knowbe4

Relatório de benchmark de phishing por setor

América do Sul, 2026



Risco humano na era da IA: navegando por novas fronteiras

A redução dos riscos de phishing é fundamental para que a segurança da força de trabalho digital seja eficaz.

Todo ataque bem-sucedido depende de uma pessoa para executar uma ação específica, como clicar em um link, baixar um anexo ou informar suas credenciais. Mesmo que um e-mail de phishing consiga passar pelas defesas técnicas, o ataque não terá sucesso se quem o receber souber denunciá-lo, excluí-lo ou simplesmente ignorá-lo.

Embora as organizações devam continuar aprimorando as barreiras técnicas com soluções de segurança de e-mail assistidas por IA, os dados apresentados neste relatório comprovam que a redução significativa dos riscos é alcançada por meio do treinamento de conscientização em segurança (SAT) alinhado às melhores práticas.

À medida que as organizações expandem sua força de trabalho humana para incluir agentes de IA, a superfície de ataque aumenta de formas que vão além da capacidade dos controles técnicos tradicionais. O SAT não é apenas a maneira mais eficaz de fortalecer a segurança da força de trabalho digital; ele é a base para criar a cultura de segurança e a vigilância organizacional necessárias para gerenciar os riscos gerados pela força de trabalho composta por pessoas e pela IA.

Benchmark: o primeiro passo rumo à resiliência

Uma estratégia eficaz de mitigação de riscos começa com uma compreensão clara do perfil de risco específico da sua organização. Para gerar resultados concretos, você deve saber como sua força de trabalho se compara à de organizações do mesmo setor, do mesmo porte e da mesma região geográfica. Somente ao identificar quem está mais suscetível é que você conseguirá oferecer intervenções de segurança oportunas e personalizadas, como treinamentos sob medida e coaching em tempo real, necessárias para mudar comportamentos.

Nosso relatório anual de benchmark de phishing por setor fornece os dados essenciais para dar esse primeiro passo. Para esta edição de 2026, realizamos uma análise abrangente de 42 milhões de simulações de phishing, com 14 milhões de usuários únicos e 64 mil organizações. Durante o período de um ano, acompanhamos a Phish-prone™ Percentage (PPP) em 19 setores e 7 regiões geográficas.

Este guia oferece uma visão geral das principais descobertas relacionadas à América do Sul.

Como calculamos a Phish-prone Percentage

A PPP é a porcentagem de funcionários de uma organização que provavelmente será vítima de ataques de engenharia social ou phishing.

Fase 1

Resultados do teste de phishing de linha de base

Antes de qualquer treinamento da KnowBe4, enviamos uma simulação inicial de phishing. Essa simulação é usada para identificar os riscos e calcular a PPP de linha de base de uma organização.

Fase 2

Resultados do teste de phishing até 90 dias após o treinamento

Os funcionários recebem o treinamento de conscientização em segurança da KnowBe4. Outra simulação é enviada para recalcular a PPP da organização e medir a eficácia do programa de treinamento.

Fase 3

Resultados do teste de phishing depois de um ano ou mais de treinamento contínuo

Depois de 12 meses de treinamento de conscientização em segurança da KnowBe4, a PPP é calculada novamente para quantificar com mais precisão a eficácia do programa de treinamento.

Benchmarks internacionais de phishing em 2026

Na linha de base, a África registra a maior PPP regional, com 35,9%. Logo depois, vêm a América do Norte, com 34,5%, e a América do Sul, com 31,5%. A Ásia apresenta a menor linha de base, com 24,9%, o que sugere um investimento prévio relativamente maior em treinamentos de conscientização ou um ambiente de ameaças mais homogêneo no momento do primeiro teste.

Os resultados depois de 90 dias são muito parecidos entre as regiões, concentrando-se entre 16% e 21,4%, o que indica que o treinamento inicial gera mudanças comportamentais de curto prazo semelhantes, independentemente do ponto de partida.

Após um ano de treinamento contínuo, a América do Sul alcança a menor PPP regional, com 3,3%, seguida pela América do Norte, com 4%. A África continua sendo a região mais desafiadora, com 7,4%.

