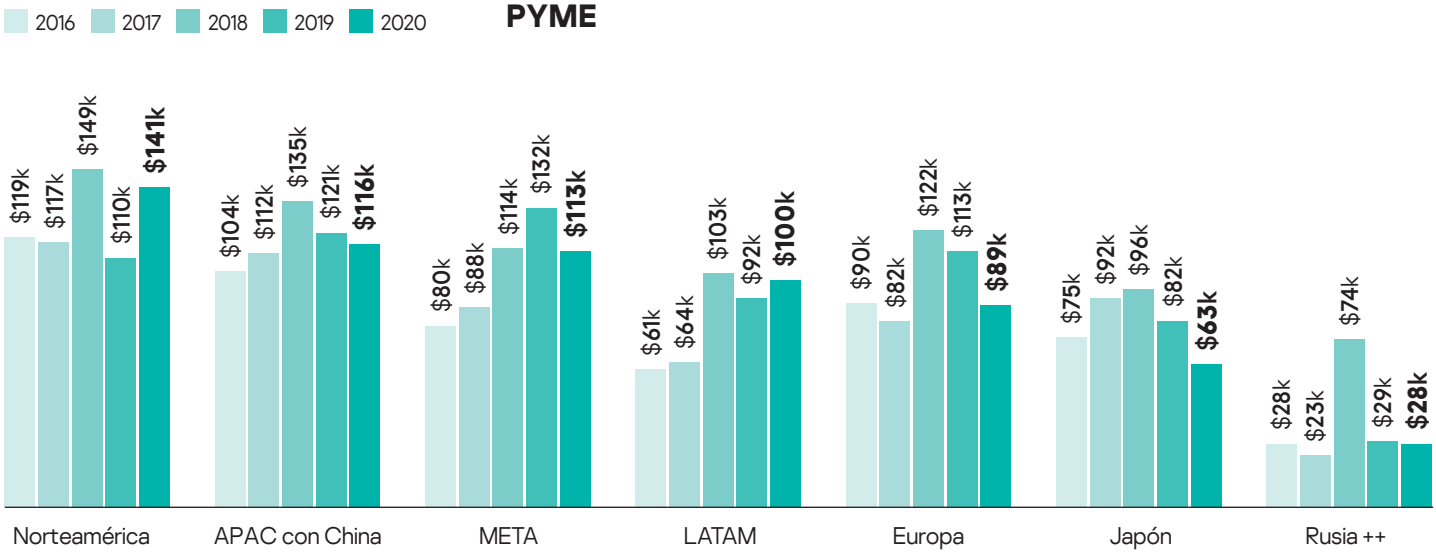
Gráfica 2: Impacto financiero total promedio de una vulneración de datos para las empresas

