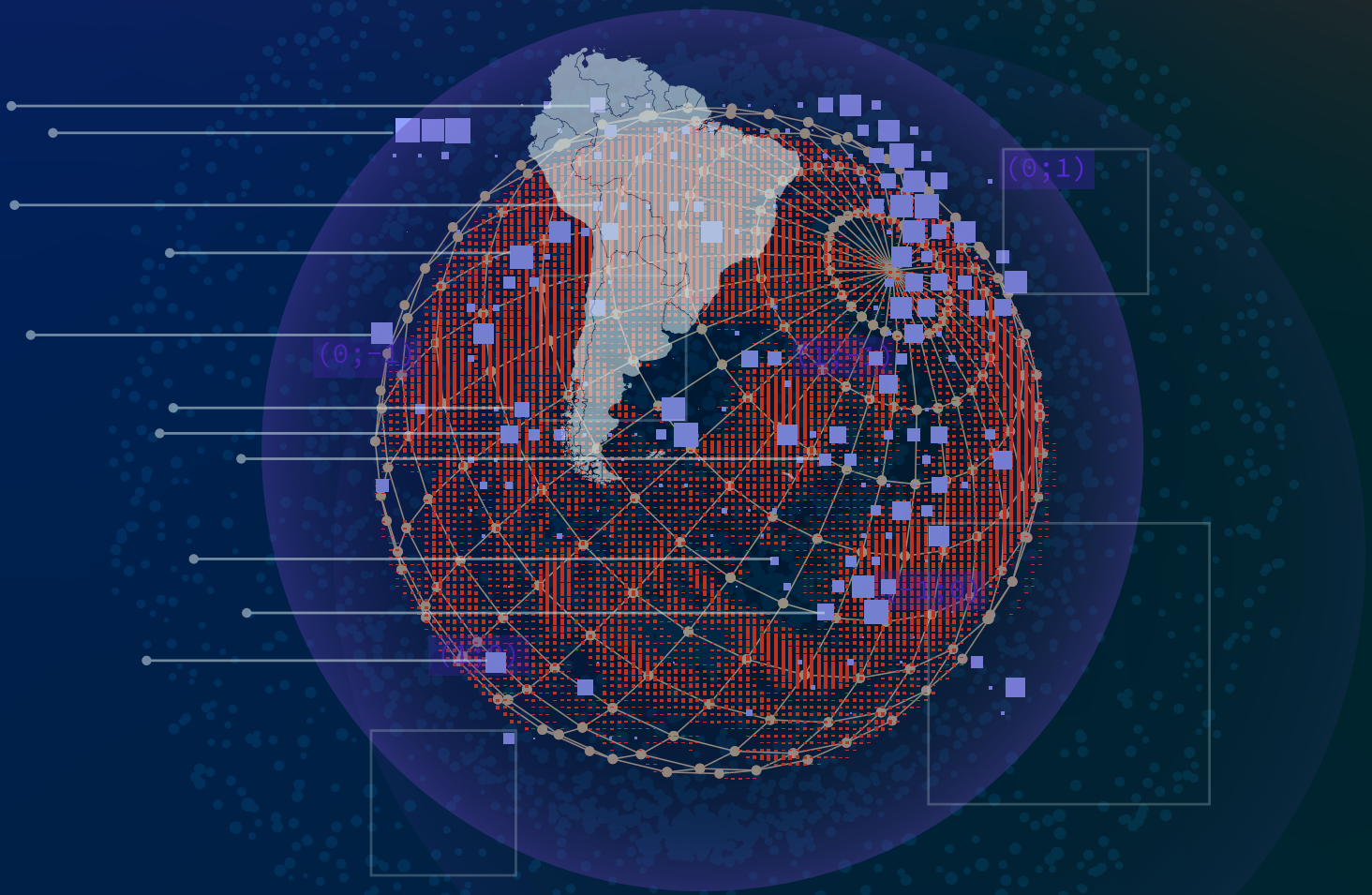
knowbe4

Informe de evaluación comparativa del phishing por industria

América del Sur 2026



Cómo enfrentar la nueva frontera del riesgo humano impulsada por la IA

Reducir el riesgo de phishing es fundamental para proteger de manera eficaz a la fuerza laboral digital.

