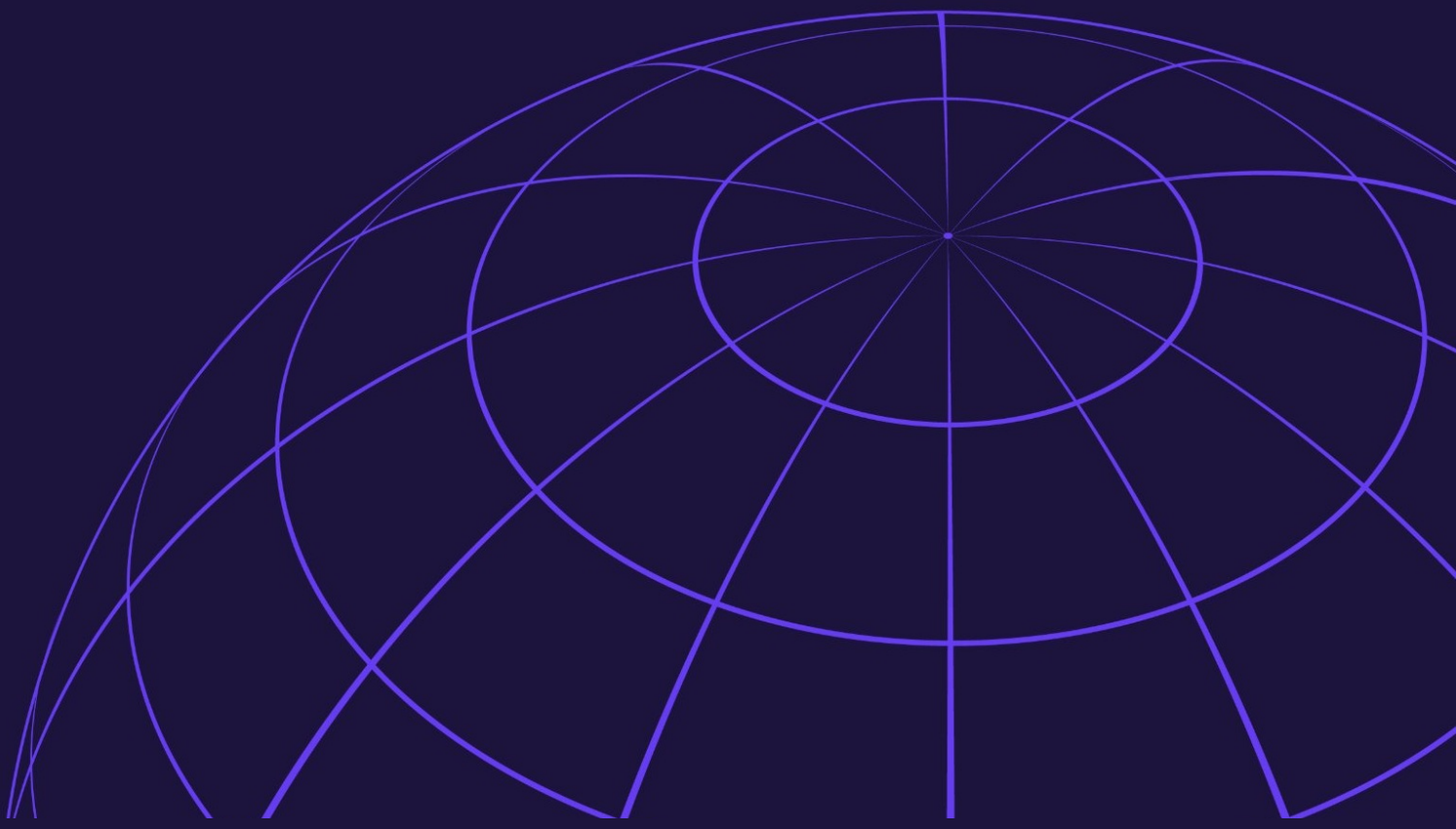
SecurityScorecard

RELATÓRIO | NOVEMBRO DE 2026

Cybersecurity no setor financeiro

LATAM e Iberia: ranking por país, vulnerabilidades e tendências

11	1195	81,1	12
PAÍSES	INSTITUIÇÕES	SCORE MÉDIO	MESES DE HISTÓRICO



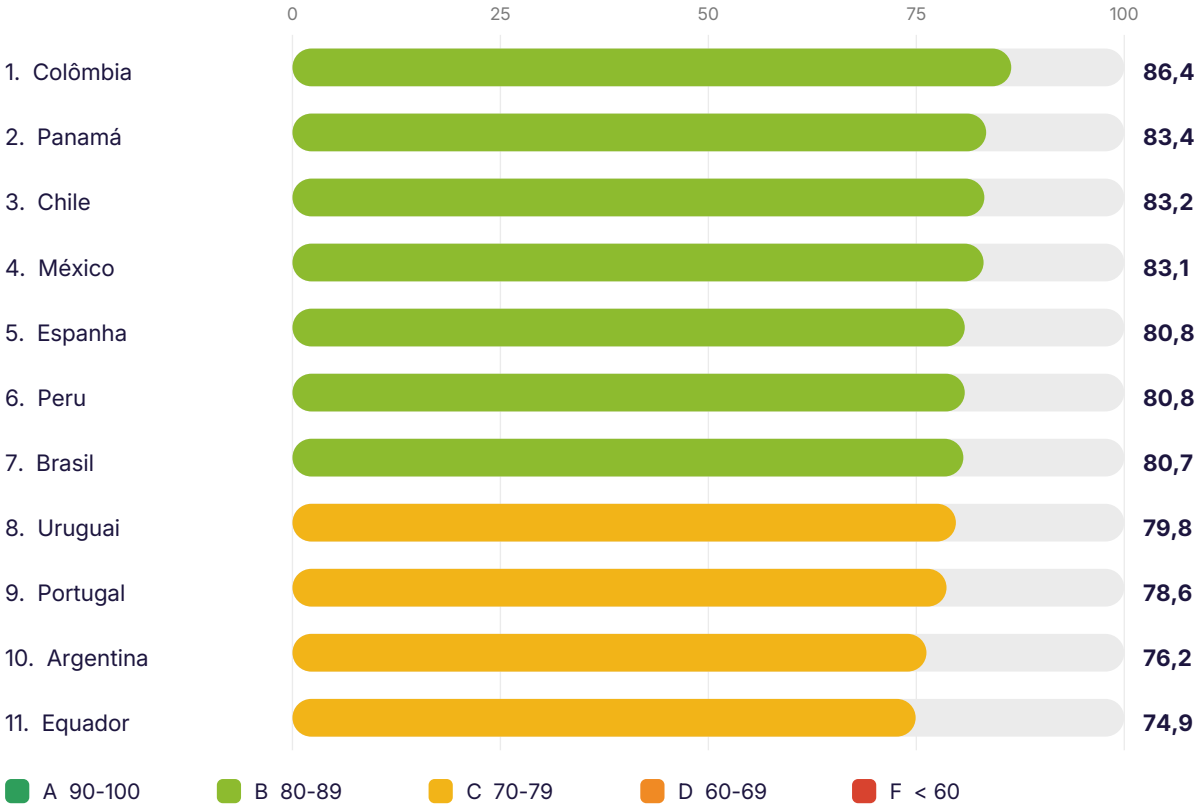
Dados de 8 de novembro de 2026 | Fontes: SecurityScorecard e Driftnet