	Fase 1 Resultados iniciais do teste de phishing de linha de base				**Fase 2** Resultados do teste de phishing até 90 dias após o treinamento				**Fase 3** Resultados do teste de phishing depois de um ano ou mais de treinamento contínuo			
Porte da organização	De 1 a 249	De 250 a 999	De 1.000 a 9.999	Mais de 10.000	De 1 a 249	De 250 a 999	De 1.000 a 9.999	Mais de 10.000	De 1 a 249	De 250 a 999	De 1.000 a 9.999	Mais de 10.000
Região												
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%**			
Ásia	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%			
Austrália e Nova Zelândia	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%	4,7%	4,5%	6,6%	4,7%
Total	**31,1%**				**21,4%**				**5%**			
América do 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 do Sul	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%**			

Relatório de benchmark de phishing

América do Sul, 2026

por Rafael Peruch Blauth, arquiteto de vendas

Introdução: o panorama de ameaças na América do Sul

O panorama da segurança cibernética na América do Sul passa por um momento importante de inflexão. À medida que organizações de toda a região aceleram sua transformação digital, elas também ficam expostas a um ambiente de ameaças cada vez mais agressivo e sofisticado. Pesquisas na área de segurança apontam, de maneira consistente, a América do Sul como uma das regiões mais visadas em todo o mundo, algo impulsionado principalmente pela potencial monetização associada a fraudes em serviços bancários móveis, a ataques de ransomware e ao comprometimento de e-mail corporativo (Business Email Compromise, BEC). De acordo com o estudo State of Ransomware da Kaspersky, realizado em 2026, essa região tornou-se a mais visada por ataques de ransomware no mundo em 2025, com 8,1% das organizações sendo afetadas por ataques. Esse risco é agravado pelo uso da inteligência artificial como ferramenta de ataque, permitindo que até mesmo criminosos sem conhecimentos técnicos lancem campanhas de phishing realistas e personalizadas em grande escala.

Como as organizações inicialmente concentraram suas defesas nas camadas técnicas, como firewalls, detecção em pontos de extremidade e gateways seguros de e-mail, os agentes de ameaças se adaptaram e passaram a concentrar seus ataques no elemento humano. A engenharia social, em especial o phishing, continua sendo o principal vetor de acesso inicial na América do Sul. Para contornar os controles técnicos, os invasores exploram as preocupações econômicas da região, as mudanças organizacionais e a tendência cultural de prestar ajuda.

Em comparação com mercados maduros, como da América do Norte e da Europa Ocidental, as organizações da América do Sul enfrentam uma vulnerabilidade maior: a escassez de profissionais especializados em segurança cibernética, aliada a investimentos historicamente mais baixos em gerenciamento de riscos comportamentais. O fator humano deixou de ser uma preocupação secundária. Hoje, ele representa a linha de frente da segurança cibernética moderna, e um único clique de um funcionário pode contornar defesas de hardware e software que custaram milhões de dólares.

Perfil da organização e do setor

O Relatório de benchmark de phishing por setor de 2026 da KnowBe4 analisa dados regionais e segmenta o mercado da América do Sul em quatro grupos de organizações, com base no tamanho da força de trabalho: pequenas (de 1 a 249 funcionários), médias (de 250 a 999 funcionários), grandes (de 1.000 a 9.999 funcionários) e de porte empresarial (10.000 ou mais).

O porte da organização influencia significativamente seu perfil de risco. Nas empresas menores, a ausência de equipes de segurança dedicadas faz com que os funcionários geralmente exerçam várias funções, criando vetores de distração que podem ser explorados pelos invasores. Nas organizações de grande porte e de porte empresarial, o volume de comunicações diárias possibilita que e-mails de phishing se misturem aos fluxos de trabalho padrão.

Globalmente, os setores sujeitos a altos níveis de estresse e que lidam com grandes volumes de dados apresentam o maior risco inerente. Os setores de Saúde e produtos farmacêuticos, Organizações sem fins lucrativos, Educação e Seguros apresentam, de maneira consistente, a maior vulnerabilidade de linha de base, com organizações de grande porte do setor de saúde atingindo uma linha de base de pico de 54%. Na América do Sul, os setores que lidam com infraestruturas críticas, serviços financeiros e varejo enfrentam uma pressão contínua de ataques de engenharia social por parte de agentes que buscam causar a maior interrupção operacional possível.

Análise de dados de benchmark

Os dados das organizações da América do Sul oferecem um panorama claro e mensurável do panorama de ameaças e do impacto do treinamento contínuo de conscientização em segurança. A análise acompanha a vulnerabilidade em três fases: Fase 1 (linha de base inicial, antes do treinamento), Fase 2 (até 90 dias após o treinamento) e Fase 3 (depois de um ano ou mais de treinamento contínuo).

