CPL.thalesgroup.com #2020DataThreat

THALES

La seguridad de los datos evoluciona hacia un enfoque de Zero Trust en América Latina

Informe de Thales sobre amenazas a datos 2020

Edición de América Latina

RESEARCH AND ANALYSIS FROM:

IDC ANALYZE THE FUTURE

Acerca del estudio

Este informe se centra en los hallazgos de más de 200 ejecutivos latinoamericanos de Brasil y México, y brinda comparaciones y contrasta con la encuesta global de IDC llevada a cabo en la web de 1.723 encuestados con responsabilidad o influencia sobre TI y la seguridad de los datos. Los encuestados provenían de 16 países: los países latinoamericanos de la muestra más Australia, Francia, Alemania, India, Indonesia, Japón, Malasia, los Países Bajos, Nueva Zelanda, Singapur, Corea del Sur, Suecia, el Reino Unido y los Estados Unidos. Las organizaciones representaban una variedad de industrias, con un énfasis principal en la salud, los servicios financieros, el comercio minorista, la tecnología y las organizaciones del gobierno federal. Los puestos de trabajo incluían desde ejecutivos de nivel C como director general (CEO), gerente de finanzas (CFO), director de datos, oficial de seguridad de la información (CISO), jefe de ciencia de datos y director de riesgos, así como vicepresidente ejecutivo superior/vicepresidente (SVP/VP), administrador de TI, analista de seguridad, ingeniero de seguridad y administrador de sistemas. Los encuestados representaron una amplia gama de tamaños organizacionales, con la mayoría de 500 a 10 000 empleados. La encuesta se realizó en noviembre de 2019. Para conocer los resultados y el análisis global del resumen, consulte cpl.thalesgroup.com/data-threat-report.

Índice

Nuestros patrocinadores son:

Resumen

de las empresas se enfrentan hoy día a interrupciones en sus mercados y cadenas de suministro que están presentando desafíos diferentes a los que han enfrentado en el pasado. A medida que las organizaciones revisan, recalibran y, en algunos casos, reinventan operaciones fundamentales, el éxito ahora más que nunca depende de la adopción de tecnologías de transformación digital (DX), incluidas la nube, los dispositivos móviles y el Internet de las cosas (IoT). La DX juega un papel clave en ayudar a las empresas a adaptarse a las nuevas normas actuales, así como a prepararse para las realidades comerciales posteriores a la COVID-19.

Actualmente, América Latina está rezagada con otras regiones en términos de transformación digital. Pero esta aparente responsabilidad en realidad le da la oportunidad a las organizaciones latinoamericanas de superar a otros países a medida que aceleran la DX para transformar su negocio en el futuro. La investigación de IDC muestra que, para algunas empresas en América Latina, la transformación digital está, de hecho, muy avanzada. El 27% de las organizaciones de América Latina en nuestro estudio afirman estar alterando agresivamente los mercados en los que operan o estar incorporando capacidades digitales que permiten una mayor agilidad empresarial. Además, el 57% de las organizaciones en esta región espera tener hasta el 25% de sus ingresos generados por servicios digitales (fuente: IDC Tendencias de inversión en América Latina 2H19).

Si bien la transformación digital puede aportar un gran valor, también hace que la seguridad de los datos sea más compleja. Esto es especialmente cierto en los tiempos de incertidumbre actuales. A medida que la DX se acelera, los equipos de seguridad deben competir para ponerse al día con los equipos de negocios/TI que pueden crear aún más vulnerabilidades y aumentar drásticamente el riesgo para las organizaciones. Las empresas dependen de la cantidad de datos almacenados en la nube, que aumenta continuamente. Las organizaciones latinoamericanas se están acercando a un punto de inflexión en el que el 49% de los datos se almacenan en la nube y el 45% de esos datos son confidenciales. Además, la mayoría de las organizaciones latinoamericanas están ejecutando entornos de nube múltiple. Todo esto se suma a que los entornos de datos actuales son cada vez más complejos. Y la complejidad es una de las principales barreras para la seguridad de los datos.

El 49%

de **los datos se almacenan en la nube,** y **el 45% de esos datos son confidenciales.**

El 73%

de los encuestados latinoamericanos ve **que la criptografía cuántica afectará a su organización en los próximos cinco años.**

Sin embargo, las organizaciones tienen disonancia cognitiva en lo que respecta a la seguridad de los datos. El 62% de los profesionales de seguridad y TI de América Latina cree que no son en absoluto vulnerables, pero sus organizaciones no están implementando los procesos ni invirtiendo en tecnologías necesarias para protegerse adecuadamente contra el aumento de los riesgos de datos. Más de la mitad ha sufrido brechas de datos o no ha superado auditorías de seguridad. Y cuando se trata de proteger los datos en la nube, la mayoría de las empresas buscan incorrectamente en sus proveedores de la nube cuál es la parte de la empresa del modelo de responsabilidad compartida. El 27% de las organizaciones de la región considera su estrategia en la nube como su iniciativa principal o el objetivo final para lograr una postura de seguridad más sólida (fuente: Informe de Ciberseguridad de América Latina de IDC 2019).

El problema de la disonancia cognitiva es más extremo en América Latina que en otras regiones del mundo, ya que la seguridad de los datos todavía representa una pequeña parte de su presupuesto general de seguridad, con un promedio de seguridad de datos de solo el 15% de su presupuesto total de seguridad de TI. El 44% de las organizaciones en América Latina tienen previsto aumentar el gasto en seguridad de datos en los próximos 12 meses, cinco puntos por debajo del 49% de los encuestados a nivel mundial que prevén que el gasto aumente. Por otro lado, las organizaciones latinoamericanas dicen que el 37% de su interés en soluciones de seguridad se centra en la seguridad de los datos, que es un porcentaje más alto que en otras regiones. Este mayor nivel de enfoque en los datos probablemente se ve impulsado por las nuevas regulaciones en materia de protección de datos y privacidad que estaban cerca de implementarse en Brasil (Lei Geral de Proteção de Dados Pessoais -LGPD), pero su aplicación se pospuso hasta 2021. Existen otras iniciativas similares con diferentes niveles de alcance y sanciones en países como México, Colombia, Chile y Argentina.

Los encuestados de América Latina reconocen que la computación cuántica se avecina, lo que promete complicar aún más la seguridad de los datos. Los requisitos de criptografía cambiarán fundamentalmente cuando la computación cuántica esté en línea, y el 73% ve que la criptografía cuántica afectará a su organización en los próximos cinco años.

A medida que las organizaciones latinoamericanas se enfrentan a retos en materia de seguridad de datos cada vez más amplios y complejos, estas deben adoptar formas mejores y más inteligentes para abordar la seguridad de los datos. Las empresas de América Latina deben adoptar un enfoque multidimensional para proteger los datos, desde la adopción de responsabilidades de seguridad compartidas en la nube hasta la implantación de un modelo de administración de acceso Zero Trust que realice la autenticación y validación de los usuarios y dispositivos que acceden a las aplicaciones y las redes. Además, deben utilizar soluciones más sólidas para la localización de datos, el fortalecimiento de la protección, la prevención de la pérdida de datos y el cifrado. Es importante que la seguridad de los datos no socave los esfuerzos de las empresas por lograr la transformación digital mediante la aplicación de marcos flexibles que lleven a la implantación de modelos de confianza discrecionales.

La COVID-19 lo cambia todo

El alcance y la amplitud de la pandemia de la COVID-19 han creado una situación para los profesionales de la recuperación de desastres y de la seguridad cibernética en una escala nunca antes vista. No solo los departamentos de TI se enfrentan a tener que operar en condiciones adversas, sino que muchos planes de respaldo que involucran ubicaciones geográficas cambiantes o instalaciones temporales también son inadecuados. Nunca antes tantas organizaciones se habían visto obligadas a "recuperarse" y a operar indefinidamente del mismo "desastre" en un período de tiempo tan corto.

La nueva realidad para muchos es clasificar las prácticas de ciberseguridad existentes: lograr que las licencias de VPN, las reglas de firewall y los programas BYOD se cuadren mientras se desarrolla un plan que incorpora una ciberseguridad más dinámica para una mayor resiliencia en el futuro.

Cuando se trata de ciberseguridad en la era posterior a la COVID-19, hay tres preguntas clave para las que todo director de información necesita respuestas:

- ¿Cuáles son los cambios en los patrones de uso y la arquitectura en mi entorno de TI?
- ¿Cómo estos cambios afectan al riesgo?
- ¿Qué cambios debo realizar en mi entorno de control y en mi postura ante la ciberseguridad?

Con este replanteamiento de la seguridad de 360 grados, se puede esperar ver incluso un gran interés en las herramientas de seguridad de datos posteriores a la COVID-19. De hecho, los datos recopilados por IDC encontraron que el 42% de las empresas espera que la demanda de inversiones en tecnología de seguridad de datos aumente como resultado de la COVID-19. La tecnología y las herramientas de seguridad, tales como la recuperación ante desastres, la autenticación multifactor y el cifrado, serán aún más relevantes a medida que las empresas y otras organizaciones busquen asegurar el acceso remoto para los empleados y a medida que más datos y cargas de trabajo se trasladen a la nube.

Fuentes:

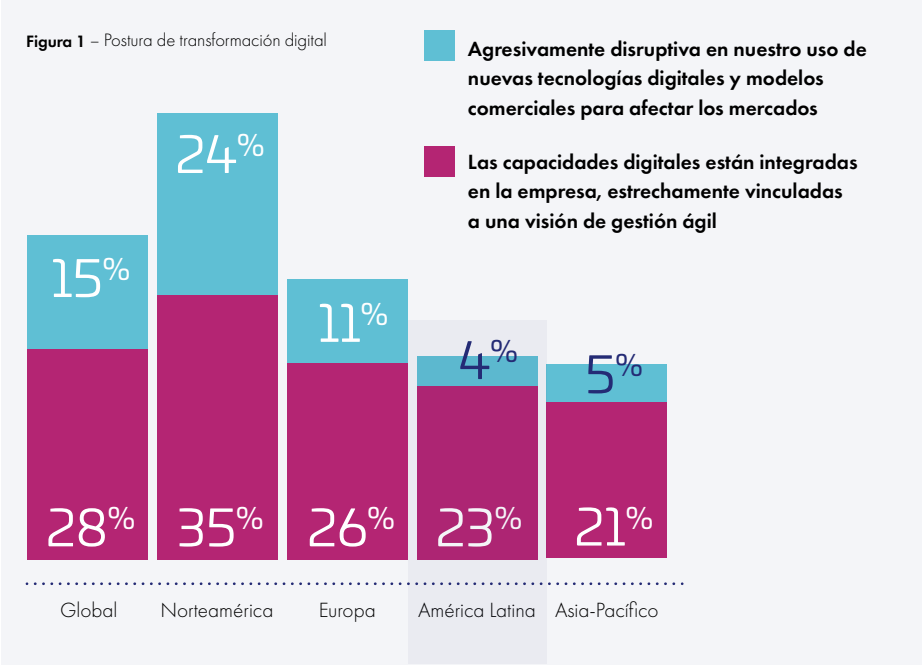
- Lindstrom, P., 2020, Impacto de la COVID-19 en el gasto en seguridad de datos por tamaño de empresa, IDC
- Dickson, F. y Westervelt, R., 2020, Post-COVID-19: Una guía de recuperación del CIO - Cybersecurity, IDC

01
Principales conclusiones

América Latina está rezagada en la transformación digital

En todo el mundo, las organizaciones están utilizando la transformación digital para reinventar de manera fundamental sus negocios y aprovechar las tecnologías digitales como la nube, los dispositivos móviles y la IoT. Pero esta tendencia es más lenta en América Latina que en otras regiones. El treinta y siete por ciento de las organizaciones latinoamericanas dijo estar aplicando la transformación digital de manera ad hoc. Solo el 27% de los encuestados de América Latina afirma estar alterando agresivamente los mercados en los que operan o estar incorporando capacidades digitales que permiten una mayor agilidad empresarial, en comparación con el 43% global (ver Figura 1).

Figura 1 – Postura de transformación digital



Fuente: Encuesta del Informe de Thales sobre amenazas a datos 2020, IDC, noviembre de 2019

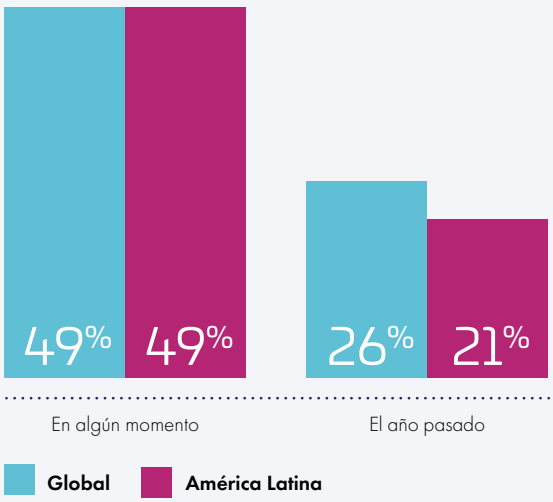
"Solo el 27% de los encuestados de América Latina afirma estar alterando agresivamente los mercados en los que operan o estar incorporando capacidades digitales que permiten una mayor agilidad empresarial".