Cybersecurity no setor financeiro

LATAM e Iberia: ranking por país, vulnerabilidades e tendências. Dados de 8 de novembro de 2026

INSTITUIÇÕES ANALISADAS	SCORE MÉDIO GERAL	MELHOR PAÍS	PIOR PAÍS
1195	81,1	Colômbia	Equador
11 países	grade B	média 86,4	média 74,9

Ranking por país (score médio)

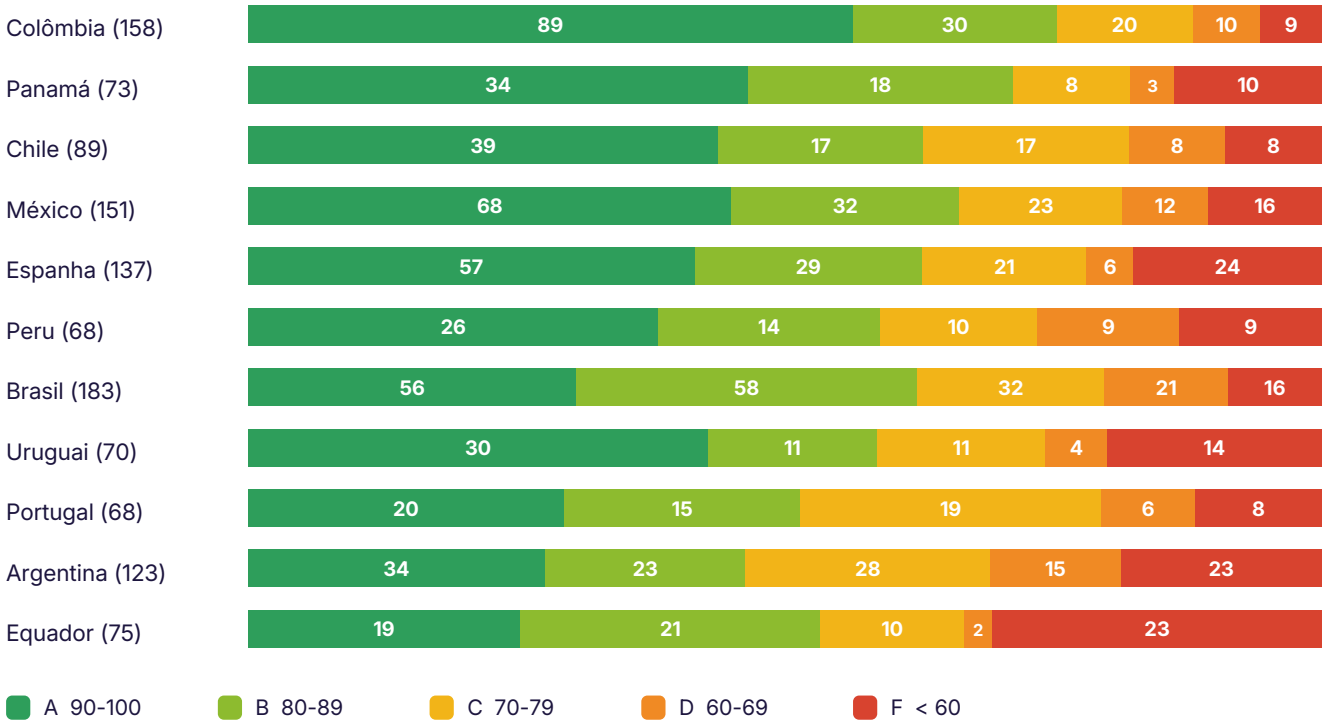


Leitura do ranking

- A **Colômbia** lidera com média de 86,4 e o **Equador** fecha o ranking com 74,9, uma diferença de 11,5 pontos.
- No conjunto, 62% das instituições têm grade A ou B e 21% ficam abaixo de 70, nas grades D e F. Essa cauda é o que mais separa os países: a proporção abaixo de 70 vai de 12% (Colômbia) a 33% (Equador).
- A postura média da região piorou nos últimos 12 meses: de 82,2 para 81,1 pontos (-1,0). 10 dos 11 países recuaram, e o mínimo foi atingido entre maio e agosto de 2026.
- 26% das instituições expõem pelo menos uma vulnerabilidade do catálogo de exploração ativa da CISA (KEV), e 10% têm uma CVE KEV associada a campanhas de ransomware.

Distribuição de grades por país

Número de instituições em cada faixa de grade, por ordem de score médio



Valores por país

País	Instit.	Média	Mediana	Mín	Máx	% A ou B	% abaixo de 70
Colômbia	158	86,4	91,0	47	100	75%	12%
Panamá	73	83,4	88,0	41	100	71%	18%
Chile	89	83,2	87,0	44	100	63%	18%
México	151	83,1	86,0	41	100	66%	19%
Espanha	137	80,8	86,0	33	100	63%	22%
Peru	68	80,8	83,5	49	100	59%	26%
Brasil	183	80,7	84,0	41	100	62%	20%
Uruguai	70	79,8	84,5	33	100	59%	26%
Portugal	68	78,6	80,0	42	100	51%	21%
Argentina	123	76,2	77,0	32	100	46%	31%
Equador	75	74,9	81,0	39	100	53%	33%

A grade é o score expresso em uma letra: A para 90 ou mais, F para abaixo de 60. A média esconde a dispersão: países com média parecida podem ter caudas muito diferentes, por isso a proporção abaixo de 70 é o melhor indicador de risco concentrado.