Todo ataque exitoso depende de que una persona realice una acción específica: hacer clic en un enlace, descargar un archivo adjunto o entregar sus credenciales. Si un correo electrónico de phishing logra eludir las defensas técnicas, el ataque aun así fracasa si quien lo recibe tiene el instinto de reportarlo, eliminarlo o simplemente ignorarlo.

Si bien las organizaciones deben seguir reforzando las barreras técnicas mediante soluciones de seguridad del correo electrónico impulsadas por IA, los datos de este informe demuestran que una reducción significativa del riesgo proviene de implementar una capacitación en concientización sobre seguridad (SAT, por sus siglas en inglés) basada en las prácticas recomendadas.

A medida que las organizaciones incorporan agentes de IA además del personal humano, la superficie de ataque crece más allá del alcance para el que fueron diseñados los controles técnicos tradicionales. La SAT no solo es la herramienta más eficaz para fortalecer la seguridad de la fuerza laboral digital, sino que también constituye la base para desarrollar la cultura de la seguridad y la vigilancia organizacional necesarias en la gestión de los riesgos que introduce una fuerza laboral integrada por personas y agentes de IA.

Evaluación comparativa: el primer paso hacia la resiliencia

Una estrategia eficaz de mitigación de riesgos comienza con una comprensión clara del perfil de riesgo específico de su organización. Para lograr avances concretos, debe saber cómo se compara su fuerza laboral con la de organizaciones de la misma industria, tamaño y región geográfica. Solo al identificar quiénes son más susceptibles será posible implementar intervenciones de seguridad oportunas y personalizadas, como capacitaciones a medida y asesoramiento en tiempo real, necesarias para modificar los comportamientos.

Nuestro informe anual de evaluación comparativa del phishing por industria proporciona los datos esenciales para dar ese primer paso. Para la edición 2026, realizamos un análisis exhaustivo de 42 millones de simulaciones de phishing, 14 millones de personas usuarias únicas y 64 000 organizaciones. Durante un período de un año, analizamos el Phish-prone™ Percentage (PPP, predisposición para ser víctima de phishing) en 19 industrias y siete regiones geográficas.

Esta guía ofrece una descripción general de las principales conclusiones para América del Sur.

Cómo calculamos el porcentaje de Phish-prone

El PPP indica el porcentaje de miembros del personal de una organización que tienen probabilidades de ser víctimas de ataques de phishing o de ingeniería social.

Fase uno

Resultados iniciales de la prueba de seguridad contra el phishing

Antes de que se lleve a cabo cualquier capacitación de KnowBe4, enviamos un simulacro de phishing inicial. Esto se usa para identificar riesgos y calcular el PPP de referencia de una organización.

Fase dos

Resultados de la prueba de seguridad contra phishing dentro de los 90 días posteriores a la capacitación

Los miembros del personal reciben la capacitación en concientización sobre seguridad de KnowBe4. Se envía otro simulacro para volver a calcular el PPP de la organización y medir la eficacia del programa de capacitación.

Fase tres

Resultados de la prueba de seguridad contra el phishing después de un año o más de capacitación continua

Al cabo de 12 meses de capacitación en concientización sobre seguridad de KnowBe4, se vuelve a calcular el PPP para seguir cuantificando la eficacia del programa de capacitación.

Referencias internacionales del phishing 2026

En la evaluación inicial, África registra el PPP regional más alto, con un 35,9 %, seguida de cerca por América del Norte, con un 34,5 %, y América del Sur, con un 31,5 %. Asia presenta el PPP inicial más bajo, con un 24,9 %, lo que sugiere una inversión previa relativamente mayor en capacitación en concientización sobre seguridad o un entorno de amenazas más homogéneo al momento de la primera evaluación.