Pero ninguna organización es inmune a las amenazas a la seguridad de los datos: el 49% de los encuestados latinoamericanos afirma haber experimentado alguna vez una brecha de datos y el 21% afirma haber sufrido una brecha en el último año (ver Figuras 2a y 2b). Otro 17 % de las organizaciones latinoamericanas indicó que no ha superado con éxito una auditoría de cumplimiento durante el último año. Nuestro estudio muestra tasas de brechas similares en América Latina con respecto a la muestra global, aunque la conciencia pública puede ser menor ya que pocos países de América Latina tienen leyes de divulgación pública en casos de brechas o incumplimiento.

El 49%

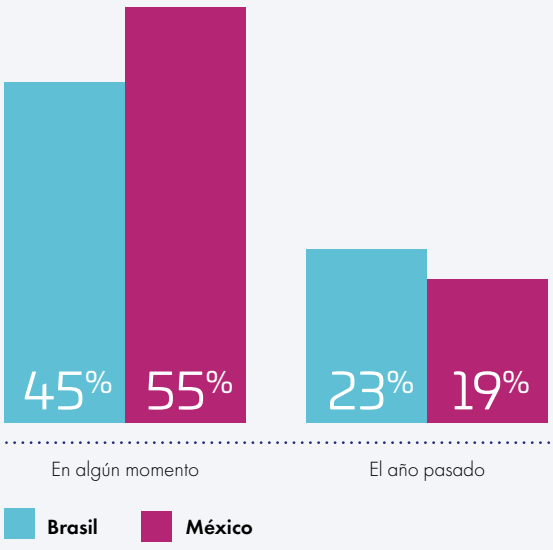
de los encuestados latinoamericanos ha experimentado una brecha y el 21% ha sufrido una brecha en el último año.

Figura 2a – Tasas de incidentes de brechas



Fuente: Encuesta del Informe de Thales sobre amenazas a datos 2020, IDC, noviembre de 2019

Figura 2a – Tasas de incidentes de brechas por país



Fuente: Encuesta del Informe de Thales sobre amenazas a datos 2020, IDC, noviembre de 2019

El 17%

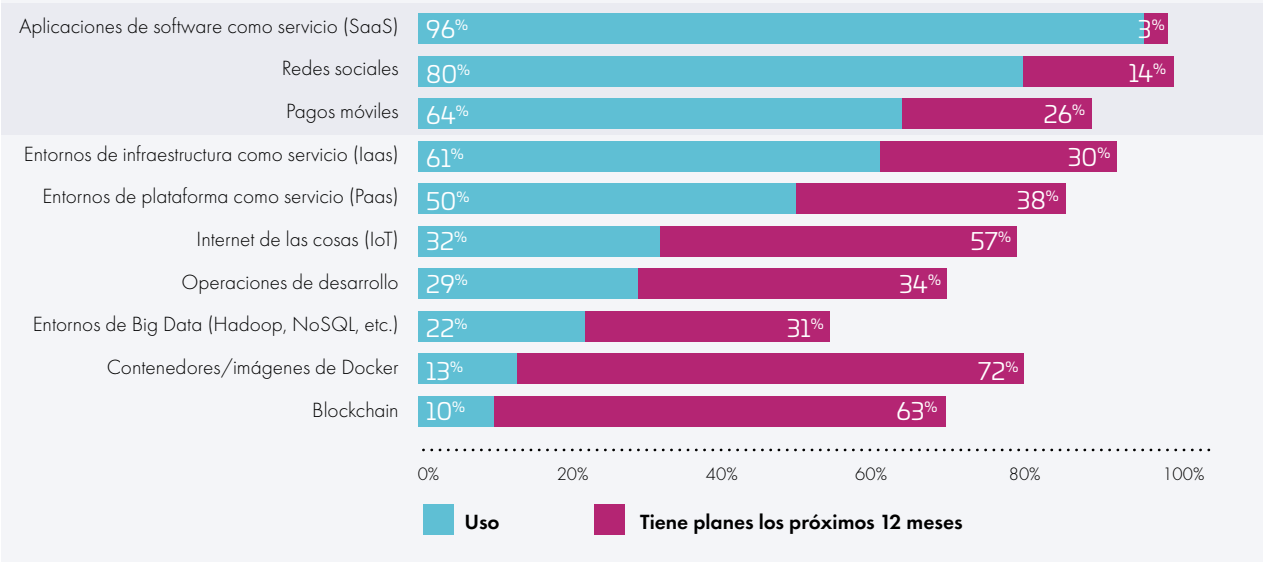
de las organizaciones latinoamericanas indicó que no ha superado con éxito una auditoría de cumplimiento durante el último año.

Si bien las organizaciones que se transforman digitalmente obtienen nuevas ventajas competitivas, también se enfrentan a nuevos retos de seguridad de datos presentados por la transformación digital. La transformación digital tiene una correlación positiva con la vulnerabilidad: cuanto más haya avanzado una organización en este proceso, más probable es que diga que haya experimentado una brecha de datos. Las organizaciones determinadas a alcanzar la transformación digital (aquellas organizaciones que toman decisiones estratégicas, organizativas, tecnológicas y financieras que las prepararán para transformarse digitalmente en los próximos años) también pueden estar más expuestas a las amenazas de datos. Su mayor nivel de sofisticación también puede implicar que sean más conscientes de que han sufrido brechas. Las empresas menos sofisticadas pueden verse menos expuestas, o simplemente pueden haber sido víctimas de brechas sin saberlo.

Las organizaciones hospedan datos confidenciales en una amplia gama de tecnologías

Las organizaciones latinoamericanas están adoptando una amplia gama de tecnologías de la Tercera Plataforma, que incluyen la nube, los dispositivos portátiles, lo social, el Big Data y el IoT. Las aplicaciones SaaS tienen la adopción más amplia por parte de las empresas latinoamericanas con un 96% (ver Figura 3). Las redes sociales y los pagos móviles también tienen altos niveles de adopción, mientras que los entornos de nube IaaS y PaaS, así como el IoT tienen altos niveles de adopción planificada. Tenga en cuenta que muchas de estas tecnologías tales como el IoT y los dispositivos móviles son tecnologías de vanguardia, lo que refuerza el mensaje de que la exposición de datos se está expandiendo mucho más allá del perímetro de la red tradicional.

Figura 3 – Niveles de adopción de tecnología: organizaciones latinoamericanas



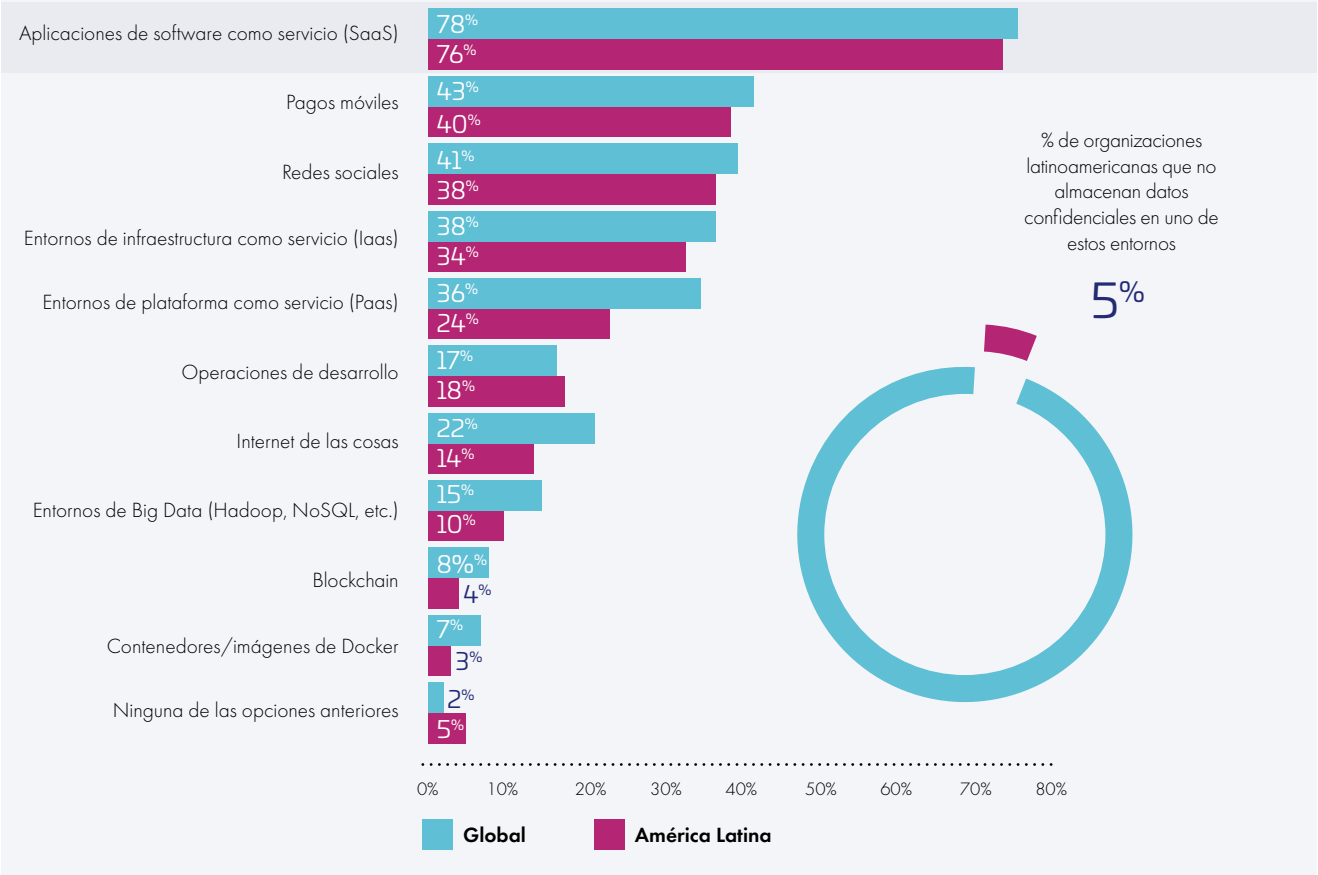
Fuente: Encuesta del Informe de Thales sobre amenazas a datos 2020, IDC, noviembre de 2019

El 76%

de las organizaciones latinoamericanas almacena datos confidenciales en aplicaciones SaaS, el 34% almacena datos en IaaS y el 24% almacena datos en entornos PaaS.

Asimismo, muchas organizaciones latinoamericanas están ubicando datos confidenciales o regulados en un conjunto de entornos igualmente amplio. El 76% almacena datos confidenciales en aplicaciones SaaS, el 34% almacena datos en IaaS y el 24% almacena datos en entornos PaaS. El noventa y cinco por ciento de las organizaciones latinoamericanas en la encuesta están almacenando datos en al menos uno de los entornos tecnológicos de nuestra encuesta (ver Figura 4).

Figura 4 – Entornos tecnológicos utilizados para almacenar datos confidenciales/regulados



Fuente: Encuesta del Informe de Thales sobre amenazas a datos 2020, IDC, noviembre de 2019

A medida que las empresas amplían su uso de las tecnologías de la nube, móviles, sociales, de Big Data e IoT utilizando proveedores subcontratados, como resultado los datos confidenciales se vuelven potencialmente cada vez más vulnerables. Por lo tanto, asegurar el perímetro contribuye en poco para proteger los datos que viven fuera de las instalaciones, lo que habla de la necesidad de adoptar un enfoque de seguridad de acceso con menos privilegios y de protección a los datos. Este enfoque seguro con privilegios mínimos elimina el antiguo enfoque binario de confianza/desconfianza de la realidad local, centrada en el perímetro y en cambio, requiere un enfoque de verificación y validación continua centrada en la identidad, que proporcione protección de acceso a la red y a las aplicaciones. Del mismo modo, tecnologías como el cifrado y la tokenización aseguran que si fallan las medidas con privilegios mínimos y los datos se piratean o filtran, o si se roban dispositivos físicos, los datos también se protegen adecuadamente.