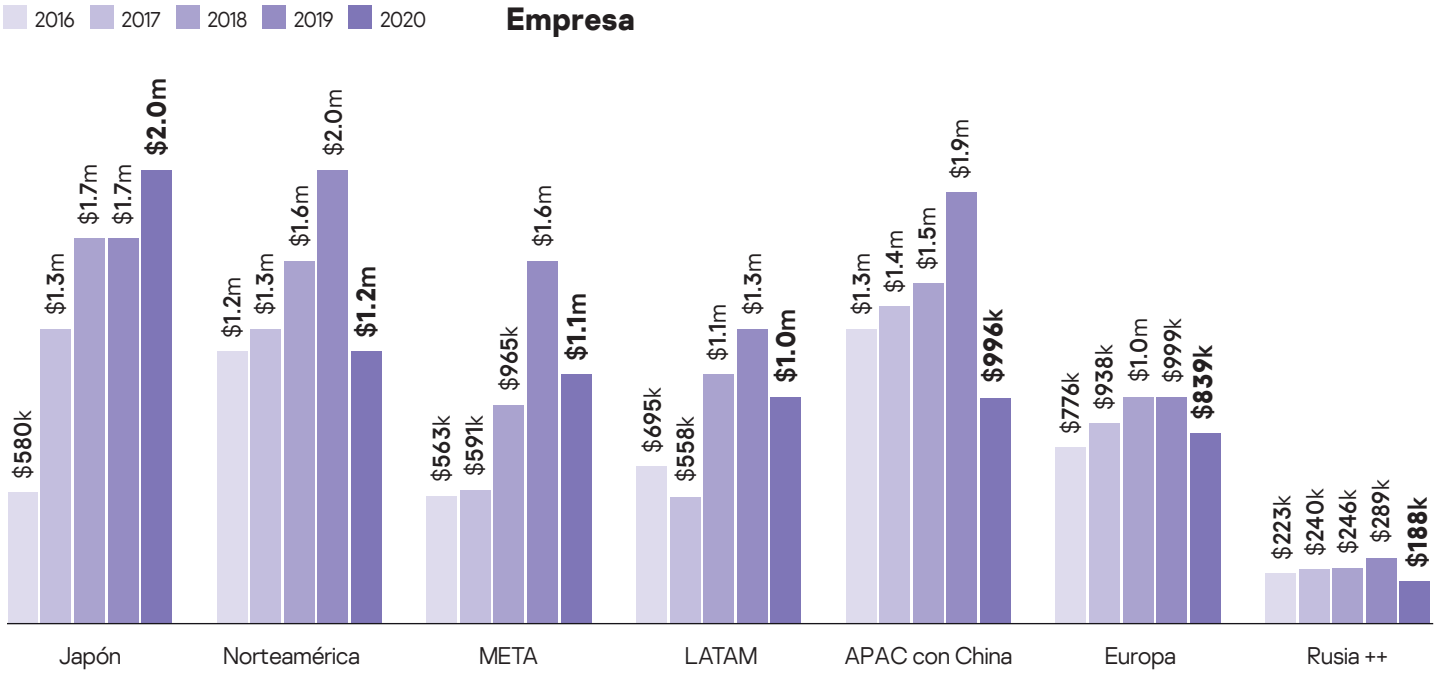


Variaciones regionales

La mayoría de las regiones del mundo siguen una pauta similar, relacionada con la disminución de los costos asociados a una vulneración de los datos en el 2020, con excepción de América del Norte y LATAM, donde los costos entre las PYMES han aumentado, y en Japón, donde el impacto financiero ha aumentado para las empresas.

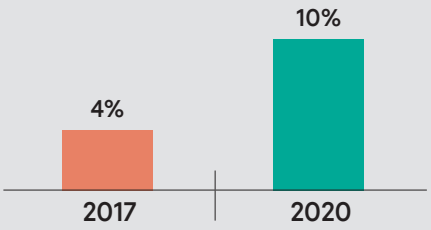
Gráfica 3: Impacto financiero promedio de una vulneración de los datos a través de las regiones





El valor de reaccionar rápidamente

Empresas que detectan los ataques casi instantáneamente



Una de las principales razones de esta constante disminución de los costos en todo el mundo podría deberse a las mejoras introducidas en la detección de los ataques y, por lo tanto, a la reducción al mínimo de los efectos de una vulneración en las empresas. En nuestra investigación se encontró que, tanto el sector de las PYMES como el empresarial, han visto acortarse significativamente en los últimos años la cantidad de tiempo que tardan en detectar y responder a las vulneraciones de los datos.

En el 2017, solo el 4% de las empresas disponían de un sistema, como la detección y respuesta para endpoints o la prevención de intrusiones en la red, que podía alertarles de una vulneración de forma casi instantánea. Hoy esa cifra ha aumentado a uno de cada diez (10%). En el 2017, un tercio de los responsables (el 33% de las PYMES y el 35% de las empresas) admitieron que tardaron varios meses en detectar una vulneración. En el 2020, eso se redujo drásticamente a solo el 13% de las empresas.

En los últimos tres años, las empresas cambiaron su forma de responder y reaccionar a la seguridad de los datos y se dieron cuenta del valor de invertir presupuestos en soluciones de detección y respuesta, en vez de reaccionar y pagar una prima financiera cuando ocurre una vulneración.