Porque a cauda importa

Em um ecossistema financeiro interconectado, os atacantes costumam entrar pela instituição mais fraca. No Equador, 33% das instituições têm score abaixo de 70, e na Argentina o índice é de 31%. Esses pontos fracos aumentam a probabilidade de incidentes que se propagam pelo sistema por meio de parceiros, processadores e fornecedores comuns. Já a Colômbia mostra o padrão oposto, com a maturidade distribuída de forma mais homogênea.

Fatores de risco

Score médio por fator da SecurityScorecard, onde cada fator pesa no score global



Score médio por fator e país

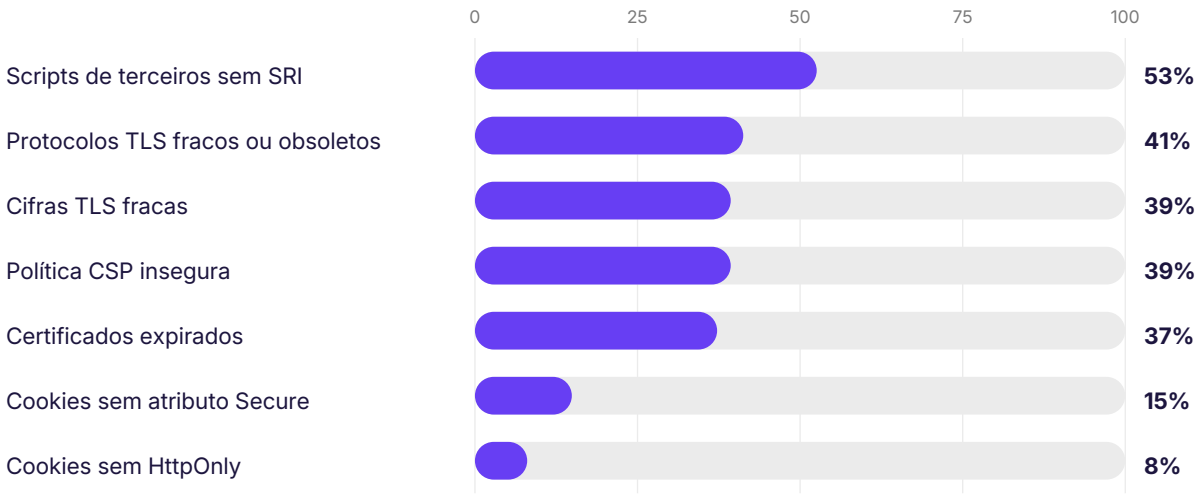
País	Rede	Aplicações	Patching	Info. exposta	DNS	Endpoints
Colômbia	90,9	88,1	92,7	96,9	98,5	98,9
Panamá	86,6	90,7	91,8	99,5	97,4	99,6
Chile	85,9	87,7	91,3	94,7	97,3	99,5
México	85,9	89,1	89,6	97,3	98,0	99,5
Espanha	86,2	83,8	89,8	96,4	96,9	99,9
Peru	86,5	87,4	89,3	97,7	97,7	99,7
Brasil	81,9	85,3	88,5	92,3	91,2	98,5
Uruguai	85,7	88,0	91,4	97,3	98,4	99,5
Portugal	84,5	81,2	87,6	98,8	96,0	99,8
Argentina	78,0	85,4	85,1	94,7	95,3	97,4
Equador	82,2	81,8	87,2	97,2	97,2	98,3

Leitura

- Os três fatores mais frágeis na região são **segurança de rede** (84,9), **segurança aplicacional** (86,3) e **cadência de patching** (89,5). Concentram-se na superfície exposta à internet e na gestão de atualizações, não em sinais de comprometimento.
- Os fatores de endpoint, reputação de IP, hacker chatter e engenharia social têm médias regionais acima de 98. O problema dominante é higiene da superfície de ataque, não atividade criminosa visível.
- A segurança de rede é o fator mais fraco em 7 dos 11 países, o que a torna o melhor ponto de partida para um programa regional de melhoria.

Vulnerabilidades mais comuns

Porcentagem de instituições com pelo menos uma ocorrência de cada problema



Prevalência por país (% de instituições afetadas)

País	Sem SRI	TLS fraco	Cifras fracas	CSP insegura	Cert. expirado	Cookie s/ Secure
Colômbia	44%	24%	27%	44%	32%	7%
Panamá	40%	34%	32%	27%	33%	7%
Chile	43%	43%	37%	34%	22%	13%
México	44%	44%	34%	27%	31%	9%
Espanha	63%	34%	41%	35%	34%	18%
Peru	44%	32%	32%	34%	29%	13%
Brasil	70%	61%	49%	54%	58%	19%
Uruguai	34%	31%	29%	26%	23%	11%
Portugal	75%	40%	44%	59%	37%	19%
Argentina	49%	56%	49%	43%	47%	21%
Equador	61%	36%	55%	40%	43%	28%

O que são e porque importam

- **Scripts de terceiros sem SRI (53%):** páginas que carregam JavaScript externo sem verificação de integridade. Se o fornecedor for comprometido, o código malicioso roda no site da instituição, o vetor típico de ataques à cadeia de suprimentos e de skimming web.
- **TLS fraco e cifras fracas (41% e 39%):** servidores que ainda aceitam versões antigas do protocolo, expondo as conexões a downgrade e interceptação.
- **Cookies sem Secure (15%) ou HttpOnly (8%):** facilitam o roubo de sessão em canais de homebanking.
- **Certificados expirados (37%) e CSP insegura (39%):** de severidade baixa, mas muito difundidos e indicativos de falhas de inventário e de processo.