Los resultados obtenidos a los 90 días son notablemente uniformes entre las distintas regiones y oscilan entre el 16 % y el 21,4 %, lo que indica que la capacitación inicial genera cambios de comportamiento similares a corto plazo, más allá del punto de partida.

Después de un año de capacitación continua, América del Sur alcanza el PPP regional más bajo, con un 3,3 %, seguida de América del Norte, con un 4 %. África continúa siendo la región más desafiante, con un 7,4 %.

	Fase 1 Resultados iniciales de la prueba de seguridad contra el phishing				**Fase 2** Resultados de la prueba de seguridad contra el phishing dentro de los 90 días posteriores a la capacitación				**Fase 3** Resultados de la prueba de seguridad contra el phishing después de un año o más de capacitación continua			
Tamaño de la organización	1-249	250-999	1000-9999	10 000+	1-249	250-999	1000-9999	10 000+	1-249	250-999	1000-9999	10 000+
Región												
África	28,9 %	30 %	34,6 %	39 %	26,6 %	28,1 %	24,8 %	14,7 %	3,9 %	15,1 %	9,1 %	3 %
Total	**35,9 %**				**21,1 %**				**7,4 %**			
Asia	23,1 %	27,8 %	28,4 %	21,6 %	18,6 %	18,9 %	19 %	12,6 %	6,6 %	6,4 %	5,8 %	3,4 %
Total	24,9 %				16 %				5,5 %			
Australia y Nueva Zelanda	24,6 %	28,5 %	32,7 %	54,5 %	23,9 %	24 %	18,5 %	16,7 %	5,7 %	5,5 %	4,8 %	4,3 %
Total	**33 %**				**21 %**				**5,3 %**			
Europa	23,5 %	26,1 %	29,6 %	38,1 %	20,8 %	22 %	21 %	21,6 %	4,70 %	4,5 %	6,6 %	4,7 %
Total	**31,1 %**				**21,4 %**				**5 %**			
América del Norte	25 %	29,5 %	35,4 %	44 %	21,7 %	21,9 %	20,3 %	16,6 %	4,3 %	3,9 %	3,8 %	4,2 %
Total	**34,5 %**				**20,1 %**				**4 %**			
América del Sur	26,6 %	25,4 %	33,6 %	32,9 %	23,7 %	21,5 %	18,4 %	12,8 %	7,2 %	3,6 %	2,2 %	2,8 %
Total	**31,5 %**				**17,7 %**				**3,3 %**			
Reino Unido e Irlanda	24,8 %	26,8 %	32,7 %	33,1 %	22,9 %	23,1 %	20 %	14 %	4,5 %	5,5 %	6,1 %	5,8 %
Total	**30,3 %**				**19,8 %**				**5,5 %**			

América del Sur 2026

Por Rafael Peruch Blauth, arquitecto de ventas

Introducción: El panorama de amenazas en América del Sur

El panorama de la ciberseguridad en América del Sur se encuentra en un punto de inflexión crítico. A medida que las organizaciones de toda la región atraviesan una rápida transformación digital, también quedan expuestas a un entorno de amenazas cada vez más agresivo y sofisticado. Las investigaciones en materia de seguridad identifican de manera constante a América del Sur como una de las regiones más atacadas del mundo, debido principalmente al potencial de monetización del fraude en la banca móvil, el ransomware y los correos electrónicos corporativos comprometidos (Business Email Compromise, BEC). Según el estudio Estado del ransomware de Kaspersky de 2026, esta región se convirtió en la más atacada por ransomware a nivel mundial en 2025, con un 8,1 % de las organizaciones afectadas. Ese riesgo se ve agravado por el uso malicioso de la inteligencia artificial, que permite incluso a personas sin conocimientos técnicos lanzar campañas de phishing realistas y personalizadas a gran escala.