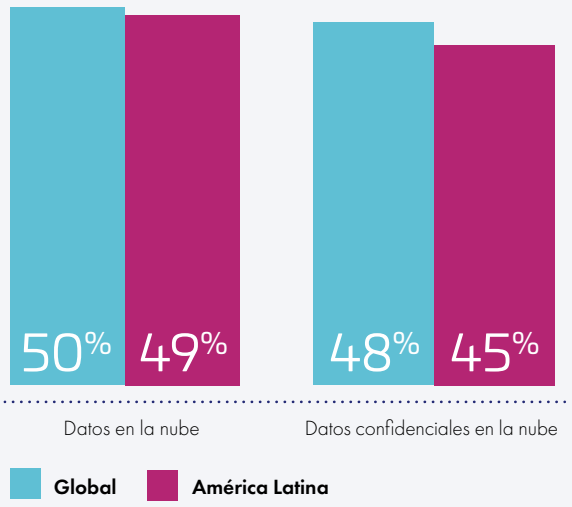
Las nubes son el entorno de datos líder que crea un riesgo significativo

Todas las organizaciones latinoamericanas encuestadas guardan algunos datos confidenciales en la nube. Los datos almacenados en la nube se acercan a un punto de inflexión, ya que los encuestados de nuestro estudio afirman estimar que el 49% de los datos está en la nube, cifra algo inferior al 50% de la muestra a nivel mundial. Más importante aún, los encuestados latinoamericanos dijeron que se estima que el 45% de esos datos en la nube sean confidenciales y el 100% de las organizaciones latinoamericanas dijo almacenar al menos algunos datos confidenciales en la nube (ver Figura 5). Los encuestados brasileños identificaron el 47% de sus datos en la nube como confidenciales, que es el cuarto país más alto a nivel mundial en nuestro estudio, solo detrás de Nueva Zelanda (56%), EE. UU. (54%) y Corea del Sur (48%).

El 100%

de los encuestados latinoamericanos dice que al menos algunos de sus datos confidenciales en la nube no se encuentran cifrados.

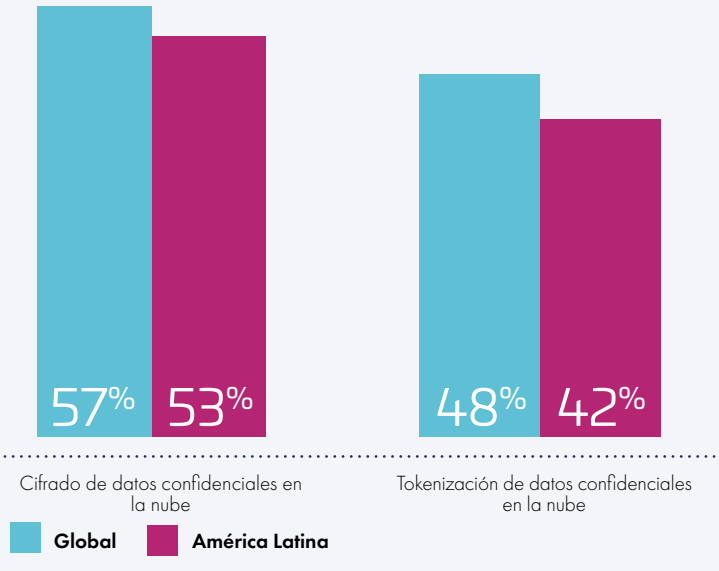
Figura 5 – Datos confidenciales almacenados en entornos de nube



Fuente: Encuesta del Informe de Thales sobre amenazas a datos 2020, IDC, noviembre de 2019

Cuantos más datos sensibles se almacenan en entornos de nubes, mayores son los riesgos de seguridad de los datos. Sin embargo, a pesar de esta exposición significativa de datos confidenciales, los índices de cifrado de datos y tokenización son bajos. De hecho, el 100% de los encuestados latinoamericanos dice que al menos algunos de sus datos confidenciales en la nube no están cifrados. Solo el 53% de los datos confidenciales almacenados en entornos de nube están protegidos mediante cifrado y menos de la mitad (el 42%) están protegidos mediante el uso de tokenización (ver Figura 6).

Figura 6 – Seguridad de datos confidenciales en la nube



Fuente: Encuesta del Informe de Thales sobre amenazas a datos 2020, IDC, noviembre de 2019

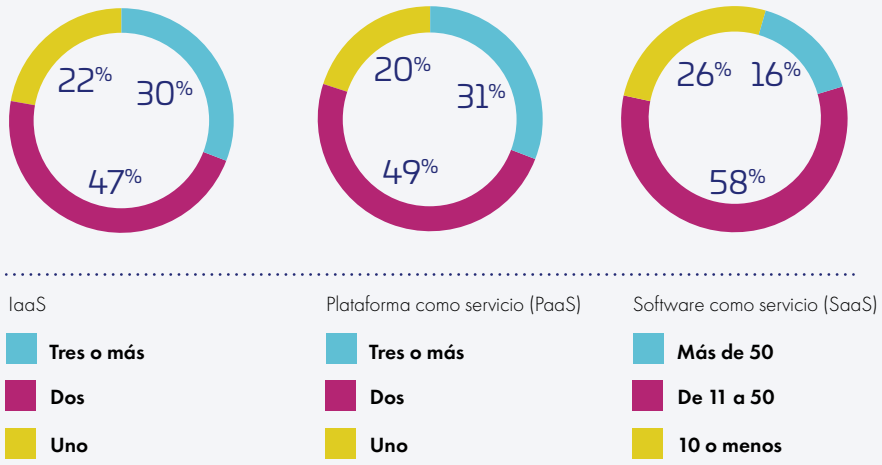
La complejidad de los entornos de datos es una de las principales barreras para la seguridad de los datos, ya que la nube múltiple se convierte en la norma

Cuantos más datos migran a la nube, más compleja se vuelve la seguridad. Esta complejidad a menudo es autoinfligida mediante el uso de entornos de nube múltiple y de múltiples sistemas de administración de llaves de cifrado. Esto es cierto en América Latina; a pesar de que América Latina está ejecutando menos entornos en la nube en promedio que otras regiones de la encuesta, no obstante la mayoría de las organizaciones latinoamericanas ejecutan múltiples entornos de nube. El 30% de las organizaciones latinoamericanas utiliza tres o más proveedores de IaaS, el 31% trabaja con más de tres proveedores de PaaS y el 16% debe administrar más de 50 aplicaciones SaaS (ver Figura 7). En comparación, América del Norte con un 35% tenía más del doble de organizaciones con más de 50 aplicaciones SaaS.

El 44%

de los encuestados latinoamericanos dice que la complejidad es la principal barrera para implementar la seguridad de los datos.

Figura 7 – Número de proveedores de IaaS/PaaS en organizaciones europeas



Fuente: Encuesta del Informe de Thales sobre amenazas a datos 2020, IDC, noviembre de 2019

"El 30% de las organizaciones latinoamericanas utiliza tres o más proveedores de IaaS, el 31% trabaja con más de tres proveedores de PaaS y el 16% debe administrar más de 50 aplicaciones SaaS".

La complejidad resultante, incluida la organización de soluciones de administración de llaves de cada proveedor de servicios en la nube en un entorno de nube múltiple, les complica la vida de los profesionales de la seguridad. La preocupación por la complejidad es por mucho, la principal barrera para implementar la seguridad de los datos (44%) y es un problema particular en esta región, con más encuestados latinoamericanos preocupados por la complejidad que en cualquier otra región. Este hallazgo es consistente con que América Latina esté menos avanzada en DX que cualquier otra región. Otras preocupaciones importantes son el impacto de la seguridad de los datos en el rendimiento y el proceso organizacional en un 34% y la falta de presupuesto en un 32% (ver Figura 8).

Figura 8 – Barreras para implementar la seguridad de los datos

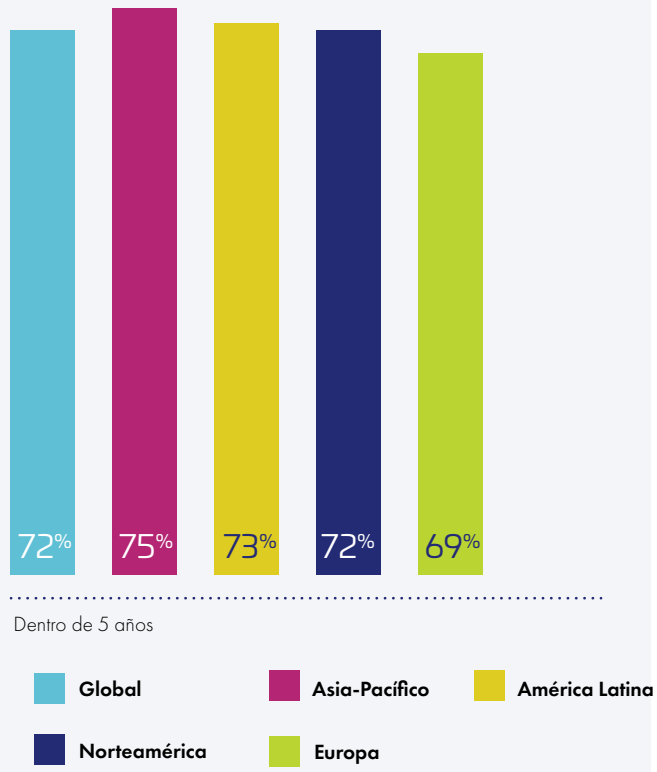
Fuente: Encuesta del Informe de Thales sobre amenazas a datos 2020, IDC, noviembre de 2019

"Más encuestados latinoamericanos están preocupados por la complejidad que cualquier otra región".

Se avistan en el horizonte problemas en cuanto a la seguridad de datos en la computación cuántica

La seguridad de los datos se volverá más compleja con la llegada de la informática cuántica. El impacto de la informática cuántica ya está aquí y el 73% de las organizaciones latinoamericanas considera que esta influirá en sus operaciones de cifrado en los próximos 5 años (ver Figura 9). Los requisitos de cifrado hacen hincapié en un problema crítico para la seguridad introducido por el potencial de la informática cuántica. Al 89% de los encuestados le preocupa que la informática cuántica aumente la exposición de los datos confidenciales y al 40% le preocupa mucho o muchísimo.

Figura 9 – Criptografía cuántica al afectar a las organizaciones



Fuente: Encuesta del Informe de Thales sobre amenazas a datos 2020, IDC, noviembre de 2019

Al **89%**

de los encuestados latinoamericanos le preocupa que la informática cuántica exponga los datos confidenciales.

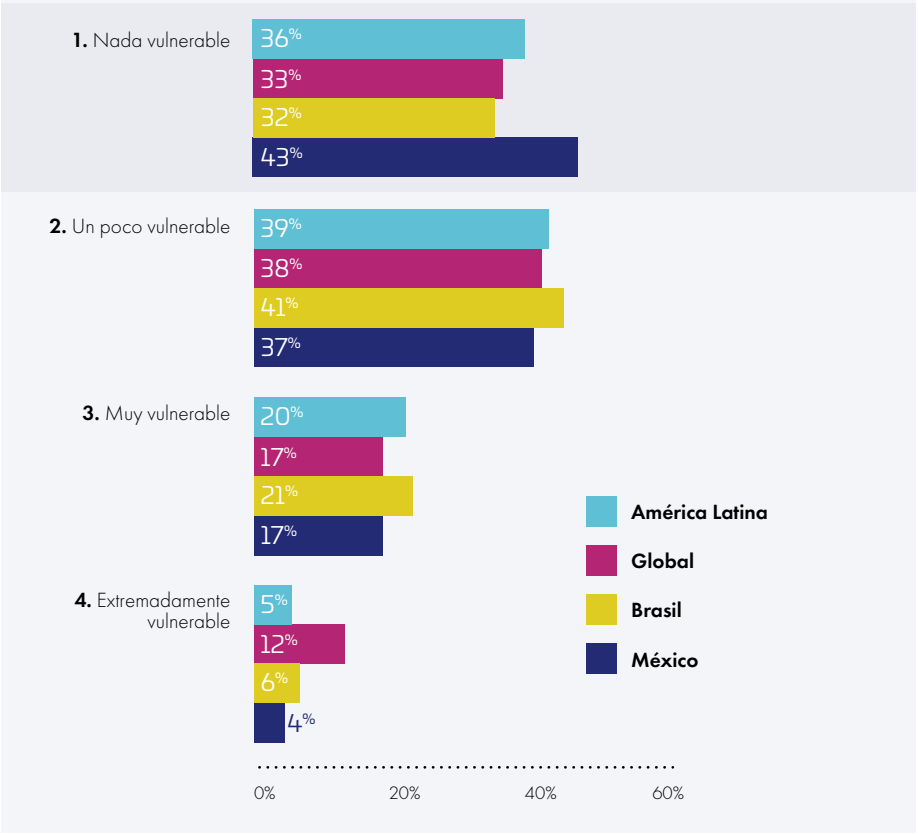
Los principales planes para compensar las amenazas de la computación cuántica son la administración de llaves que admite el generador de números aleatorios cuántico seguro (34%), cambiar fundamentalmente la arquitectura de TI y ciberseguridad (33%) y alejarse de la criptografía simétrica (32%). Pero muchas organizaciones latinoamericanas no están seguras de cómo responder a pesar de que pueden surgir amenazas en los próximos cinco años. El 21% de los encuestados planea airear los sistemas críticos y el 8% no tiene ningún plan.

"Muchas organizaciones latinoamericanas no están seguras de cómo responder a pesar de que las amenazas en cuanto a la computación cuántica pueden surgir en los próximos cinco años".