Vulnerabilidades mais críticas

Lente SecurityScorecard (1195 instituições): exposição a falhas já exploradas ativamente, não apenas a falhas com pontuação CVSS alta

COM CVE ALTA OU CRÍTICA
41%
das instituições

COM CVE DO CATÁLOGO KEV
26%
exploração ativa (CISA)

KEV ASSOCIADA A RANSOMWARE
10%
campanhas conhecidas

EPSS ACIMA DE 90%
31%
alta probabilidade

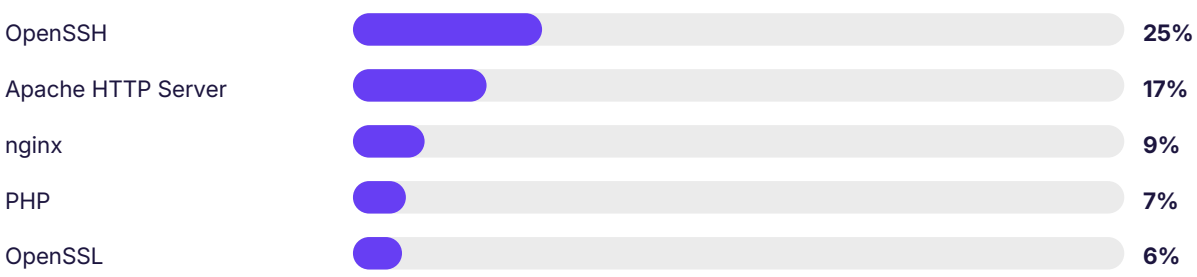
Exposição por país (% de instituições)

País	CVE alta/crítica	CVE em KEV	KEV + ransomware	EPSS acima de 90%
Colômbia	38%	20%	6%	27%
Panamá	33%	22%	8%	25%
Chile	37%	21%	6%	24%
México	38%	23%	7%	28%
Espanha	36%	26%	8%	29%
Peru	43%	21%	6%	29%
Brasil	54%	39%	16%	42%
Uruguai	30%	19%	7%	21%
Portugal	43%	29%	15%	34%
Argentina	53%	36%	20%	41%
Equador	37%	21%	15%	27%

Vulnerabilidades de maior relevância na região

CVE	Produto / tipo	% instit.	KEV	EPSS	Ransomware
CVE-2023-44487	HTTP/2 Rapid Reset (negação de serviço)	16%	Sim	100,0%	Não
CVE-2024-38475	Apache HTTP Server, escape incorreto	11%	Sim	100,0%	Não
CVE-2021-40438	Apache mod_proxy, SSRF	9%	Sim	100,0%	Sim
CVE-2024-6387	OpenSSH, regreSSHion (execução remota)	15%	Não	99,5%	Não
CVE-2025-53770	Microsoft SharePoint (ToolShell)	<1%	Sim	100,0%	Sim
CVE-2021-44228	Apache Log4j (Log4Shell)	<1%	Sim	100,0%	Sim

Famílias de software mais expostas (CVE alta ou crítica)

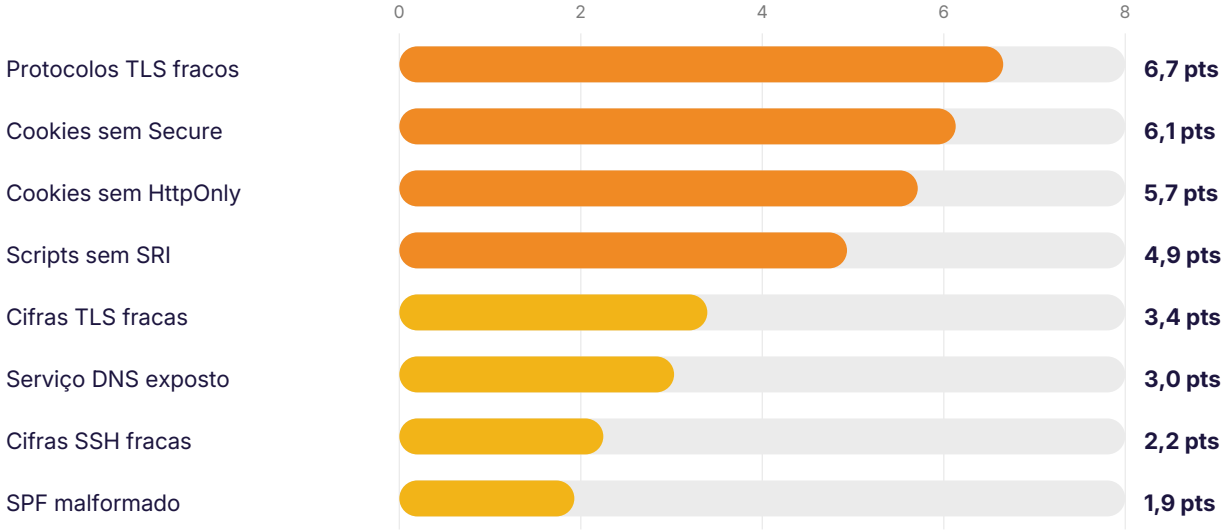


A SecurityScorecard infere versões de software por sinais externos (banners). Parte dos achados pode estar corrigida por backport e deve ser validada internamente.

Vulnerabilidades de maior impacto

Impacto no score e custo potencial de um incidente

Pontos de score perdidos por instituição afetada (média)



Impacto econômico (setor financeiro)

CUSTO MÉDIO DE UMA VIOLAÇÃO

USD 6,29 M

IBM 2026, vs 5,56 M no ano anterior

TEMPO PARA IDENTIFICAR

165 dias

setor financeiro, IBM 2026

ATAQUES COM IA

+1 M USD

custo adicional médio por violação

Leitura

- As falhas que mais pontos custam são de configuração simples: TLS fraco (6,7 pontos por instituição afetada), cookies sem Secure ou HttpOnly e scripts sem SRI. Corrigi-las é barato e tem retorno imediato no score.
- Os problemas de menor severidade individual (CSP, certificados expirados) só pesam pela escala: aparecem em metade ou mais das instituições.
- Do lado do risco real, o impacto máximo vem das vulnerabilidades KEV associadas a ransomware e dos incidentes na cadeia de fornecedores: o relatório Verizon DBIR 2026 indica que o envolvimento de terceiros em violações subiu para 48%, contra 30% no ano anterior.
- O custo de uma violação no setor financeiro é o segundo mais alto entre 17 setores, segundo a IBM, e cresce mais rápido do que a média global.