Consolidación de los principales retos de la ciberseguridad

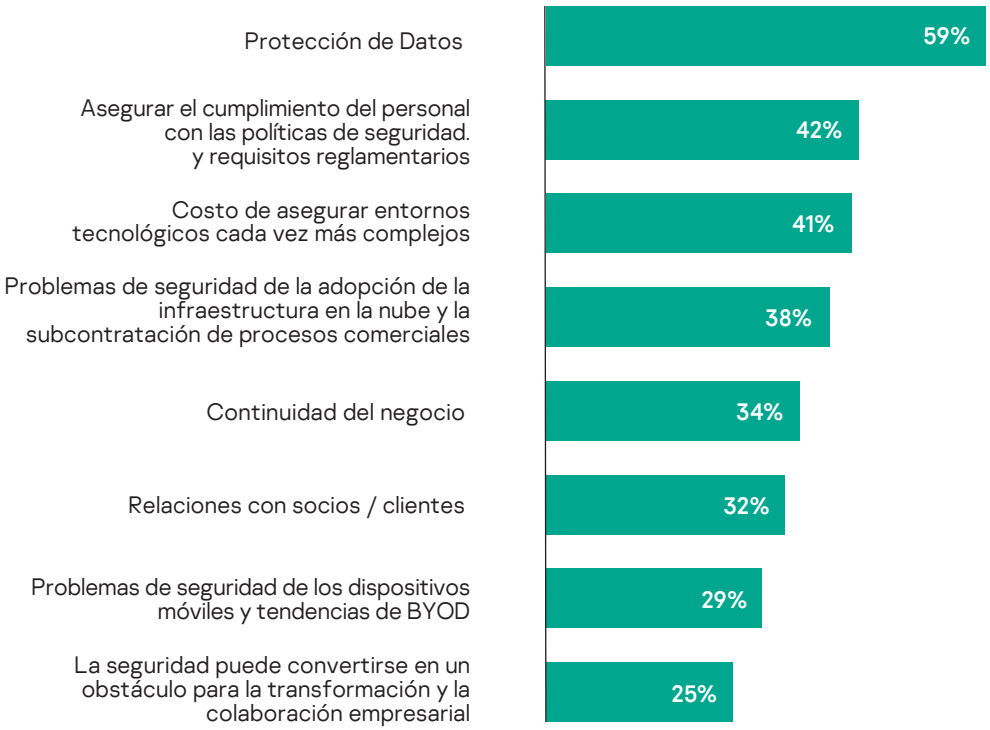
Para todas las empresas, los tres desafíos más importantes en cuanto a temas de seguridad de TI se refiere, no han cambiado en los últimos 12 meses. La protección de los datos (59%), la garantía del cumplimiento de las políticas de seguridad y los reglamentos de la industria (42%), y el costo de proteger entornos tecnológicos cada vez más complejos (41%), son las principales preocupaciones de los encargados de tomar decisiones.

En el entorno actual del COVID-19, no es sorprendente ver que estos factores siguen encabezando la lista de preocupaciones. Las empresas de todo el mundo han cambiado sus modelos de operación y han trasladado a toda su fuerza laboral al trabajo a distancia, lo cual ejerció una presión adicional en las empresas para garantizar que sus sistemas estén protegidos y cumplan con las normas, y de que sus extensos entornos de TI sigan siendo seguros. Con más gente trabajando de forma remota y fuera de la relativa comodidad y seguridad de un entorno de oficina, esto también hace que las personas tengan la responsabilidad de seguir actuando de forma responsable cuando utilizan dispositivos laborales y personales.

Cuando profundizamos en las preocupaciones específicas de la ciberseguridad, obtenemos algunas percepciones muy significativas sobre cómo han cambiado. El phishing y los ataques de ingeniería social a las cuentas de los clientes son el principal desafío mencionado por la mitad de las PYMES (50%) y empresas (48%). A esto se unen las preocupaciones con respecto a los ataques a las filiales (44% para las PYMES y 42% para las empresas).

Sin duda alguna, la pandemia ha desempeñado un papel en el aumento y, de hecho, en la confirmación de estos temores, ya que nuestros propios expertos han descubierto que los ataques de phishing se han vuelto más selectivos y con un enfoque más diverso durante la pandemia.