Si bien las organizaciones tradicionalmente han centrado sus defensas en capas técnicas —como firewalls, detección en terminales y puertas de enlace seguras para el correo electrónico—, quienes llevan a cabo los ataques han adaptado sus estrategias y ahora se enfocan en el factor humano. La ingeniería social, en particular el phishing, sigue siendo el principal mecanismo de acceso inicial en América del Sur. Las personas atacantes aprovechan la incertidumbre económica regional, los cambios organizacionales y la tendencia cultural a ayudar para eludir los controles técnicos.

En comparación con mercados más consolidados, como América del Norte o Europa Occidental, las empresas sudamericanas enfrentan una vulnerabilidad adicional: la escasez de personal especializado en ciberseguridad, sumada a presupuestos históricamente más limitados para la gestión del riesgo del comportamiento. El factor humano ya no es una preocupación secundaria, sino que es la primera línea de defensa de la ciberseguridad moderna, debido a que un clic de un solo miembro del personal puede eludir defensas de hardware y software que representan millones de dólares.

Perfil de las organizaciones y de la industria

El Informe de evaluación comparativa del phishing por industria 2026 de KnowBe4 analiza datos regionales y segmenta el mercado sudamericano en cuatro grupos de organizaciones según el tamaño de su fuerza laboral: pequeñas (de 1 a 249 miembros del personal), medianas (de 250 a 999), grandes (de 1000 a 9999) y muy grandes (de más de 10 000).

La escala de una organización influye de manera significativa en su perfil de riesgo. En las empresas más pequeñas, la falta de personal dedicado a la seguridad hace que cada miembro a menudo desempeñe múltiples funciones, lo que genera distracciones que las personas atacantes aprovechan. En las organizaciones grandes y muy grandes, el elevado volumen de comunicaciones diarias permite que los correos electrónicos de phishing pasen inadvertidos entre los flujos de trabajo habituales.

A nivel mundial, las industrias con altos niveles de estrés y grandes volúmenes de datos presentan el mayor riesgo inherente. Los sectores de atención médica y farmacéutico, organizaciones sin fines de lucro, educación y seguros muestran de forma constante la mayor vulnerabilidad inicial, y las grandes organizaciones del sector de la salud alcanzan un PPP inicial de hasta el 54 %. En América del Sur, los sectores relacionados con infraestructura crítica, servicios financieros y comercio minorista enfrentan una presión constante de ingeniería social por parte de atacantes que buscan maximizar la interrupción operativa.

Análisis de los datos comparativos de referencia

Los datos de las organizaciones de América del Sur ofrecen una visión clara y cuantificable tanto del panorama de amenazas como del impacto de la capacitación continua en concientización sobre seguridad. El análisis realiza un seguimiento de la vulnerabilidad a lo largo de tres fases: fase 1 (evaluación inicial, antes de la capacitación), fase 2 (dentro de los 90 días posteriores a la capacitación) y fase 3 (después de un año o más de capacitación continua).

América del Sur	Fase 1 Resultados iniciales de la prueba de seguridad contra phishing	Fase 2 Resultados de la prueba de seguridad contra phishing dentro de los 90 días posteriores a la capacitación	Fase 3 Resultados de la prueba de seguridad contra el phishing después de un año o más de capacitación continua
1-249	26,6 %	23,7 %	7,2 %
250-999	25,4 %	21,5 %	3,6 %
1000-9999	33,6 %	18,4 %	2,2 %
10 000+	32,9 %	12,8 %	2,8 %
PPP promedio en organizaciones de todos los tamaños	**31,5 %**	**17,7 %**	**3,3 %**

Sin capacitación, las organizaciones de América del Sur registran un PPP promedio del 31,5 %; es decir, casi uno de cada tres miembros del personal interactuará con un correo electrónico malicioso. Las organizaciones grandes (33,6 %) y muy grandes (32,9 %) presentan el mayor riesgo inicial, lo que refleja la mayor superficie de ataque asociada a contar con una fuerza laboral más numerosa.