Exposição da infraestrutura própria

Lente Driftnet: serviços expostos e vulnerabilidades observadas nos IPs registrados em nome das instituições

COM INFRA PRÓPRIA
217 de 1195
18% das instituições

SERVIÇO SENSÍVEL EXPOSTO
19%
FTP, admin remota, SMB ou BD

ADMIN. REMOTA EXPOSTA
12%
Telnet, RDP, VNC, WinRM

CVE DO CATÁLOGO KEV
21%
nos IPs próprios (Driftnet)

Por país (instituições com infraestrutura própria identificada)

País	Com infra / total	Serviço sensível	FTP	Admin. remota	KEV (Driftnet)	KEV (SSC)
Colômbia	37 / 158	24%	14%	19%	16%	19%
Panamá	7 / 73	0%	0%	0%	0%	43%
Chile	12 / 89	0%	0%	0%	8%	33%
México	12 / 151	8%	0%	0%	25%	42%
Espanha	32 / 137	22%	12%	3%	12%	31%
Peru	11 / 68	0%	0%	0%	18%	18%
Brasil	39 / 183	31%	18%	23%	33%	59%
Uruguai	5 / 70	20%	20%	20%	20%	20%
Portugal	17 / 68	0%	0%	0%	24%	35%
Argentina	24 / 123	29%	21%	12%	33%	33%
Equador	21 / 75	24%	5%	24%	14%	24%

Todas as porcentagens desta página têm como base as instituições com infraestrutura própria identificada em cada país. A última coluna é a lente SecurityScorecard aplicada às mesmas instituições. Amostras pequenas: uma instituição pesa entre 5 e 20 pontos percentuais.

Leitura

- **18% das instituições têm infraestrutura própria identificável.** Os demais publicam seus serviços por meio de cloud, CDN, WAF ou operadoras, o que desloca parte do risco para terceiros.
- **Nos IPs próprios, 19% das instituições expõem pelo menos um serviço sensível:** FTP em 11%, administração remota em 12%, SMB em 2% e bases de dados em 5%.
- **21% das organizações têm pelo menos uma CVE do catálogo KEV da CISA nos seus endereços IP próprios** e 10% têm uma vinculada a ransomware. As mais frequentes são falhas do Apache HTTP Server, do jQuery e o HTTP/2 Rapid Reset.
- **Comparação entre países com cautela.** As amostras de Panamá e Uruguai são pequenas, de 5 a 9 instituições cada. Nos países em que mais bancos operam a própria infraestrutura, a exposição pode parecer maior simplesmente porque mais parte do perímetro é visível.

Duas lentes sobre a mesma exposição

SecurityScorecard e Driftnet medem âmbitos diferentes e complementam-se

SecurityScorecard: avalia o domínio de cada instituição e os ativos atribuídos a ele, incluindo serviços hospedados por fornecedores (1195 instituições).

Driftnet: observa os endereços IP registrados em nome de cada instituição (217 instituições com infraestrutura própria identificada). Cada fonte enxerga ativos que a outra não enxerga, portanto compare as cifras apenas quando ambas usam o mesmo conjunto de instituições.

Mesmas 217 instituições, as duas lentes

Indicador	SecurityScorecard	Driftnet	Pelo menos uma	Ambas
CVE do catálogo KEV	34%	21%	42%	13%
FTP exposto	8%	11%	14%	5%
Telnet exposto	9%	11%	15%	4%

Porcentagem das 217 instituições com infraestrutura própria identificada.

Leitura

- **Cobertura combinada:** juntas, as duas lentes assinalam 42% das instituições com CVE KEV, contra 34% pela SecurityScorecard e 21% pela Driftnet, isoladamente. Em FTP, as prevalências são semelhantes (8% e 11%), e juntas chegam a 14%.
- **A SecurityScorecard assinala mais casos de KEV.** Uma explicação provável é que atribui ao domínio ativos que estão fora do espaço de IPs da instituição, por exemplo serviços hospedados por fornecedores. A Driftnet acrescenta casos que só se veem a partir do IP próprio.
- **TLS:** é avaliado apenas pela SecurityScorecard, que avalia o suporte a versões antigas do protocolo em cada servidor. A Driftnet registra a versão negociada na conexão, que não revela o suporte a versões antigas, e por isso não é usada para esta métrica.
- **Como usar em conjunto:** a SecurityScorecard dá o score e a prevalência por país, a Driftnet dá a visão de IP e serviço da infraestrutura própria. Uma vulnerabilidade assinalada pelas duas é um achado mais robusto e deve ser tratada primeiro.