América do Sul	Fase 1 Resultados iniciais do teste de phishing de linha de base	Fase 2 Resultados do teste de phishing até 90 dias após o treinamento	Fase 3 Resultados do teste de phishing depois de um ano ou mais de treinamento contínuo
De 1 a 249	26,6%	23,7%	7,2%
De 250 a 999	25,4%	21,5%	3,6%
De 1.000 a 9.999	33,6%	18,4%	2,2%
Mais de 10.000	32,9%	12,8%	2,8%
PPP média entre organizações de todos os portes	**31,5%**	**17,7%**	**3,3%**

Sem treinamento, as organizações da América do Sul apresentam, em média, uma PPP de 31,5%. Isso significa que quase um em cada três funcionários irá interagir com um e-mail malicioso. As organizações de grande porte (33,6%) e as de porte empresarial (32,9%) apresentam o maior risco de linha de base, refletindo a maior superfície de ataque decorrente de um quadro de funcionários mais numeroso.

Até 90 dias após o treinamento, a média regional cai significativamente para 17,7%. A melhoria mais significativa de curto prazo ocorre nas organizações de porte empresarial, que apresentam queda de 32,9% para 12,8%, o que demonstra que a conscientização responde rapidamente à capacitação inicial.

Depois de um ano ou mais de treinamento contínuo e testes simulados, a média regional de PPP cai para 3,3%, uma redução de aproximadamente 89% em relação à linha de base inicial. No longo prazo, as organizações de grande porte registram o menor índice: 2,2%. Os dados são claros: o treinamento comportamental contínuo é a maneira mais eficaz de reduzir os riscos relacionados ao fator humano.

Pontos principais

Sozinhos, os controles técnicos não são suficientes

Uma PPP de linha de base de 31,5% demonstra que os perímetros técnicos não conseguem compensar a vulnerabilidade humana. Se um em cada três funcionários está suscetível, a questão não é se ocorrerá uma violação, mas quando.

O porte da organização exige uma abordagem sistemática

As organizações de grande porte e as de porte empresarial apresentam a maior vulnerabilidade inicial (33,6% e 32,9%). À medida que as organizações crescem, a descentralização das comunicações passa a exigir um programa estruturado e contínuo de treinamento para manter linhas de base consistentes de segurança.

Um único treinamento não é suficiente

A melhoria que ocorre da Fase 2 (17,7%) para a Fase 3 (3,3%) demonstra que treinamentos anuais ou realizados apenas para fins de conformidade não são suficientes. O treinamento contínuo faz com que a vigilância da segurança deixe de ser apenas uma política e passe a ser um hábito.

Os funcionários são um ativo de defesa

A redução do risco regional de longo prazo para 3,3% valida o conceito de firewall humano. Com treinamentos e simulações regulares, os funcionários deixam de ser um ponto de vulnerabilidade e passam a ser uma primeira linha de defesa eficaz.

O retorno sobre o investimento é mensurável

Uma redução de aproximadamente 89% na vulnerabilidade a ataques de phishing ao longo de 12 meses oferece uma boa justificativa para o investimento em conscientização em segurança, reduzindo diretamente o risco de ataques de ransomware, interrupções operacionais, penalidades por não conformidade e danos à reputação.

Sobre a KnowBe4

A KnowBe4 capacita a força de trabalho moderna a tomar decisões de segurança mais inteligentes todos os dias. Escolhida por mais de 70 mil organizações no mundo todo, a KnowBe4 é pioneira em segurança da força de trabalho digital, protegendo tanto agentes de IA quanto pessoas. **A Plataforma KnowBe4** oferece simulação de ataques e treinamento, segurança de colaboração e proteção de agentes com base na tecnologia AIDA (Artificial Intelligence Defense Agents) e em um nível de risco proprietário. A plataforma conta com 15 anos de dados comportamentais para combater ameaças avançadas, incluindo engenharia social, injeção de prompts e IA oculta. Ao proteger pessoas e agentes, a KnowBe4 é líder do setor em confiança e defesa da força de trabalho.

Mais informações em: www.KnowBe4.com/pt.

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.: (0800) 761 2668 | www.KnowBe4.com/pt | Sales@KnowBe4.com

Os nomes de outros produtos e empresas mencionados aqui são marcas comerciais e/ou marcas registradas de suas respectivas empresas.

Copyright © 2026 KnowBe4 Todos os direitos reservados.