El sentido de la seguridad de los datos de las organizaciones está en conflicto con la realidad

A pesar de las amenazas generalizadas y en expansión a la seguridad de los datos, el 36% de los encuestados latinoamericanos afirma que "no son en absoluto vulnerables" a las amenazas internas y el 22% dijo que "no son en absoluto vulnerables" a las amenazas externas, por encima del promedio mundial de 33% y 18% para esas dos preguntas respectivamente. México se cree menos vulnerable a las amenazas internas, con un 43% que dice que "no son vulnerables en absoluto" y Brasil lo está en un 32%. (ver Figura 10).

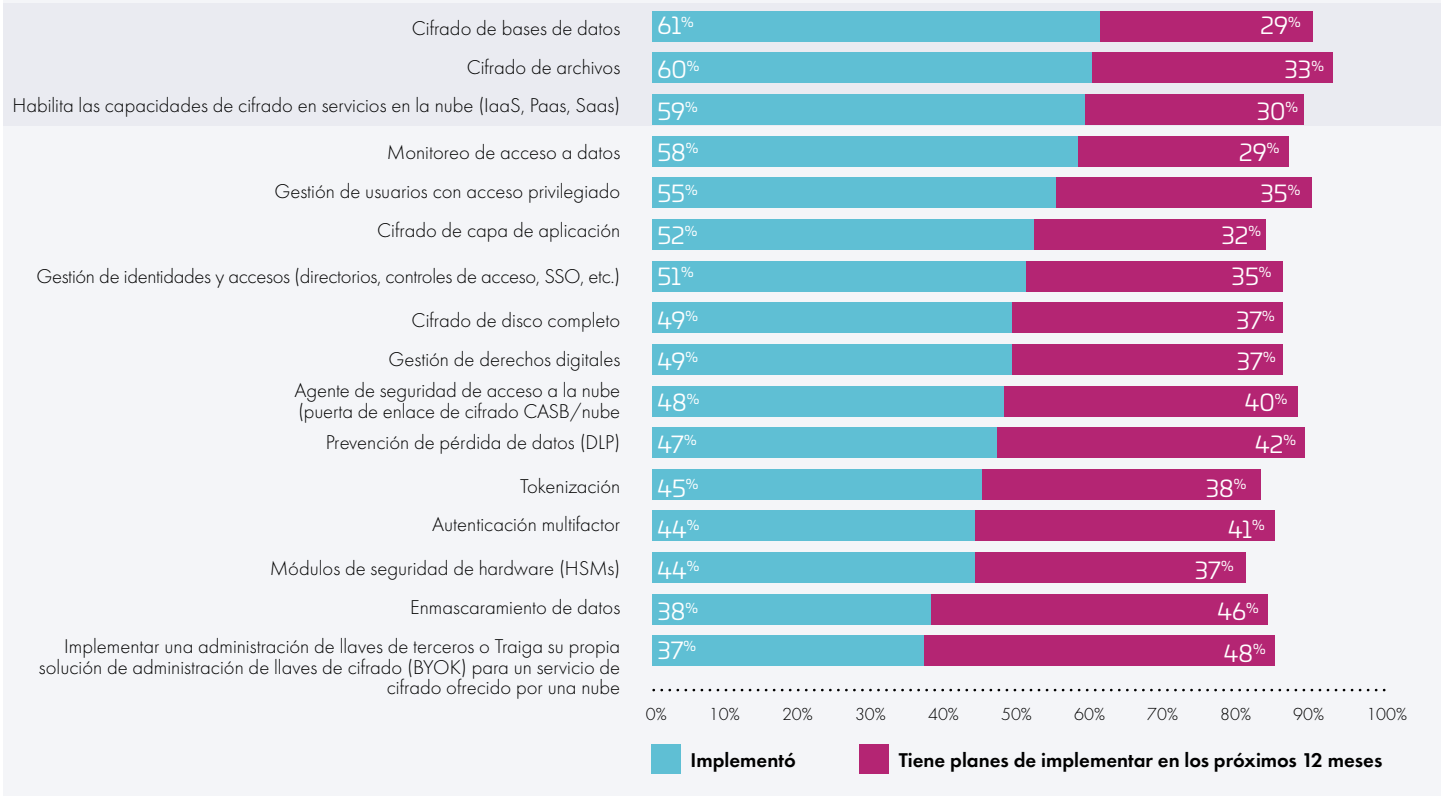
Figura 10 – Vulnerabilidad a las amenazas de seguridad de datos internos



Fuente: Encuesta del Informe de Thales sobre amenazas a datos 2020, IDC, noviembre de 2019

Estos bajos niveles de vulnerabilidad percibida apuntan a una desconexión entre la percepción y la realidad. Esta confianza no cuenta con el respaldo de prácticas o inversiones en seguridad de datos. Las organizaciones latinoamericanas no han cambiado significativamente sus posturas de seguridad al utilizar herramientas que las harían menos vulnerables, incluso después de la serie de ataques en finanzas durante 2018 y los ataques que afectaron la infraestructura crítica en México en 2019. Tal como se mencionó anteriormente, las tasas de cifrado y tokenización de datos confidenciales en la nube son bajas. Además, solo el 60% de los encuestados implementa el cifrado de archivos (a la par que la muestra global en el 61%) mientras que el 61% implementa el cifrado de la base de datos (un poco más alto que la muestra global en el 59%) (ver Figura 11).

Figura 11 – Implementación de herramientas de cifrado y seguridad de datos en organizaciones latinoamericanas



Fuente: Encuesta del Informe de Thales sobre amenazas a datos 2020, IDC, noviembre de 2019

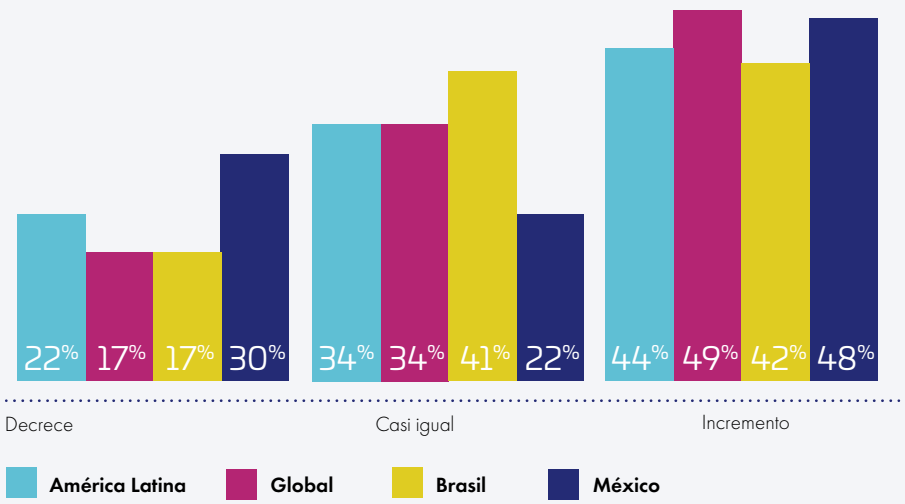
El 61%

de los encuestados latinoamericanos implementan cifrado de bases de datos y el 60% implementa cifrado de archivos.

El gasto en seguridad de datos está aumentando pero es inferior a la tasa global

Las organizaciones latinoamericanas planean gastar más dinero en seguridad de datos el próximo año. El 44% de los encuestados latinoamericanos dijo que gastaría algo o mucho más en seguridad de datos dentro de 12 meses, lo que es menor que el total global (49%). Pero el crecimiento del presupuesto en seguridad de datos está disminuyendo levemente y más de una de cada cinco organizaciones latinoamericanas planea reducir el gasto en seguridad de datos en 2020 (ver Figura 12). A nivel de país, México se destaca ya que el 30% de las organizaciones mexicanas planea disminuir el gasto en seguridad de datos en 2020, en comparación con solo el 17% en Brasil y el 17% a nivel mundial.

Figura 12 – Gasto en seguridad de datos - América Latina



Fuente: Encuesta del Informe de Thales sobre amenazas a datos 2020, IDC, noviembre de 2019

El **30%**

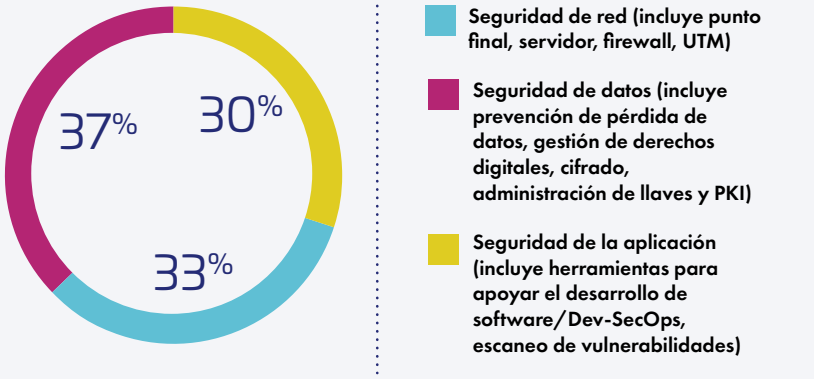
de las organizaciones mexicanas planea disminuir el gasto en seguridad de datos en 2020, en comparación con solo el 17% en Brasil y el 17% a nivel mundial.

El **15%**

de los presupuestos de seguridad de TI se gasta en seguridad de datos en América Latina.

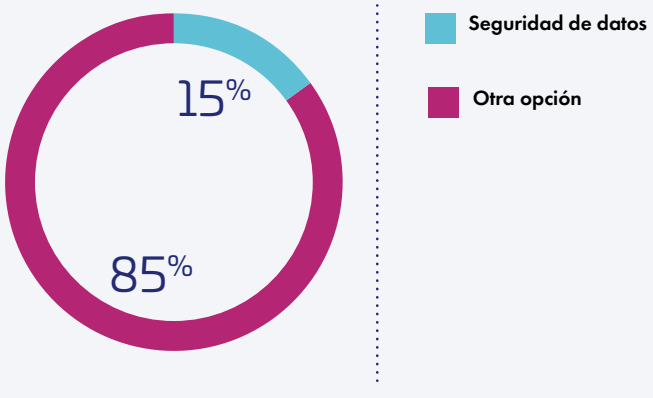
Las organizaciones latinoamericanas están enfocando predominantemente su interés en la seguridad de los datos (37%), seguidas de la seguridad de la red (33%) y la seguridad de las aplicaciones (30%), lo que podría conducir a un cambio en la forma como la región está invirtiendo efectivamente. Actualmente, las organizaciones están utilizando entre el 40% y el 45% de sus presupuestos en seguridad de redes (fuente: Informe de soluciones de seguridad de América Latina de IDC 2019). Este es un enfoque apropiado ya que las iniciativas de transformación digital han cambiado fundamentalmente la naturaleza y ampliado el perímetro; las empresas deben mirar más allá de centrarse simplemente en la protección de la red. En particular, América Latina cuenta con el mayor enfoque en la seguridad de datos de cualquier región de la muestra y más alto que el total mundial (34%), lo que indica que América Latina está por delante de la curva cuando se trata de cambiar el enfoque de seguridad para estar más alineado con los vectores de amenazas actuales. Pero los encuestados latinoamericanos no necesariamente están poniendo su dinero donde dicen, ya que el gasto en seguridad de datos no está en línea con esa tasa de atención y solo un promedio del 15% de los presupuestos de seguridad de TI se gasta en seguridad de datos (ver Figuras 13a y 13b).

Figura 13a – Proporción del enfoque de seguridad en organizaciones latinoamericanas



Fuente: Encuesta del Informe de Thales sobre amenazas a datos 2020, IDC, noviembre de 2019

Figura 13b – Proporción del presupuesto en seguridad de TI de América Latina exclusivo de la seguridad de datos



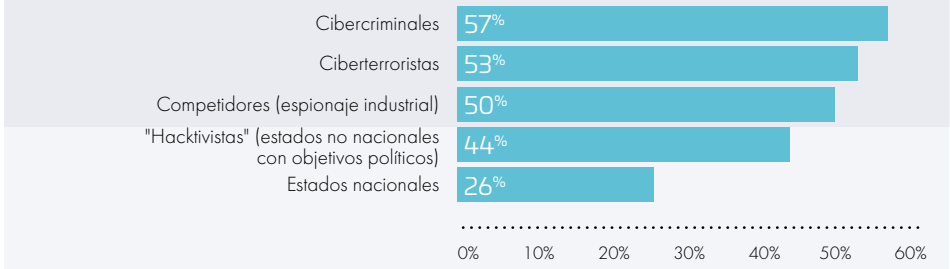
Fuente: Encuesta del Informe de Thales sobre amenazas a datos 2020, IDC, noviembre de 2019

Demostrando aún más una desconexión entre los presupuestos de seguridad y el enfoque de los departamentos de seguridad, los encuestados latinoamericanos creen que los actores malintencionados crean riesgos a los datos con amenazas intencionales de hacer daño, lo que representa las mayores amenazas a la seguridad de datos. El 57% está preocupado por los ciberdelincuentes que dañan o hacen que su organización se vea mal públicamente, seguidos por los ciberterroristas (53%) y el espionaje industrial (50%). Curiosamente, los encuestados latinoamericanos están menos preocupados por los problemas del día a día, que en realidad pueden ser una amenaza mayor y sobre los cuales tienen más control, incluido el acceso de proveedores de servicios (42%), las cuentas de administración ejecutiva (40%) y los socios con acceso interno (39%) (ver Figuras 14 y 15). Las empresas deben tener cuidado de no aprovisionar en exceso la cantidad y la amplitud de las cuentas, ya que el riesgo de las amenazas a datos internos a menudo se debe más al descuido que al comportamiento malicioso.