Gráfica 4: Principales preocupaciones en seguridad de TI para todas las empresas



Rango de preocupación

2017	2018	2019	2020
1st	1st	1st	1st
5th	3rd	2nd	2nd
4th	6th	3rd	3rd
2nd	2nd	5th	4th
3rd	5th	4th	5th
6th	4th	6th	6th
7th	7th	7th	7th
N/A	N/A	8th	8th

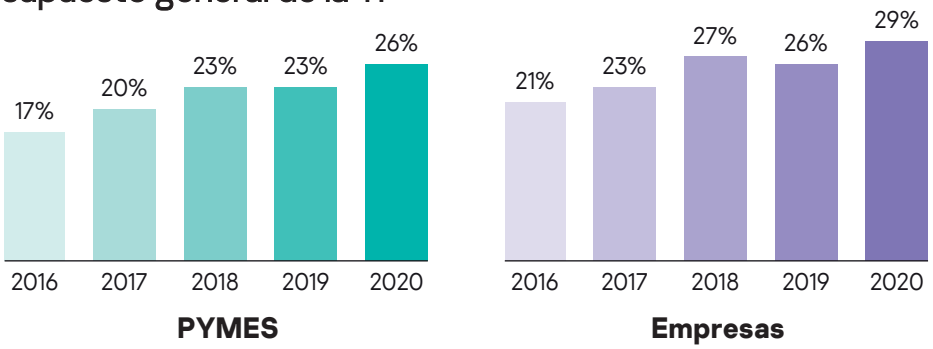
Reajuste en los presupuestos de seguridad de la TI

La planificación de un presupuesto puede ser un punto importante para muchas empresas, con prioridades y parámetros variables, donde todos tienen un papel que desempeñar. Cuando se trata de asignar el gasto en TI, los líderes empresariales ya indicaron la interrupción digital y tecnológica como sus principales prioridades para el 2020 según Gartner, incluso antes de que la pandemia aumentara y la tecnología se convirtiera en el principal eje de casi todas las empresas.

En el 2020, las empresas llevaron a cabo cambios significativos y rápidos en sus operaciones cotidianas para seguir funcionando y mantener su capacidad de recuperación ante la evolución de los desafíos. Por lo tanto, hemos visto cambios en los objetivos para el gasto en seguridad de TI en los últimos 12 meses, a medida que cambian las prioridades empresariales y los presupuestos disponibles se vuelven aún más estrechos y analizados.

Es interesante que el "valor" de los presupuestos de seguridad de TI siga aumentando, pero no en términos monetarios. Como parte del gasto total en TI, la proporción que se asigna a la seguridad está aumentando en tamaño. En el 2019, el 23% del presupuesto de TI para las PYMES se asignó a la seguridad, en comparación con el 26% en el 2020. Dentro de las empresas, el porcentaje aumentó del 26% al 29% en los últimos 12 meses. Sin embargo, cuando observamos las cifras específicas, los presupuestos permanecen en gran medida estáticos (para las PYMES) o disminuyen (para las empresas). Estos hallazgos coinciden con las recientes cifras de Gartner, en las que se sugiere que el gasto mundial en TI disminuirá un 8% en el 2020 debido al impacto de la pandemia del COVID-19.

Gráfica 5: Presupuesto de seguridad de la TI como parte del presupuesto general de la TI



	PYMES 2018	PYMES 2019	PYMES 2020	Empresas 2018	Empresas 2019	Empresas 2020
Presupuesto promedio de TI	$1.1m	$1.2m	$1.1m	$42.1m	$74.1m	$54.3m
Presupuesto promedio de seguridad de TI	$256k	$267k	$275k	$10.2m	$18.9m	$14.0m
Crecimiento esperado del presupuesto de seguridad de TI (más de tres años)	+14%	+11%	+12%	+15%	+11%	+11%

Las prioridades de inversión

Más de dos tercios (71%) de las PYMES y empresas planean aumentar la inversión en seguridad de TI durante los próximos tres años, mientras que el 17% planea mantenerla sin cambios. Para aquellas PYMES que buscan aumentar su gasto en seguridad, este se citó como uno de los tres principales impulsores que se desean aumentar para responder a una mayor complejidad en la infraestructura de la TI (43% en comparación con el 36% del año anterior). De acuerdo con las conclusiones destacadas anteriormente en el informe, a esto le sigue la necesidad de mejorar la experiencia en seguridad de especialistas internos (39%) y para un tercio (34%) de las PYMES, en el nivel superior de administración se desean aumentar los presupuestos para mejorar las defensas de la empresa.