Dentro de los 90 días posteriores a la implementación de la capacitación, el promedio regional disminuye de forma significativa hasta el 17,7 %. La mejora más pronunciada a corto plazo se observa en las organizaciones muy grandes, cuyo PPP desciende del 32,9 % al 12,8 %, lo que demuestra que la concientización responde rápidamente a la capacitación inicial.

Después de un año o más de capacitación continua y pruebas de phishing simuladas, el PPP promedio regional desciende al 3,3 %, lo que representa una reducción de aproximadamente el 89 % con respecto al valor inicial. Las organizaciones grandes obtienen el mejor resultado a largo plazo, con un 2,2 %. Los datos demuestran claramente que la capacitación continua orientada a modificar comportamientos es la herramienta más eficaz para reducir el riesgo asociado al factor humano.

Conclusiones principales

Los controles técnicos por sí solos no son suficientes

Un PPP inicial del 31,5 % demuestra que los perímetros de seguridad técnicos no pueden compensar la vulnerabilidad humana. Si uno de cada tres miembros del personal es vulnerable, no se trata de si ocurrirá una violación de seguridad, sino de cuándo.

El crecimiento exige un enfoque sistemático

Las organizaciones grandes y muy grandes presentan la mayor vulnerabilidad inicial (33,6 % y 32,9 %). A medida que las organizaciones crecen, la descentralización de las comunicaciones requiere un programa formal y continuo de capacitación para mantener niveles de seguridad consistentes.

Una capacitación puntual no es suficiente

La mejora observada entre la fase 2 (17,7 %) y la fase 3 (3,3 %) demuestra que la capacitación anual o enfocada únicamente en el cumplimiento normativo no es suficiente. La capacitación continua convierte la vigilancia en materia de seguridad en un hábito, en lugar de limitarla al cumplimiento de una política.

El personal es un activo para la defensa

Reducir el riesgo regional a largo plazo al 3,3 % confirma el valor del concepto de firewall humano. Las simulaciones y la capacitación periódicas transforman al personal de un factor de riesgo en una primera línea de defensa eficaz.

El retorno de la inversión es cuantificable

Una reducción aproximada del 89 % en la vulnerabilidad al phishing durante un período de 12 meses constituye un sólido argumento de negocio para invertir en concientización sobre seguridad, ya que reduce directamente el riesgo de ransomware, interrupciones operativas, sanciones por incumplimiento y daños a la reputación.

Acerca de KnowBe4

KnowBe4 capacita a la fuerza laboral actual para que pueda tomar decisiones de seguridad más acertadas todos los días. Con la confianza de más de 70 000 organizaciones en todo el mundo, KnowBe4 es pionero en seguridad digital para la fuerza laboral, protegiendo tanto a agentes de IA como a personas. **La plataforma KnowBe4** ofrece simulación de ataques y capacitación, seguridad de la colaboración y seguridad de agentes impulsada por AIDA (Artificial Intelligence Defense Agents), además de un puntaje de riesgo propio. La plataforma aprovecha 15 años de datos de comportamiento para combatir amenazas avanzadas, como ingeniería social, inyección de prompts e IA oculta. AI proteger a personas y agentes, KnowBe4 lidera la industria en confianza y defensa de la fuerza laboral.

Obtenga más información en www.KnowBe4.com.

Follow us on Linkedin

Follow us on X

KnowBe4 Brazil | R. Gomes de Carvalho, 911 | Sala 208 - Vila Olímpia | CEP: 04547-003 | São Paulo-SP
Tel.: +55 (0800) 761 2668 | www.KnowBe4.com/es | Sales@KnowBe4.com

Los nombres de otros productos y empresas aquí mencionados pueden ser marcas comerciales o marcas comerciales registradas de sus respectivas empresas.

Copyright © 2026 KnowBe4 Todos los derechos reservados.