El 57%

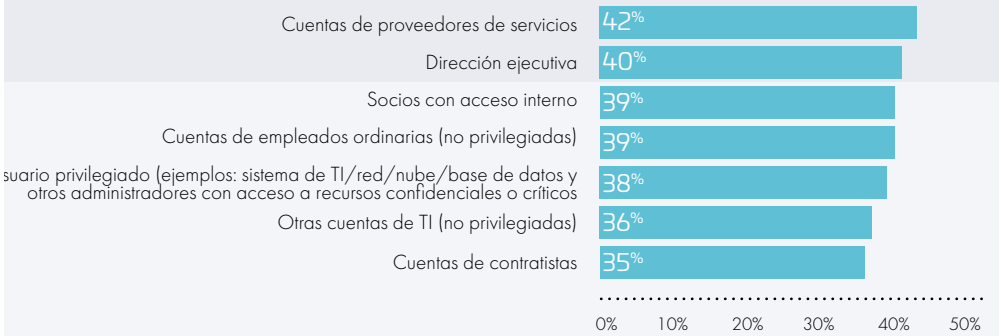
de los encuestados latinoamericanos están preocupados de que los ciberdelincuentes dañen o hagan que su organización se vea mal públicamente.

Figura 14 – Amenazas a datos por parte de actores maliciosos



Fuente: Encuesta del Informe de Thales sobre amenazas a datos 2020, IDC, noviembre de 2019

Figura 15 – Amenazas de datos internos



Fuente: Encuesta del Informe de Thales sobre amenazas a datos 2020, IDC, noviembre de 2019

02

La seguridad de los datos en la nube se encuentra en un punto de inflexión

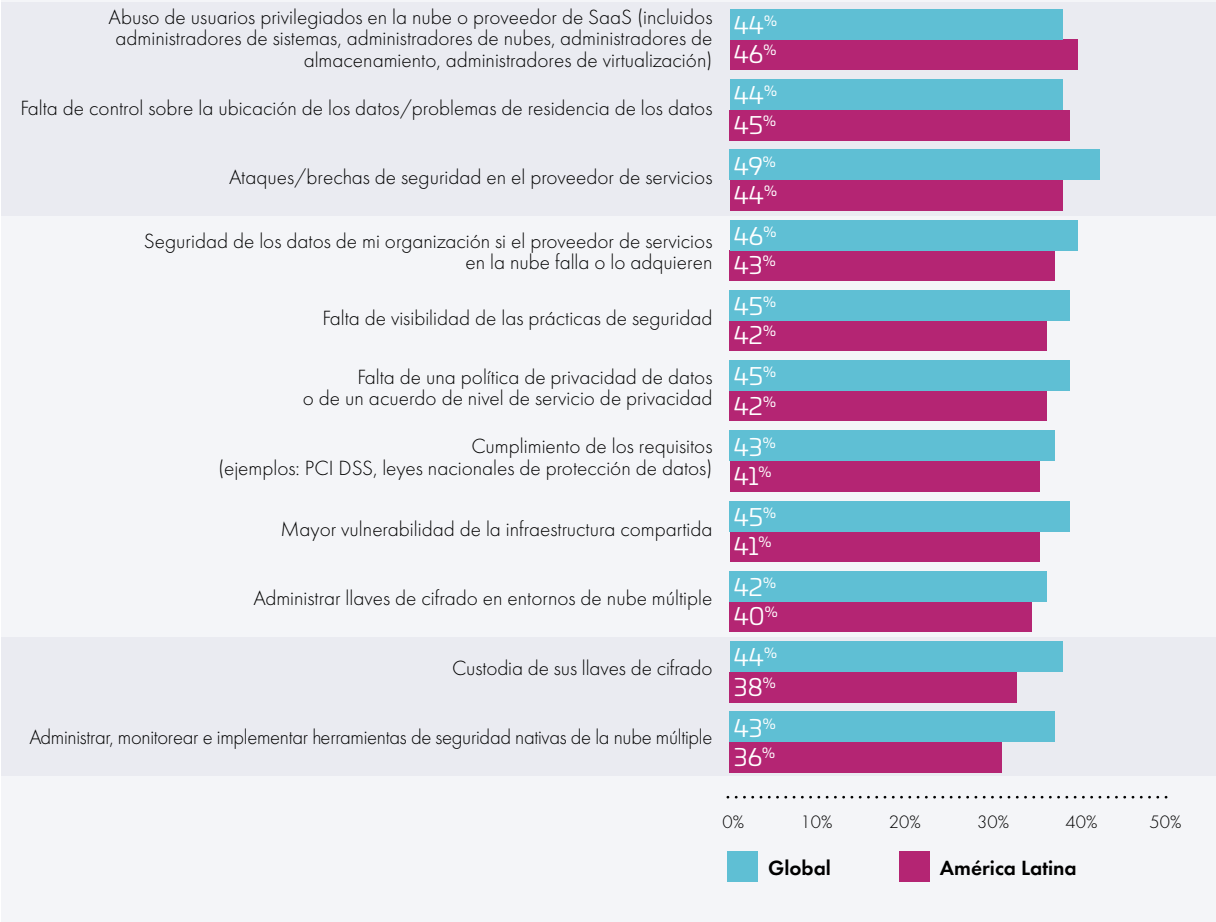
Casi la mitad (49%) de los datos corporativos de América Latina ahora se almacenan en la nube y una parte significativa de esos datos son confidenciales. A medida que los datos en la nube se acercan a un punto de inflexión, los departamentos de seguridad de TI deben ahora más que nunca, adoptar y ser dueños de su parte del modelo de responsabilidad compartida en la nube. Las organizaciones deben implementar las mejores prácticas de seguridad de los datos, ya que el proveedor de la nube a menudo no garantiza la seguridad al nivel de los datos. No obstante, el 41% de las organizaciones en América Latina considera que su estrategia en la nube tiene un impacto sobre sus planes para mejorar su postura de ciberseguridad. Por otra parte, el 27% de las organizaciones de la región considera la adopción de la nube como su iniciativa principal o el objetivo final para lograr una postura de seguridad más sólida (fuente: Informe de Ciberseguridad de América Latina de IDC 2019).

Los encuestados latinoamericanos están preocupados por muchos problemas de la seguridad de los datos relacionados con la nube. Sin embargo, las organizaciones están más preocupadas por los problemas con sus proveedores de servicios en la nube, tales como el acceso de los proveedores a los datos, la falta de control sobre dónde residen los datos y las brechas en el proveedor. Aunque son preocupaciones válidas, la posibilidad real de que estos elementos provoquen problemas de seguridad es bastante baja. Estas mismas organizaciones están menos preocupadas por cuestiones sobre las que tienen control directo y que representan mayores vulnerabilidades potenciales, como la administración de llaves de cifrado (ver Figura 16). Es interesante que esta falta de atención a los temas sobre los que tienen control es aún mayor en América Latina que en la muestra global.

El 41%

de las organizaciones en América Latina considera que su estrategia en la nube tiene un impacto sobre sus planes para mejorar su postura de ciberseguridad.

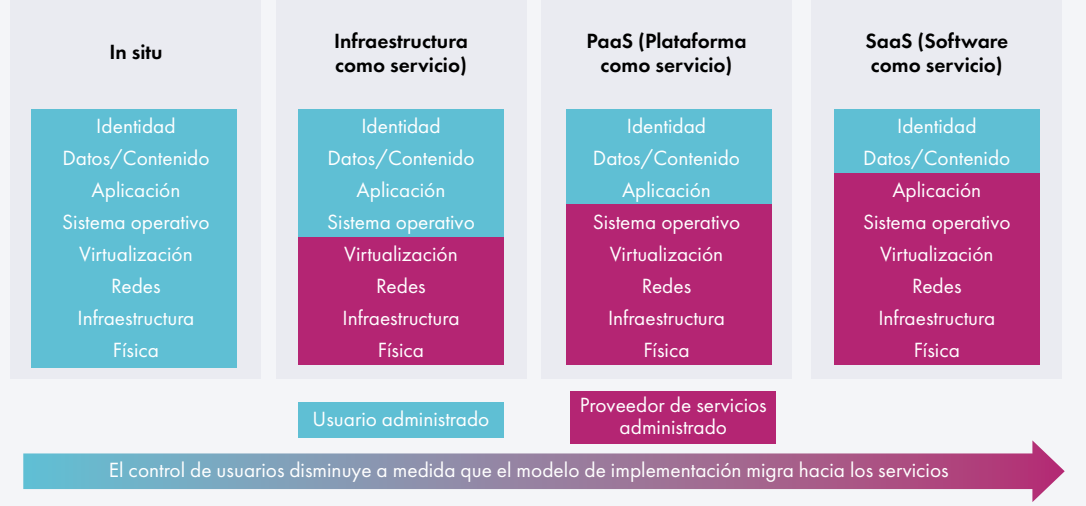
Figura 16 – Preocupaciones en materia de seguridad en la nube



Fuente: Encuesta del Informe de Thales sobre amenazas a datos 2020, IDC, noviembre de 2019

Esta discrepancia entre las amenazas que perciben los encuestados y aquellas en las que deberían centrarse realmente implica que los encuestados no han considerado completamente la seguridad de los datos en un mundo en el que la nube tiene prelación. Cada tipo de entorno de nube requiere un cambio en la responsabilidad de seguridad de las identidades, los datos, las aplicaciones, los sistemas operativos, la virtualización de servidores, la red, la infraestructura y el hardware. Las organizaciones latinoamericanas deben centrarse en la seguridad en la nube en la parte del modelo de responsabilidad compartida donde la organización puede influir en la seguridad de sus datos (ver Figura 17).

Figura 17 – Modelo de Responsabilidad Compartida



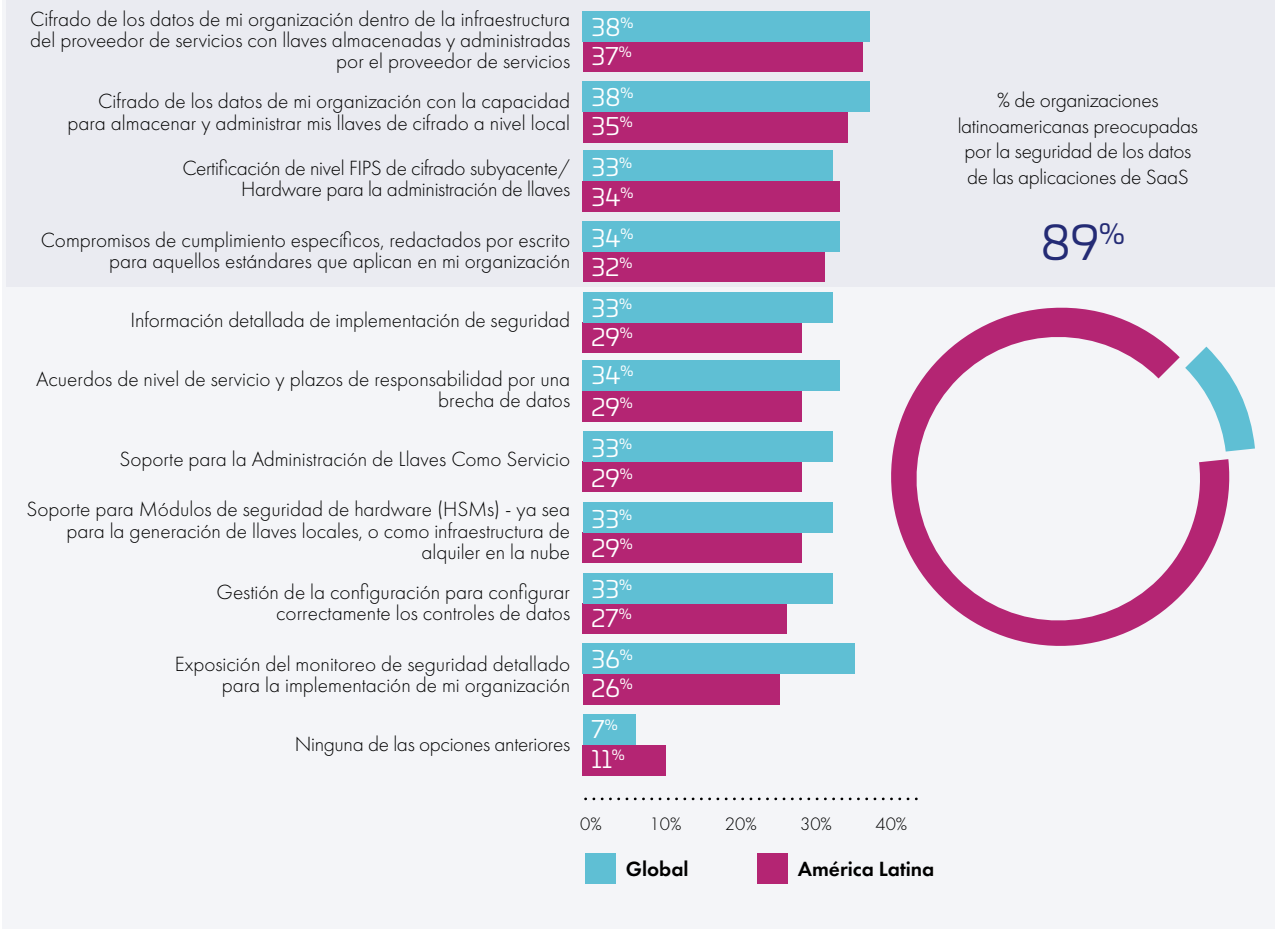
Fuente: IDC, Noviembre 2019

"Las organizaciones latinoamericanas deben enfocarse en la seguridad en la nube en la parte del modelo de responsabilidad compartida donde la organización puede influir en la seguridad de sus datos".