El deseo de las empresas de aumentar los presupuestos de seguridad muestra una tendencia similar. El 43% afirma que las razones principales son el aumento de la complejidad de la infraestructura de TI, la mejora de los conocimientos técnicos internos (41%) y el deseo de la alta dirección de contar con defensas más sólidas (34%).

En el caso de quienes invierten en tecnología como respuesta a una vulneración de los datos, las tecnologías de detección para las redes (46% de las empresas y PYMES) y los endpoints (45% de las empresas y 41% de las PYMES) son seguidas de cerca por la inteligencia contra amenazas, tanto para las empresas como para las PYMES, 41% y 39% respectivamente. Esto sugiere que las empresas entienden el valor, no solo de responder rápidamente, sino de tener la información y los conocimientos necesarios para reaccionar ante las amenazas en constante cambio, a medida que el panorama cibernético sigue evolucionando.

En contraste con aquellos que buscan invertir más en seguridad de la TI, el 9% de las PYMES y el 11% de las empresas indicaron que planean reducir sus presupuestos en esta área durante los próximos tres años. La razón principal de esto, especialmente visible en las empresas, es la sensación de que se ha invertido lo suficiente para asegurar una empresa y que no es necesario mantener los niveles actuales de inversión.

Por ejemplo, un tercio (32%) de los altos directivos de las empresas no ven ninguna razón para invertir tanto en la seguridad de la TI, y esta es la razón principal para reducir los presupuestos. En el caso de las PYMES, una cuarta parte (25%) cree que son lo suficientemente seguras y no necesitan gastar más dinero en esta área, pero la razón principal para reducir la inversión se debe a los recortes generales de los gastos de la empresa y a la optimización del presupuesto general (29%).

Gráfica 6: Principales razones para disminuir las inversiones en seguridad de la TI

Razones para tratar de reducir el gasto en seguridad de la TI en los próximos tres años	PYME		Empresa	
	%	Rango	%	Rango
Recortes generales en los gastos de las empresas/optimización del presupuesto general	29%	1	26%	5
Las grandes inversiones de los años pasados resolvieron problemas clave, ahora solo se necesita mantenimiento	25%	3	30%	2
Los principales administradores no ven ninguna razón para invertir tanto en seguridad de TI	23%	5	32%	1
Estamos suficientemente seguros y no hay necesidad de invertir más en seguridad de TI	25%	2	22%	7
La subcontratación de algunas funciones de seguridad de TI nos permite reducir los costos	22%	7	26%	4
El presupuesto de TI se reasignó a otras necesidades de la empresa	19%	8	27%	3
Debido a la reducción de la empresa	23%	4	20%	10
No se registraron incidentes de seguridad en los últimos 12 meses	22%	6	21%	8
Cambiamos a una solución/proveedor de protección para endpoints más económico	19%	8	23%	6
A petición de nuestros accionistas e inversores	15%	10	21%	9

Conclusión

Apesar de los acontecimientos únicos del 2020, en nuestra investigación se identificaron una serie de tendencias recurrentes y se sugiere una perspectiva positiva para dar prioridad a la seguridad de la TI y al aumento del gasto en este ámbito, tanto en la comunidad de las PYMES como en la de las empresas.

La disminución del impacto financiero de una vulneración de los datos en las empresas es sin duda una buena noticia, lo cual sugiere que las medidas de mitigación están funcionando en su mayor parte y que los presupuestos se están utilizando en los sitios adecuados.

