

SUPLEMENTO SOBRE AMÉRICA LATINA

INFORME DE AMENAZAS A DATOS DE 2023

Perspectivas y caminos hacia
la soberanía digital y la transformación

Principales conclusiones

En este informe, compartimos las principales conclusiones del estudio del Informe Global de Amenazas a Datos, enfocado en la región de América Latina, y examinaremos brevemente las oportunidades y desafíos de la soberanía digital, así como las recomendaciones para el futuro. Sin demasiada sorpresa, muchos de los resultados de este estudio estuvieron muy cerca de las respuestas globales; no obstante, destacaremos las principales diferencias.



Solo somos humanos:

la causa principal de las brechas de datos en la nube es el error humano.

Como respuesta a esto, las empresas están empoderando a sus usuarios para que eviten errores. La fuerte adopción de la autenticación de múltiples factores (MFA) en América Latina ha aumentado al 62 %. Además, el 30 % de los encuestados identifican a la administración de identidad y acceso (IAM) como la tecnología de seguridad más efectiva para proteger a los datos confidenciales de los ciberataques, lo cual indica un creciente enfoque en la prevención del error humano como fuente de debilidades de seguridad en la región.

62%

Si bien las actitudes internas hacia la seguridad están mejorando, los resultados en materia de seguridad no acompañan.

La amplia mayoría (87 %) de los encuestados de América Latina confiaría sus datos personales a los sistemas de sus organizaciones.



Si bien el 46 % responde que sufrió una brecha en los últimos 12 meses, esto representa 9 puntos porcentuales más que la cifra global y solo 3 puntos porcentuales más que la encuesta de América Latina de 2022. Esto indica que, mientras que la región continúa teniendo porcentajes de brechas más altos que los globales, los aumentos no son significativos en términos de comparaciones anuales. Sin embargo, queda claro que hay trabajo por hacer para reducir los porcentajes de las brechas.

La multinube es una realidad, independientemente de la madurez de la nube.

Más de cuatro quintos (83 %) de las empresas de América Latina tiene entornos de producción en más de una nube pública, 4 puntos porcentuales más que el porcentaje global, con un promedio de 2,3 proveedores de nube por organización, lo que guarda similitud con los resultados globales.



La soberanía digital es una iniciativa estratégica emergente.

98%

de los encuestados de América Latina dice que designar o cambiar la localización y la jurisdicción de los datos o implementar el cifrado de todos los datos son medidas aceptables para lograr diversos niveles de soberanía digital.

69%

de las organizaciones de América Latina tiene, al menos, cinco sistemas de administración de claves empresariales, 7 puntos porcentuales más que los resultados globales (62 %), generando así mayor complejidad.



La concientización de los riesgos relativos a la nube se está emparejando con la adopción de la nube.

76%

de los encuestados de América Latina manifiestan preocupaciones de seguridad sobre el 5G y, de estos, la mayoría afirma que proteger las identidades de las personas y los dispositivos que se conectan con las redes 5G es su prioridad, lo que resulta similar a las respuestas globales. Los encuestados de América Latina clasifican a la infraestructura de la nube (consolas de administración, herramientas de automatización y procesos de implementación) y a la identidad (robo de credenciales e identidad y falsificación de credenciales) como los objetivos número uno y número dos de los ciberataques.

Resultados dispares cuando se trata de luchar contra el ransomware.

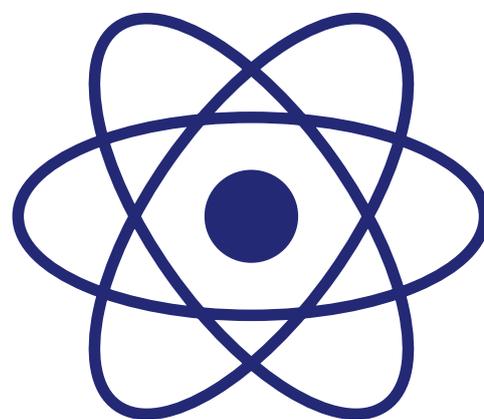


60%



24%

El 60 % de las organizaciones de América Latina tiene un plan formal de ransomware, lo cual representa un aumento significativo desde 2022 (42 %) cuando se realizó la consulta por primera vez. Un cuarto (24 %) de los encuestados de América Latina indicó que ha sufrido un ataque de ransomware, apenas más alto que el porcentaje global y 8 puntos porcentuales más que en 2022. No es de extrañar que quienes informaron un impacto significativo por los ataques de ransomware también hayan aumentado 7 puntos porcentuales en América Latina, mientras que los resultados globales indican un aumento de 2 puntos porcentuales.