Las preocupaciones por la seguridad en la nube también crecen a medida que las organizaciones implementan más datos en entornos SaaS, IaaS y PaaS.

Según nuestro estudio, el 89% de los encuestados latinoamericanos tiene al menos algún nivel de preocupación sobre la seguridad de los datos de las aplicaciones SaaS. Los problemas de seguridad de SaaS abarcan una amplia gama de riesgos, con el cifrado de datos, el almacenamiento de llaves locales y la certificación de nivel FIPS a la cabeza de la lista (ver Figura 18).

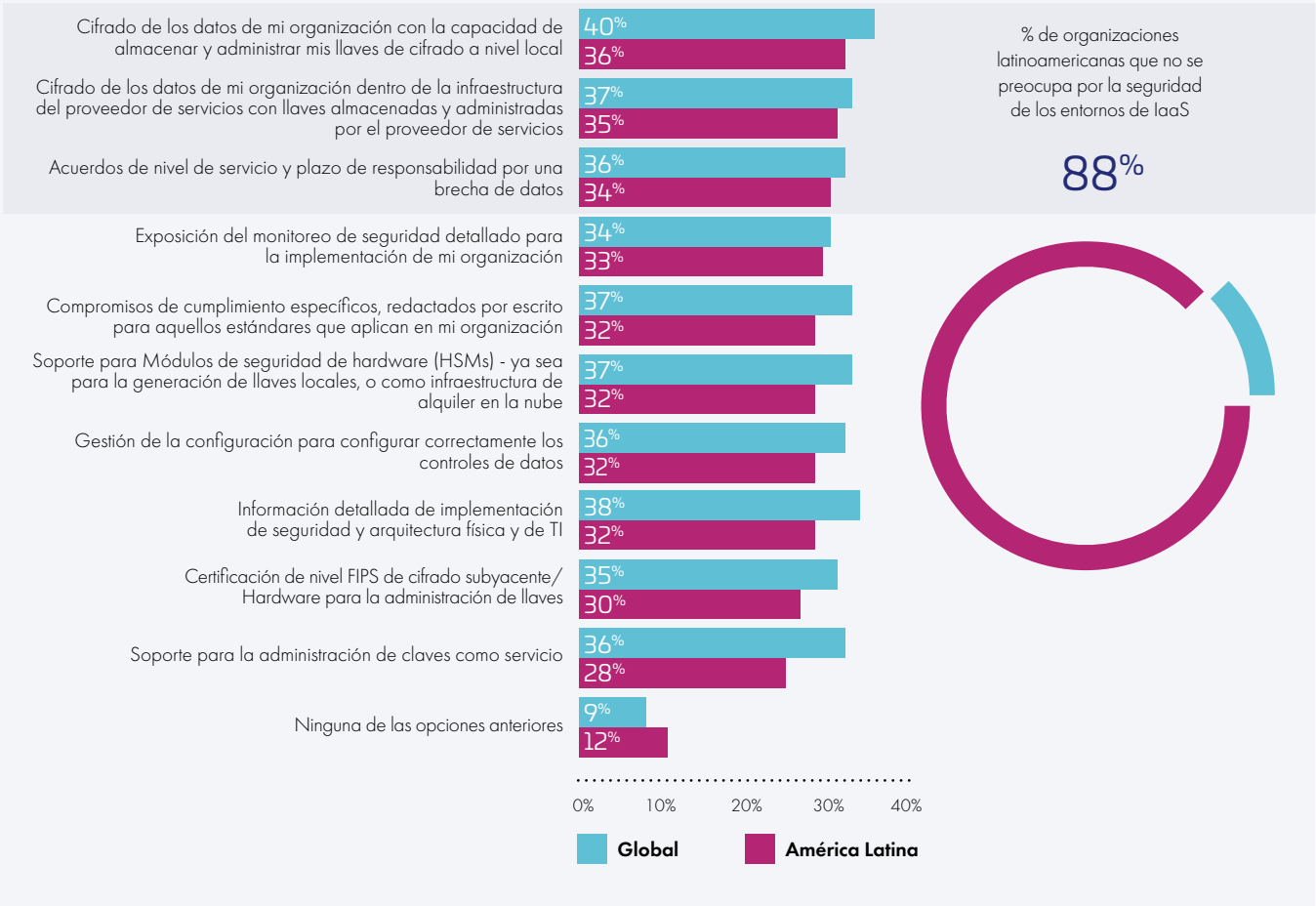
Figura 18 – Preocupaciones de seguridad en la SaaS



Fuente: Encuesta del Informe de Thales sobre amenazas a datos 2020, IDC, noviembre de 2019

El 88% de los encuestados latinoamericanos tiene al menos algunas preocupaciones sobre la seguridad de los datos de los entornos IaaS. De manera similar al SaaS, las preocupaciones de seguridad del IaaS también cubren una amplia gama de problemas con el almacenamiento de llaves locales, el cifrado de datos y los acuerdos de nivel de servicio como preocupaciones principales (ver Figura 19).

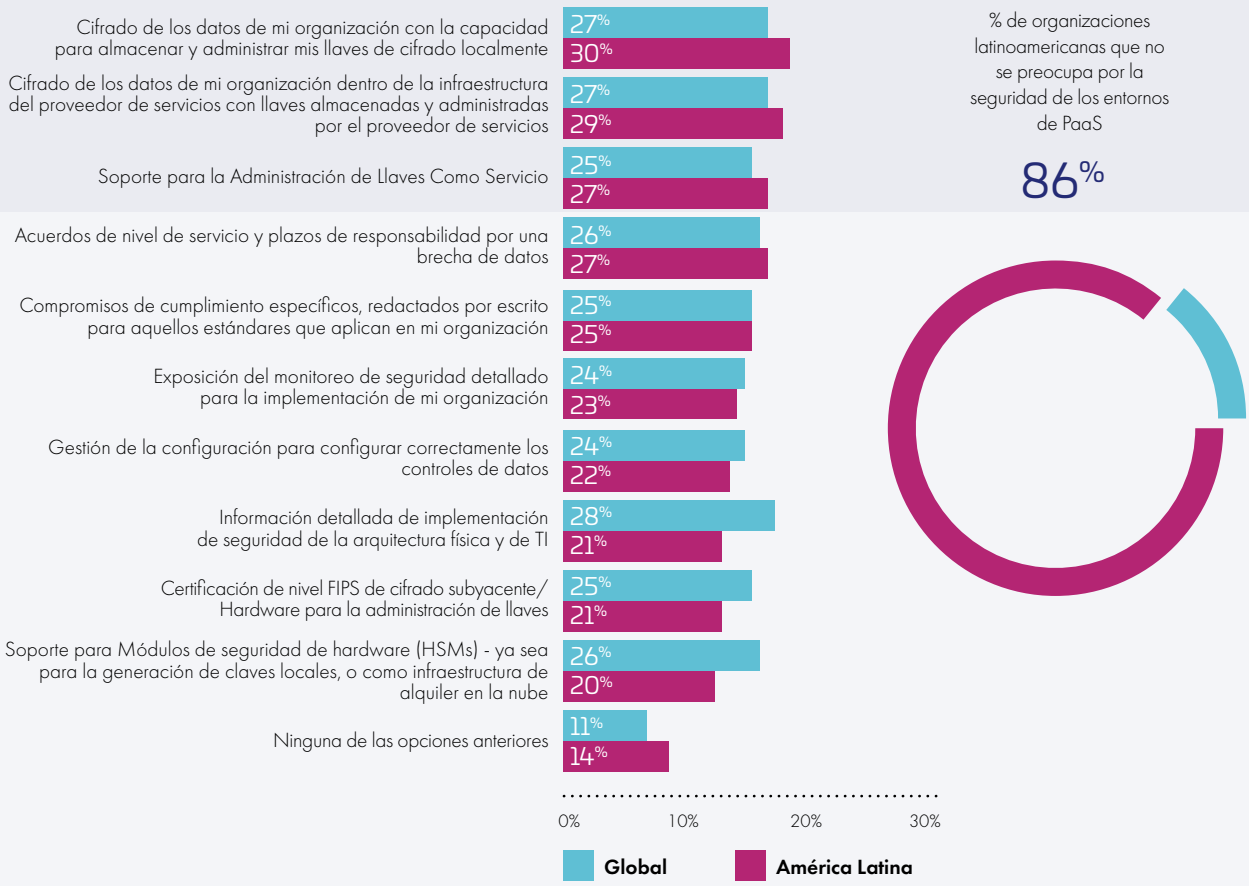
Figura 19 – Preocupaciones de seguridad en la IaaS



Fuente: Encuesta del Informe de Thales sobre amenazas a datos 2020, IDC, noviembre de 2019

El 86% de los encuestados latinoamericanos también tiene al menos alguna preocupación sobre la seguridad de los datos de los entornos PaaS con almacenamiento de llaves local, cifrado de datos, administración de llaves como servicio y acuerdos de nivel de servicio llevándose a cabo (ver Figura 20). Esta preocupación crecerá a medida que las organizaciones cambien su enfoque de las implementaciones de IaaS a PaaS para respaldar sus iniciativas de desarrollo y modernización de aplicaciones en DX.

Figura 20 – Preocupaciones de seguridad en la PaaS



Fuente: Encuesta del Informe de Thales sobre amenazas a datos 2020, IDC, noviembre de 2019

Un componente crítico de la transformación digital es el filo. DX crea oportunidades para nuevas tecnologías que involucran a las empresas y a los consumidores donde estos se encuentran, pero introduce nuevas complejidades a medida que las empresas llevan una cantidad cada vez mayor de datos y capacidad de cálculo al límite. Un aumento en las tecnologías de vanguardia exige que el gasto en seguridad se aleje de la seguridad empresarial tradicional e incluso se aleje de la nube. Los dispositivos móviles y el IoT son ejemplos específicos de esto, pero los macrodatos, los contenedores y las operaciones de desarrollo también están habilitando tecnologías que ayudan a expandir y personalizar la informática de filo.

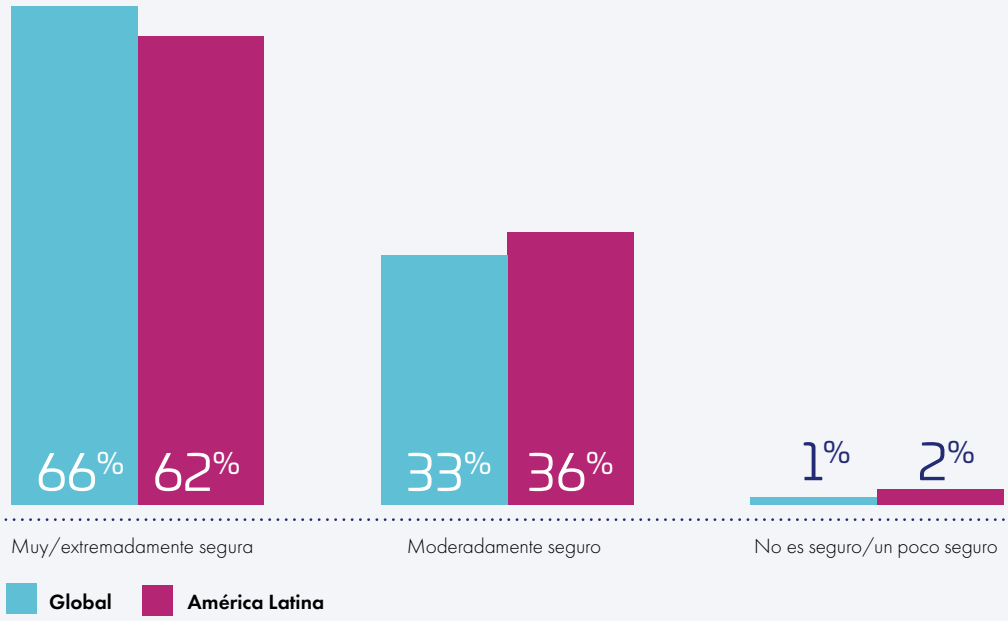
Con la expansión del uso de tecnologías DX, el descubrimiento de datos confidenciales y la administración de llaves asumen un papel aún más crítico en la seguridad de los datos. Sin embargo, las empresas latinoamericanas no perciben el descubrimiento de datos y la administración de llaves como las principales preocupaciones, lo que genera brechas potenciales en las prácticas de seguridad de datos.