O que a Driftnet acrescenta ao relatório

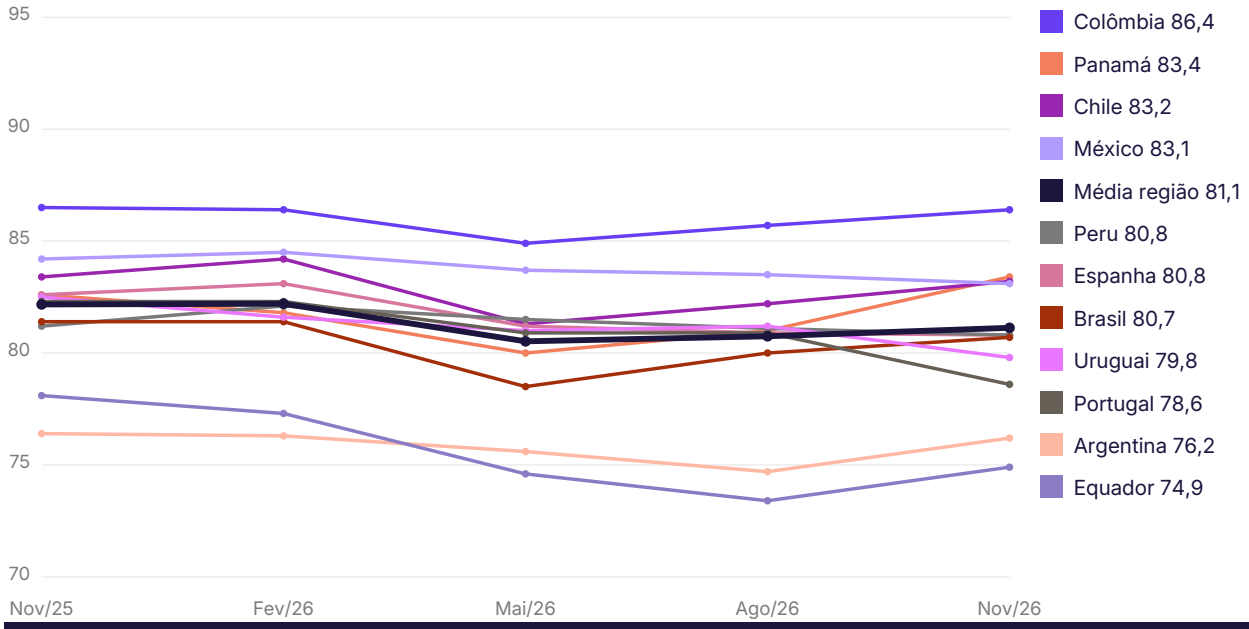
- **Dimensão e forma da exposição:** serviços sensíveis expostos na infraestrutura própria, que o score por si só não detalha.
- **Risco de terceiros:** a maioria das instituições publica serviços através de fornecedores, o que reforça a prioridade de monitorar a cadeia.
- **Limites:** a atribuição é por nome da entidade no registro de IPs, por isso instituições hospedadas em fornecedores ficam fora desta lente. Os números por país são indicativos.

Próximos passos recomendados: ampliar a atribuição por ASN e por certificados (CT logs), medir a evolução da exposição com coletas periódicas e incluir fornecedores críticos de cada país.

Tendências

Evolução do score nos últimos 12 meses e fatores que moldam o risco em 2026

Score médio por país (mesma amostra de instituições ao longo do tempo)



País	Nov/25	Fev/26	Mai/26	Ago/26	Nov/26	Variação 12m
Colômbia	86,5	86,4	84,9	85,7	86,4	-0,1
Panamá	82,6	81,8	80,0	81,0	83,4	+0,8
Chile	83,4	84,2	81,3	82,2	83,2	-0,2
México	84,2	84,5	83,7	83,5	83,1	-1,1
Espanha	82,6	83,1	81,2	80,9	80,8	-1,8
Peru	81,2	82,1	81,5	81,1	80,8	-0,4
Brasil	81,4	81,4	78,5	80,0	80,7	-0,7
Uruguai	82,5	81,6	81,0	81,2	79,8	-2,7
Portugal	82,3	82,3	80,9	80,9	78,6	-3,7
Argentina	76,4	76,3	75,6	74,7	76,2	-0,2
Equador	78,1	77,3	74,6	73,4	74,9	-3,2
Região	**82,2**	**82,2**	**80,5**	**80,7**	**81,1**	**-1,0**

Leitura dos dados

- **Queda generalizada:** 10 dos 11 países perderam pontos em 12 meses, entre 0,8 (Panamá) e 3,7 (Portugal).
- **Fundo e recuperação parcial:** o ponto mais baixo da região foi entre maio e agosto de 2026, com leve recuperação desde agosto em 6 dos 11 países.
- **Divergência:** Panamá e Colômbia recuaram menos (0,8 e 0,1 pontos), e Portugal foi o mais atingido (3,7 pontos).

Tendências do setor para 2026

O que os dados externos indicam sobre a evolução das ameaças

- **IA ofensiva e automação.** A IA está passando de ferramenta de defesa a motor de ataque: phishing e deepfakes mais convincentes, fraude automatizada e intrusões mais rápidas. A IBM estima que os ataques assistidos por IA acrescentam em média 1 milhão de dólares ao custo de cada violação, e o setor financeiro é um dos mais visados.
- **Ransomware mais fragmentado e rápido.** Analistas regionais esperam mais grupos Ransomware-as-a-Service, extorsão mais sofisticada e ataques mais difíceis de atribuir. A exposição a vulnerabilidades KEV associadas a ransomware, medida neste relatório, é o indicador mais direto desse risco.
- **Cadeia de fornecedores como vetor principal.** Bancos dependem de dezenas de terceiros (processadores, cloud, fintechs, KYC). O envolvimento de terceiros em violações subiu para 48%, contra 30% no ano anterior, segundo o Verizon DBIR 2026. Scripts externos sem SRI e fornecedores com score baixo são hoje uma das portas de entrada mais prováveis.
- **Pressão sobre o canal digital.** O crescimento do homebanking, dos pagamentos em tempo real e das fintechs amplia a superfície exposta. Malware bancário móvel com controle remoto, antes focado na Europa, está se expandindo para a Argentina e o Brasil.
- **Mais ataques na América Latina.** Relatórios do setor reportam aumentos fortes dos ataques semanais na região em relação ao ano anterior (entre 53% e 108%, conforme a fonte e a métrica) e apontam a América Latina como uma das regiões mais visadas em 2026.
- **Regulação em consolidação, mas desigual.** Há reforço de exigências sobre cibersegurança e IA, com maturidade regulatória desigual entre países, o que cria oportunidades de arbitragem para atacantes em ecossistemas interconectados. A Europa (DORA e NIS2) estabelece o padrão para risco de terceiros e resiliência operacional.
- **Do questionário anual ao monitoramento contínuo.** A tendência de gestão de risco é substituir avaliações pontuais por monitoramento externo contínuo, priorização por exploração real (KEV e EPSS) e métricas quantitativas comparáveis entre instituições.

Prioridades recomendadas

- Corrigir primeiro o que está no KEV e tem EPSS alto, antes de ordenar por CVSS.
- Desativar TLS antigo e cifras fracas, e corrigir atributos de cookies. É o maior ganho de score por esforço.
- Aplicar SRI e CSP em todos os scripts de terceiros.
- Monitorar fornecedores críticos de forma contínua e exigir níveis mínimos de score em contrato.
- Seguir o score por país e por instituição ao longo do tempo, não só a média.