La criptografía poscuántica avanza desde el ámbito académico hacia el mundo real.

67%

de los encuestados de América Latina declara que el descifrado de la red es la amenaza de seguridad de mayor preocupación de la computación cuántica, lo cual se asemeja al promedio global.

Cambiar la normativa y los eventos externos demandará respuestas para la seguridad de los datos.

82%

Más de cuatro de cada cinco (82 %) encuestados de América Latina está muy o un poco preocupado porque la soberanía de los datos o la normativa en materia de privacidad afectará los planes de implementación en la nube de su organización. Más de la mitad (55 %) está de acuerdo con que es más complejo administrar la normativa en materia de privacidad y protección de datos en un entorno de nube que en las redes propias; porcentaje apenas más bajo que el promedio global.

Anticipando la soberanía digital

La anticipación de la soberanía digital es un tema central para las empresas. La soberanía digital da a las empresas mayor libertad con los datos, hardware y software usados en sus propuestas y servicios. Permite a las empresas localizar de manera más efectiva el cumplimiento de las leyes de privacidad para mantener la custodia segura de los datos de información confidencial y públicamente identificable a fin de cumplir con diferentes normativas en materia de privacidad, seguridad de datos y resiliencia. De este modo, la soberanía digital representa una oportunidad significativa para que las empresas optimicen sus sistemas y arquitecturas, al tiempo que sirven mejor a las partes interesadas y a los ciudadanos.

El 82 % de los encuestados de América Latina está algo preocupado o muy preocupado porque los planes de implementación en la nube puedan ser afectados por la soberanía de los datos o la normativa de privacidad, un porcentaje similar al global.

En respuesta, las empresas necesitan comprender y simplificar sus estrategias de seguridad de datos multinube. Casi todos los encuestados (98 %) creen que designar la localización o la jurisdicción de los datos o implementar el cifrado total de los datos son métodos aceptables de responder a los requisitos variables de la soberanía digital o de la nube.

Casi dos tercios (64 %) de los encuestados de América Latina usa administradores de claves o claves de cifrado de proveedores de servicios en la nube y, de este modo, dependen de ellos y no logran su soberanía digital.

Las empresas necesitan simplificar y estar preparadas para ser flexibles con una variedad de esquemas de cifrado para responder a diferentes requisitos operativos y de soberanía de los datos. Más de la mitad (64 %) de las empresas encuestadas de América Latina ha delegado todos o la mayoría del control de las claves de cifrado a sus proveedores de servicios en la nube, lo que demuestra un incremento de 19 puntos porcentuales desde 2022 (45 %).

82%

de los encuestados de América Latina está algo preocupado o muy preocupado porque los planes de implementación en la nube puedan ser afectados por la soberanía de los datos o la normativa de privacidad, un porcentaje similar al global.

64%

de los encuestados de América Latina usa administradores de claves o claves de cifrado de proveedores de nube y, de este modo, dependen de ellos y no logran su soberanía digital.