El 98% de las organizaciones latinoamericanas en este estudio se siente al menos un poco seguras ya que envían más datos a las implementaciones de nuevas tecnologías, aunque en menor medida que la muestra global (99%). El sesenta y dos por ciento de los encuestados latinoamericanos se sienten muy o extremadamente seguros, en comparación con el 66% de la muestra global (ver Figura 21).

El 98%

de las organizaciones latinoamericanas siente al menos una seguridad moderada a medida que envían más datos a las implementaciones de nuevas tecnologías.

Figura 21 – Nivel de seguridad de las implementaciones de nuevas tecnologías



Fuente: Encuesta del Informe de Thales sobre amenazas a datos 2020, IDC, noviembre de 2019

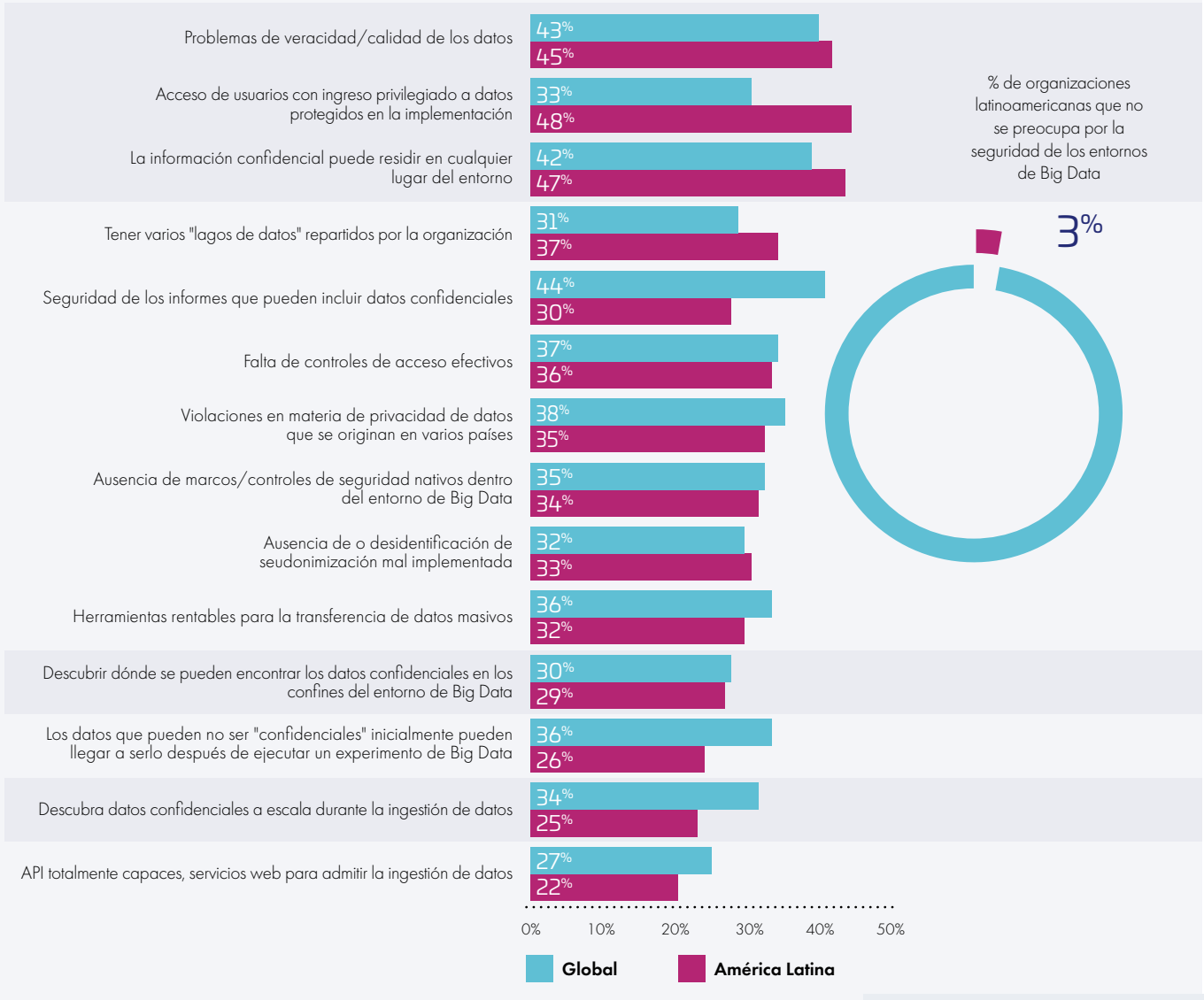
03

Preocupaciones de seguridad y métodos de mitigación según el entorno de datos

Preocupaciones de seguridad del Big Data

El 97% de los encuestados latinoamericanos están preocupados por la seguridad de los datos en sus entornos de Big Data. Las principales preocupaciones de seguridad de Big Data son la calidad de los datos, el acceso de usuarios privilegiados y los datos que residen en cualquier parte del entorno. Sin embargo, las preocupaciones sobre el descubrimiento de datos son muy bajas, incluido el descubrimiento de datos confidenciales dentro de su entorno de Big Data (29%) y durante la ingestión de datos (25%) (ver Figura 22). Los principales métodos para aliviar los problemas de seguridad de los macrodatos incluyen el cifrado de datos, las certificaciones en materia de cumplimiento y una autenticación más sólida.

Figura 22 – Preocupaciones de seguridad del Big Data



Fuente: Encuesta del Informe de Thales sobre amenazas a datos 2020, IDC, noviembre de 2019

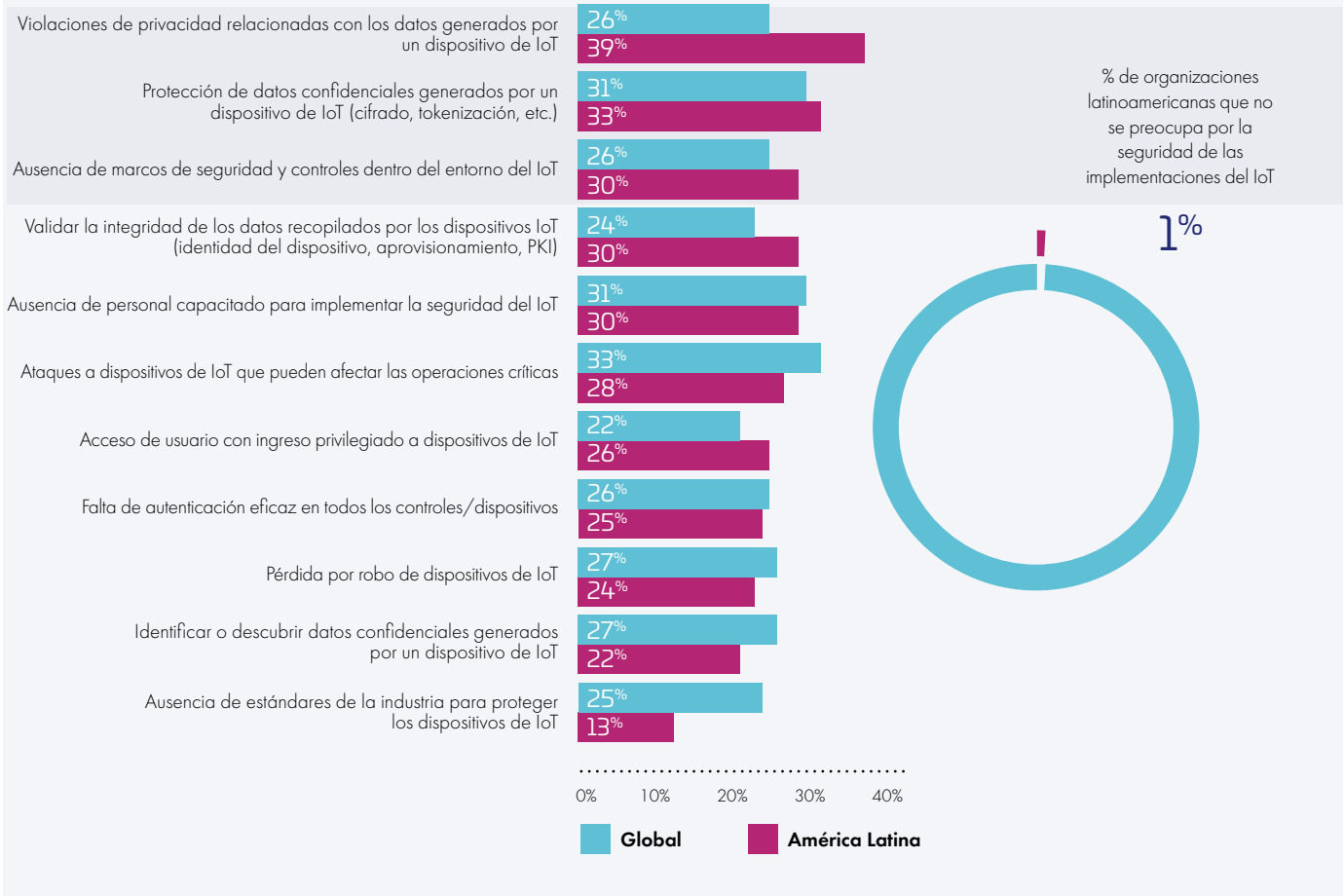
El 97%

de los encuestados latinoamericanos se encuentra preocupado por la seguridad de los datos en sus entornos de Big Data.

Preocupaciones de seguridad del Internet de las cosas (IoT)

Todas las organizaciones latinoamericanas de nuestra encuesta están preocupadas por la seguridad de los datos en entornos de IoT. Las preocupaciones de seguridad de IoT incluyen la privacidad de los datos, el cifrado/la tokenización y la falta de marcos de seguridad (ver Figura 23). El cifrado/la tokenización de datos, la autenticación de identidad digital y el antimalware se utilizan para abordar las principales preocupaciones en materia de seguridad de IoT. A medida que se implementan los dispositivos de IoT, la administración de llaves se hace cada vez más importante para implementar eficazmente la seguridad de la identidad y el cifrado de datos en estos dispositivos de IoT. Sin embargo, las organizaciones latinoamericanas se centran principalmente en la seguridad de la red y la aplicación de políticas para abordar el ángulo de seguridad dentro de los proyectos de IoT.

Figura 23 – Preocupaciones de seguridad del Internet de las cosas (IoT)



Fuente: Encuesta del Informe de Thales sobre amenazas a datos 2020, IDC, noviembre de 2019

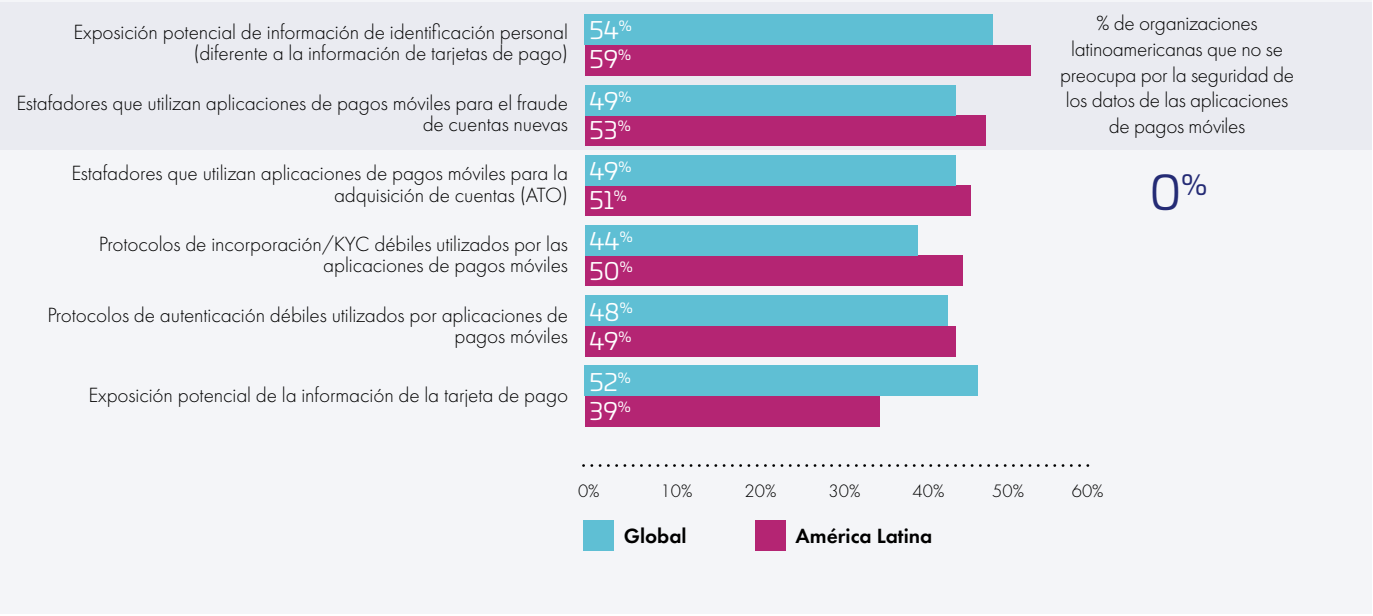
El 99%

de las organizaciones latinoamericanas tienen preocupaciones sobre la seguridad de los datos en sus implementaciones de IoT.