Sin embargo, las cifras no deben ser una señal de complacencia, sino que deben servir de prueba para que las medidas de seguridad de TI, sólidas y robustas, funcionen y sean cruciales para ahorrar posibles costos a largo plazo. La creciente proporción de la seguridad de la TI, dentro del gasto total en la TI, apunta al valor que se da a las medidas de ciberseguridad y es, sin duda, un área que las empresas deben seguir desarrollando para mantener los niveles de seguridad y protección más altos en medio de un panorama de amenazas siempre variable.

Es evidente que es fundamental la aceptación y comprensión por parte de los principales administradores para garantizar y aumentar la inversión, en particular en las empresas. Incluso cuando los encuestados mencionaron presupuestos reducidos para los próximos años, el desarrollo y gasto en infraestructuras de ciberseguridad, hasta este momento, han sido principalmente positivos. El reconocimiento, la inteligencia y la reacción final ante las amenazas han evolucionado, junto con el deseo de mejorar y reforzar los equipos de seguridad interna.

Como forma de vigilancia proactiva, debería haber una mayor conciencia sobre cómo el trabajo remoto y los equipos más dispersos aumentan los niveles de vulnerabilidad de las empresas. Solo tenemos que observar la rápida evolución de las tácticas de ingeniería social, incluyendo el phishing, para ver cómo los cibercriminales siguen mejorando su arsenal de ataques y mantienen a los equipos de TI en alerta.

Para ayudar a que las empresas se enfrenten a estos desafíos continuos y garantizar que los presupuestos y las medidas se ajusten a las prioridades actuales y a las amenazas en constante evolución, Kaspersky sugiere las siguientes medidas.

- Utilice un enfoque basado en el riesgo cuando planifique su presupuesto de ciberseguridad. Analice las amenazas más relevantes para su industria y el tamaño de su empresa, después considere el costo para la empresa y la probabilidad de que ocurra el riesgo al priorizar lo que debe enfrentar primero
- La subcontratación puede ser una buena opción para las empresas que no cuentan con los conocimientos técnicos internos necesarios o con procesos de evaluación de riesgos. Acordar un acuerdo de nivel de servicio garantizado (SLA) con cualquier tercero y trasladar los gastos de CapEx a OpEx es una forma de mantener los gastos de seguridad bajo control
- Proporcione a todo su personal una formación básica en limpieza de ciberseguridad. Mejore siempre las habilidades de sus trabajadores de seguridad de TI, para que puedan defenderse incluso de ataques sofisticados. Por ejemplo, Kaspersky proporciona entrenamiento en línea sobre la búsqueda de amenazas con las reglas de YARA
- A pesar de que el costo de las vulneraciones de los datos disminuye cada año, las empresas deben mantenerse alertas y utilizar siempre una solución de ciberseguridad dedicada que combine la protección de los endpoints con capacidades de detección. La solución Integrated Endpoint Security de Kaspersky proporciona visibilidad y conocimiento instantáneo de los incidentes, junto con opciones de investigación inmediata y respuesta automatizada
- Las soluciones de seguridad que se pueden administrar desde la nube deben simplificar la protección de las oficinas y sucursales remotas, lo cual fue otra de las principales preocupaciones de los especialistas en ciberseguridad este año
- Garantice la protección contra el spam y el phishing para que los actores maliciosos no puedan beneficiarse de la credibilidad de los empleados, ya sea que están vinculados al COVID-19 o a cualquier otro evento o tendencia. Esto también es relevante para los servicios de correo SaaS, como Microsoft Office 365
- Para proteger a los clientes del phishing, edúquelos sobre los posibles engaños que pueden utilizar los malhechores. Envíe regularmente información sobre cómo identificar los fraudes y qué medidas tomar en dicha situación. En caso de que la cuenta de un cliente quede comprometida, será de gran valor contar con una solución antifraude que pueda detectar anomalías y comportamientos sospechosos de los usuarios

Para obtener más información sobre los costos variables asociados con la seguridad de TI y cómo mantener a su empresa protegida contra la evolución de las amenazas y las vulneraciones de los datos, siga a **#securityeconomics** para ver nuestra serie de informes sobre el tema.

Noticias sobre las amenazas cibernéticas:securelist.com
Noticias sobre la seguridad de TI: business.kaspersky.com

kaspersky.com

kaspersky

GBD-7018 Q3/20 V1