Volver a lo básico

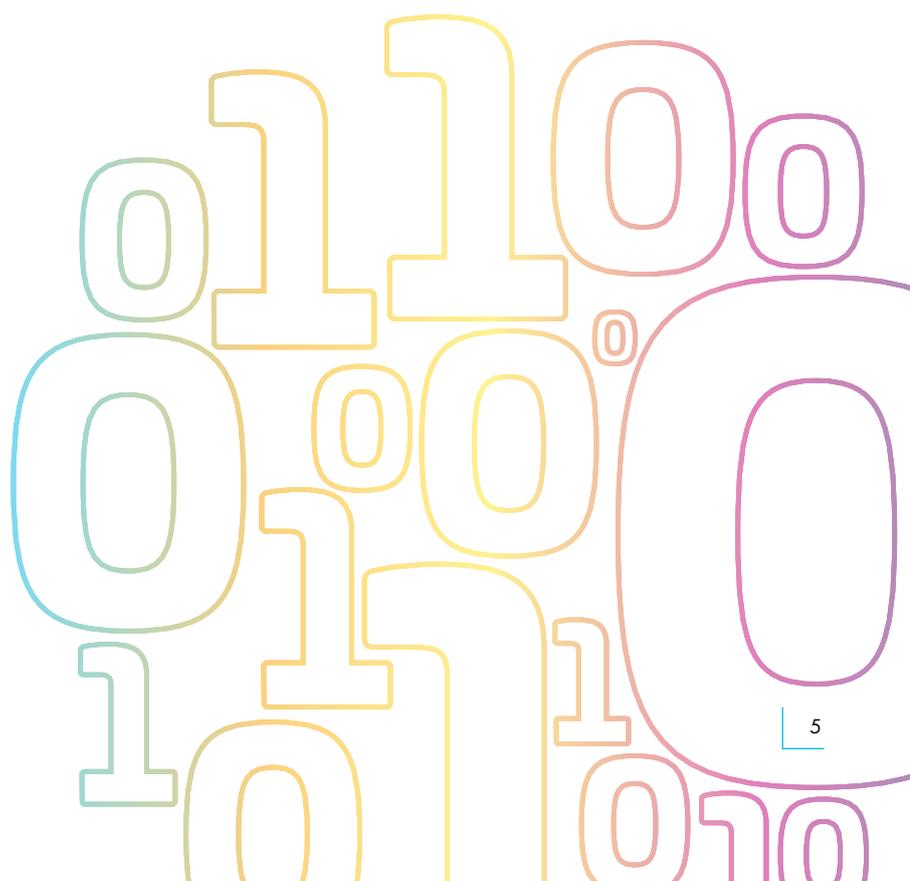
La colaboración con otras partes interesadas, tales como consumidores, socios, clientes y organismos reguladores, ofrece una mejor aceptación de la seguridad de los datos. Las iniciativas de seguridad de los datos pueden originar acciones no tradicionales; por lo tanto, se necesitan nuevos modelos de colaboración. Al habilitar datos seguros para todas las partes interesadas, las empresas pueden establecer una línea de base robusta y más flexible de controles para mercados que son cada vez más dinámicos.

La simplificación es clave. Dos tercios (67 %) de los encuestados de América Latina tiene de cinco a diez administradores de claves, lo cual aumenta la complejidad y el costo de la gobernanza uniforme de los datos en múltiples nubes. Esto indica un aumento de 14 puntos porcentuales desde 2022.

La soberanía digital representa una oportunidad a corto y a largo plazo para las empresas. Si bien la normativa cambiante en materia de datos requiere respuestas más inmediatas, lograr la independencia de los datos, la operación y el software a largo plazo de cualquier proveedor de servicios en la nube le brinda a la empresa las bases para incorporar nuevas tecnologías de nube para crecer estratégicamente. Las empresas que mantienen más controles de seguridad de los datos y no dependen de un único proveedor de servicios en la nube pueden aplicar controles más confiables en el entorno con el mejor valor de ejecución.

67%

de los encuestados de América Latina tiene de cinco a diez administradores de claves, lo cual aumenta la complejidad y el costo de la gobernanza uniforme de los datos en múltiples nubes. Esto indica un aumento de 14 puntos porcentuales desde 2022.



Acerca de este estudio

Esta investigación se basó en una encuesta global en línea a 2889 participantes, que se llevó a cabo durante noviembre y diciembre de 2022 en poblaciones específicas de cada país y que tuvo como objetivo a profesionales de la seguridad y la administración de TI. Además de los criterios relativos al nivel de conocimiento sobre el tema general de la encuesta, los criterios de selección excluyeron a aquellos encuestados que indicaron su afiliación a organizaciones con ingresos anuales de menos de 100 millones de dólares estadounidenses (y con ingresos de 100 a 250 millones de dólares estadounidenses en países seleccionados). Esta investigación se realizó como un estudio observacional y no realiza afirmaciones causales. Se extrajeron datos del estudio global de 206 encuestados de Brasil y México.

S&P Global
Market Intelligence

Fuente: Encuesta personalizada del Informe de Amenazas a Datos de 2023 de S&P Global Market Intelligence, encargada por Thales.

Patrocinado por



THALES
Building a future we can all trust

Para conocer la ubicación de todas las oficinas y la información de contacto,
visite cpl.thalesgroup.com/contact-us.

cpl.thalesgroup.com/data-threat-report