Problemas de seguridad de los pagos móviles

El cien por ciento de los encuestados latinoamericanos tiene al menos algunas preocupaciones sobre la seguridad de los datos con los pagos móviles. Los encuestados tienen muchas preocupaciones de seguridad con los pagos móviles y deberían tenerlas. La exposición a la PII y los estafadores que utilizan aplicaciones de pago móvil para el fraude de nuevas cuentas, así como la toma de control de cuentas son las principales preocupaciones (ver Figura 24). Se consideran muchas y variadas soluciones para abordar la seguridad de los pagos móviles. Las principales de ellas son los protocolos cifrados de red inalámbrica, las pantallas de bloqueo y el cifrado de datos.

Figura 24 – Problemas de seguridad de los pagos móviles



Fuente: Encuesta del Informe de Thales sobre amenazas a datos 2020, IDC, noviembre de 2019

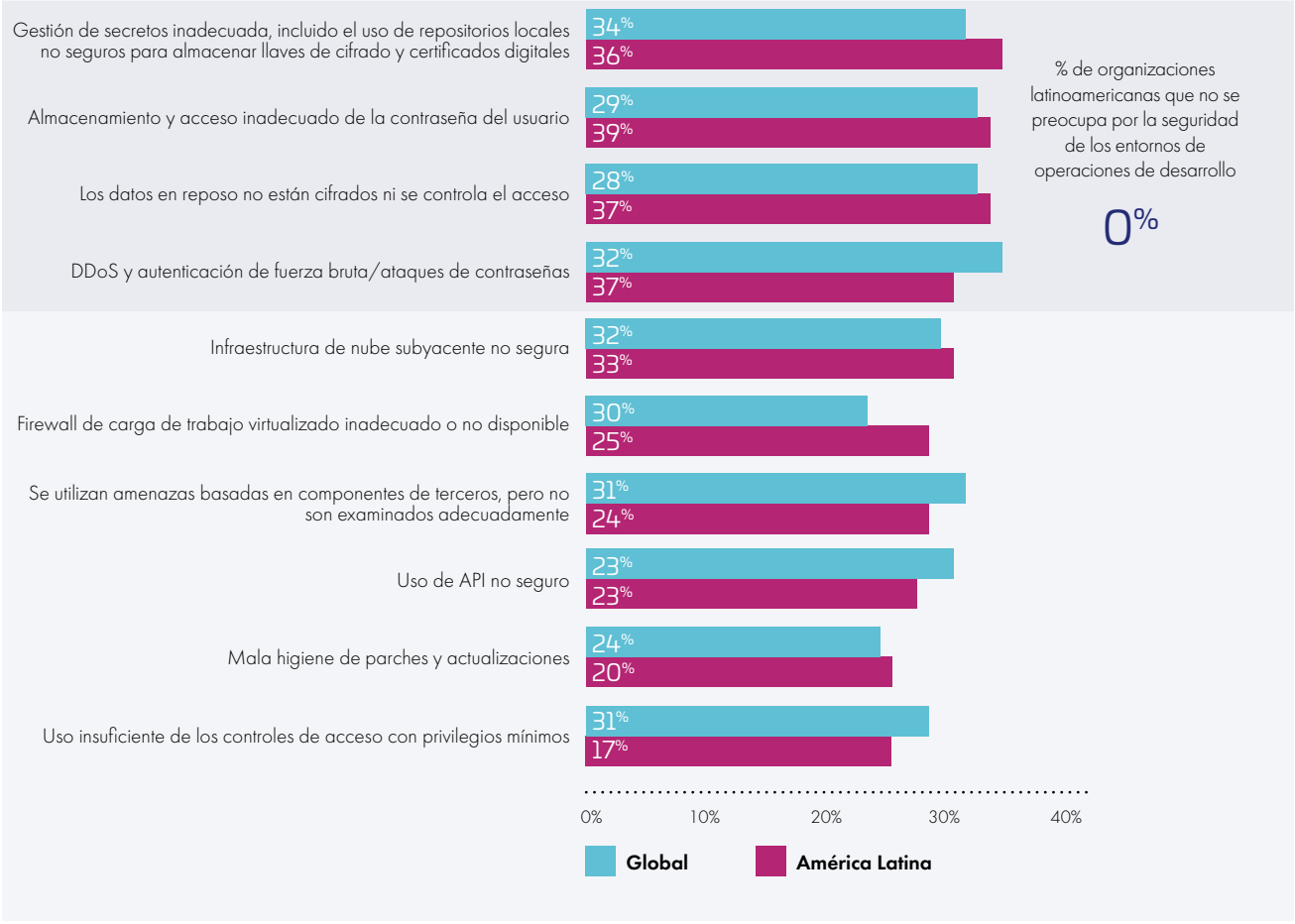
El 100%

de los encuestados latinoamericanos tiene preocupaciones sobre la seguridad de los datos con los pagos móviles.

Preocupaciones de seguridad en las operaciones de desarrollo

Cuando se trata de entornos de operaciones de desarrollo, el 100% de los encuestados latinoamericanos está preocupado por la seguridad de los datos de su entorno de operaciones de desarrollo. Los encuestados están más preocupados por la administración de secretos, el almacenamiento de contraseñas y el cifrado de datos en reposo (ver Figura 25). Se están considerando muchos enfoques diferentes para aliviar los problemas de seguridad de operaciones de desarrollo, liderados por el cifrado/la tokenización de los datos en reposo, la comunicación segura mediante HTTPS y la administración de acceso.

Figura 25 – Preocupaciones de seguridad en las operaciones de desarrollo



Fuente: Encuesta del Informe de Thales sobre amenazas a datos 2020, IDC, noviembre de 2019

El 100%

de los encuestados latinoamericanos se encuentra preocupado por la seguridad de los datos de sus entornos de operaciones de desarrollo.

04

Orientación de IDC/ Conclusiones clave

Las organizaciones latinoamericanas enfrentan desafíos de seguridad de datos cada vez más extensos y complejos como parte de la implementación de sus estrategias de transformación digital y en la nube, especialmente a la luz de las realidades actuales de la COVID-19 y la preparación para las eventualidades posteriores a una pandemia. A continuación, se incluyen las pautas y los puntos clave de IDC para ayudar a estas organizaciones a elevar su postura de seguridad de datos y desarrollar sus políticas en materia de seguridad:

- **Las soluciones de seguridad de datos, especialmente el cifrado, son fundamentales para permanecer alerta frente a la realidad del riesgo de datos posterior a la COVID-19.** Este punto es especialmente relevante ya que el trabajo actual de la migración desde el hogar ha obligado a los empleados a acceder y modificar mayores cantidades de datos corporativos fuera de las instalaciones, a veces en dispositivos BYO. Incluso si una organización pierde visibilidad sobre dónde residen los datos, se requieren tecnologías de seguridad de datos tales como el cifrado para proteger los datos corporativos de una manera independiente de la ubicación.

- **¿Estamos seguros de que los empleados regresarán a las oficinas?** Las organizaciones necesitan de nuevos métodos de seguridad de datos para proteger el panorama de TI posterior a la COVID-19 a medida que los datos migran desde las instalaciones de la empresa a la nube y regresan a las oficinas, ya que no hay certeza de que los empleados opten por regresar a la oficina. Los gobiernos latinoamericanos tienen diferentes capacidades económicas para detener la propagación de la pandemia y la infraestructura de salud también representa un desafío. Por lo tanto, podríamos esperar más tiempo para un gran retorno a la oficina y mientras tanto, las empresas deben ocuparse de sus preocupaciones de seguridad relacionadas con el trabajo remoto. La migración al trabajo desde casa puede ser permanente para muchos. La protección de datos posterior a la COVID-19 comienza con el cifrado, pasa al cifrado inteligente con controles de acceso incorporados y finalmente, se convierte en una gestión de derechos integrada y una prevención integral de la pérdida de datos basada en adoptar un enfoque de acceso basado en privilegios mínimos a los datos y aprovisionado según las funciones por ricas plataformas de identidad, ya que en muchos casos de uso, el perímetro posterior a la COVID-19 reside en los datos en sí.

- **Invierta en herramientas de seguridad de datos modernas, híbridas y basadas en la nube múltiple que hagan que el modelo de responsabilidad compartida funcione a medida que las organizaciones latinoamericanas buscan ponerse al día en iniciativas de transformación digital.** América Latina va rezagada de otras regiones en términos de transformación digital y necesitará superar a otros países a medida que apliquen la DX para transformar su negocio en el futuro, especialmente cuando buscan adaptarse a los cambios provocados en la economía actual por la COVID-19. Las organizaciones deben centrarse en soluciones que puedan simplificar el panorama de la seguridad de los datos y reducir la complejidad en múltiples entornos de nube y heredados, así como en tecnologías modernas de transformación digital basadas en la nube. En un modelo de responsabilidad compartida, las empresas no deben depender demasiado de los proveedores de servicios para las medidas de seguridad de los datos. Además, las organizaciones deben considerar todos los elementos de seguridad de datos directamente bajo su control, como identidad, cifrado (tanto en tránsito como en reposo), administración de llaves, tokenización y prevención de pérdida de datos.

- **Considere un modelo Zero Trust para proteger los datos.** Las organizaciones aún se centran en la seguridad de la red, ya que su objetivo es controlar el acceso en el perímetro. La seguridad de los datos debe ir más allá de esa ventaja tradicional, ya sea en la nube, en entornos virtuales, en centros de datos o en otras tecnologías DX. Estos entornos de datos requieren un modelo Zero Trust más persistente que no abdica de la seguridad de los datos como un problema de otra persona.

- **Aumente el enfoque en las soluciones de descubrimiento de datos y la centralización de la administración de llaves para fortalecer la seguridad de los datos.** Las preocupaciones sobre la seguridad de los datos deberían evolucionar a medida que el perímetro se expande con una mayor adopción de entornos de Big Data, dispositivos de IoT, pagos móviles, contenedores y entornos de operaciones de desarrollo. Un mayor énfasis en el descubrimiento de datos confidenciales en estos entornos, así como en los entornos existentes, refuerza la postura de seguridad de los datos al saber dónde se encuentran los datos confidenciales y cómo acceder a ellos. Además, el cifrado de datos confidenciales es fundamental y las organizaciones deben centralizar la administración de llaves para ayudar a simplificar el cifrado en entornos que de otro modo serían complejos.

- **El impacto de la computación cuántica en la criptografía está en el horizonte.** La seguridad de los datos no es más fácil ya que el poder de la computación cuántica puede exponer datos confidenciales más temprano que tarde. Las organizaciones deben comenzar a planificar su infraestructura y los ajustes de administración de llaves para contrarrestar los cambios fundamentales en la criptografía provocados por la computación cuántica.

- **Concéntrese en los vectores de amenazas correctos.** Sí, los malos actores están desarrollando sus métodos a diario. Los profesionales de la seguridad deben evolucionar continuamente para adaptarse. Pero enfóquese en los vectores de amenazas que están bajo su control directo. Tenga cuidado con el aprovisionamiento excesivo de la cantidad y la amplitud de cuentas tanto internas como externas con los proveedores de servicios

Arboretum Plaza II, 9442 Capital of Texas Highway North,
Suite 100, Austin, TX 78759 USA
Tel: +1 888 343 5773 o +1 512 257 3900
Fax: +1 954 888 6211 | correo electrónico: CPL_Sales_AMS_TG@thalesgroup.com

> cpl.thalesgroup.com <

cpl.thalesgroup.com/latam-data-threat-report

#2020DataThreat

Oficinas en Argentina, Brasil, Colombia y México