1. Colômbia

1.º lugar entre 11 países | 158 instituições analisadas

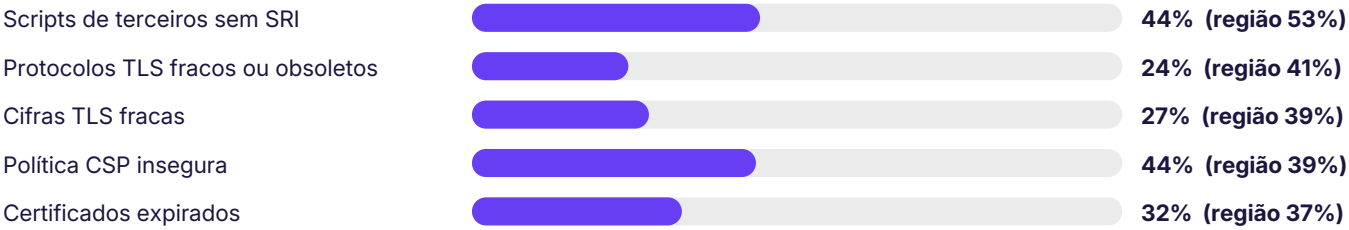
SCORE MÉDIO	MEDIANA	ABAIXO DE 70	VARIAÇÃO 12M
86,4	91,0	12%	-0,1
grade B	mín 47 | máx 100	região 21%	pontos de score



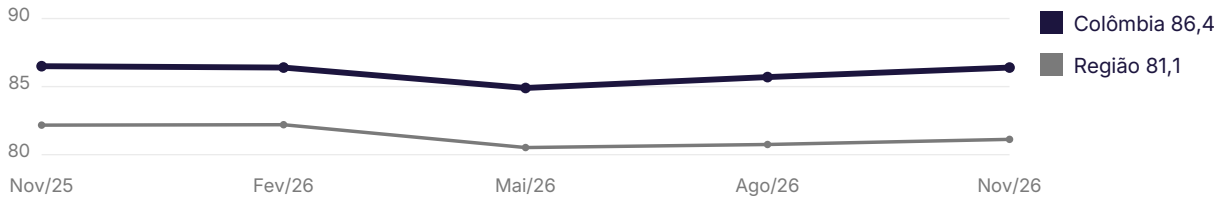
Score por fator (país vs região)



Problemas mais comuns (% de instituições afetadas)



Evolução do score médio



Análise

A Colômbia ocupa o 1.º lugar entre 11 países, com score médio de 86,4, 5,3 pontos acima da média regional de 81,1. Das instituições do país, 75% têm grade A ou B e 12% ficam abaixo de 70.

Em relação à região, o fator mais forte é **segurança de rede** (+5,9) e o mais fraco é **segurança de endpoints** (-0,1). O problema mais acima da média regional é **política CSP insegura** (44% das instituições, contra 39% na região).

Nos últimos 12 meses, o score médio caiu 0,1 pontos, de 86,5 para 86,4. Na exposição crítica, 20% das instituições têm CVE do catálogo KEV (média regional: 26%) e 6% têm uma CVE KEV associada a ransomware (média regional: 10%).

2. Panamá

2.º lugar entre 11 países | 73 instituições analisadas

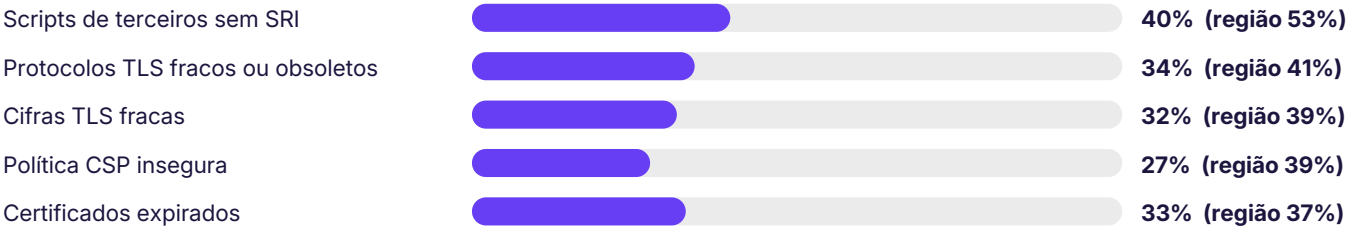
SCORE MÉDIO	MEDIANA	ABAIXO DE 70	VARIAÇÃO 12M
83,4	88,0	18%	+0,8
grade B	mín 41 | máx 100	região 21%	pontos de score



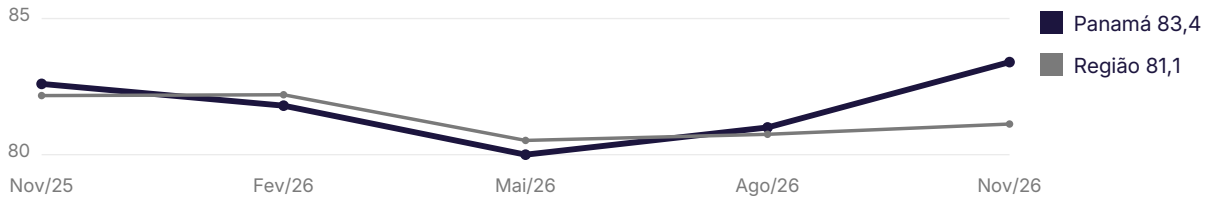
Score por fator (país vs região)



Problemas mais comuns (% de instituições afetadas)



Evolução do score médio



Análise

O Panamá ocupa o 2.º lugar entre 11 países, com score médio de 83,4, 2,3 pontos acima da média regional de 81,1. Das instituições do país, 71% têm grade A ou B e 18% ficam abaixo de 70.

Em relação à região, o fator mais forte é **segurança aplicacional** (+4,4) e o de menor vantagem é **segurança de endpoints** (+0,5). O problema mais próximo da média regional é **certificados expirados** (33% das instituições, contra 37% na região).

Nos últimos 12 meses, o score médio subiu 0,8 pontos, de 82,6 para 83,4. Na exposição crítica, 22% das instituições têm CVE do catálogo KEV (média regional: 26%) e 8% têm uma CVE KEV associada a ransomware (média regional: 10%).

3. Chile

3.º lugar entre 11 países | 89 instituições analisadas

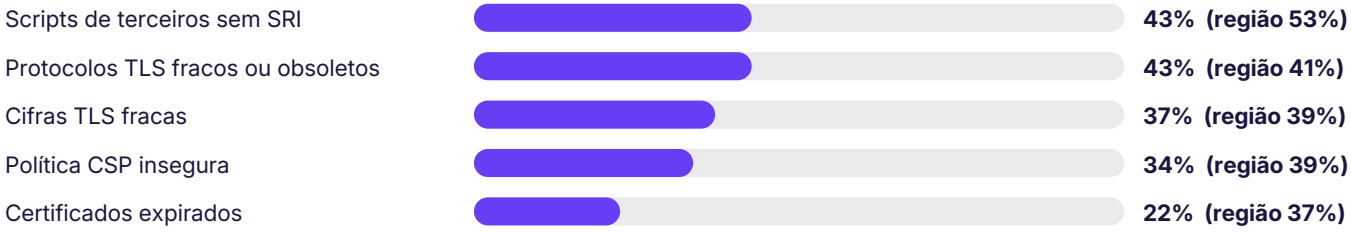
SCORE MÉDIO	MEDIANA	ABAIXO DE 70	VARIAÇÃO 12M
83,2	87,0	18%	-0,2
grade B	mín 44 | máx 100	região 21%	pontos de score



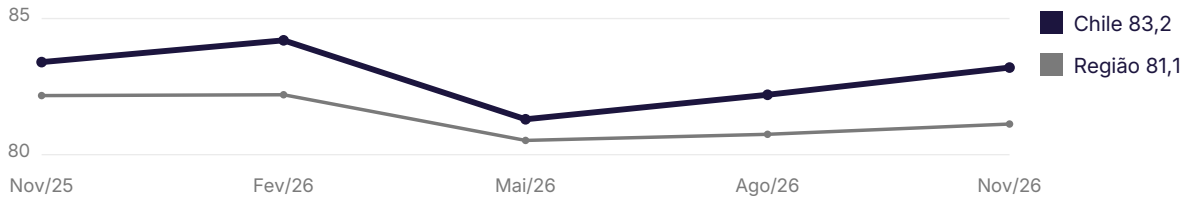
Score por fator (país vs região)



Problemas mais comuns (% de instituições afetadas)



Evolução do score médio



Análise

O Chile ocupa o 3.º lugar entre 11 países, com score médio de 83,2, 2,1 pontos acima da média regional de 81,1. Das instituições do país, 63% têm grade A ou B e 18% ficam abaixo de 70.

Em relação à região, o fator mais forte é **cadência de patching** (+1,8) e o mais fraco é **informação exposta** (-1,4). O problema mais acima da média regional é **cookies sem HttpOnly** (12% das instituições, contra 8% na região).

Nos últimos 12 meses, o score médio caiu 0,2 pontos, de 83,4 para 83,2. Na exposição crítica, 21% das instituições têm CVE do catálogo KEV (média regional: 26%) e 6% têm uma CVE KEV associada a ransomware (média regional: 10%).

4. México

4.º lugar entre 11 países | 151 instituições analisadas

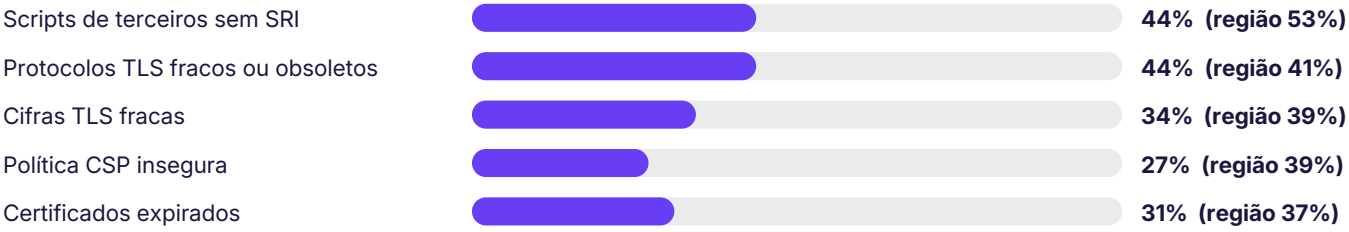
SCORE MÉDIO	MEDIANA	ABAIXO DE 70	VARIAÇÃO 12M
83,1	86,0	19%	-1,1
grade B	mín 41 | máx 100	região 21%	pontos de score



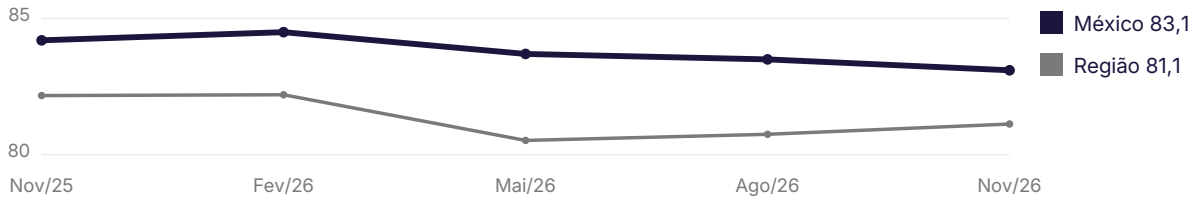
Score por fator (país vs região)



Problemas mais comuns (% de instituições afetadas)



Evolução do score médio



Análise

O México ocupa o 4.º lugar entre 11 países, com score médio de 83,1, 2,0 pontos acima da média regional de 81,1. Das instituições do país, 66% têm grade A ou B e 19% ficam abaixo de 70.

Em relação à região, o fator mais forte é **segurança aplicacional** (+2,8) e o de menor vantagem é **cadência de patching** (+0,1). O problema mais acima da média regional é **protocolos TLS fracos ou obsoletos** (44% das instituições, contra 41% na região).

Nos últimos 12 meses, o score médio caiu 1,1 pontos, de 84,2 para 83,1. Na exposição crítica, 23% das instituições têm CVE do catálogo KEV (média regional: 26%) e 7% têm uma CVE KEV associada a ransomware (média regional: 10%).

5. Espanha

5.º lugar entre 11 países | 137 instituições analisadas

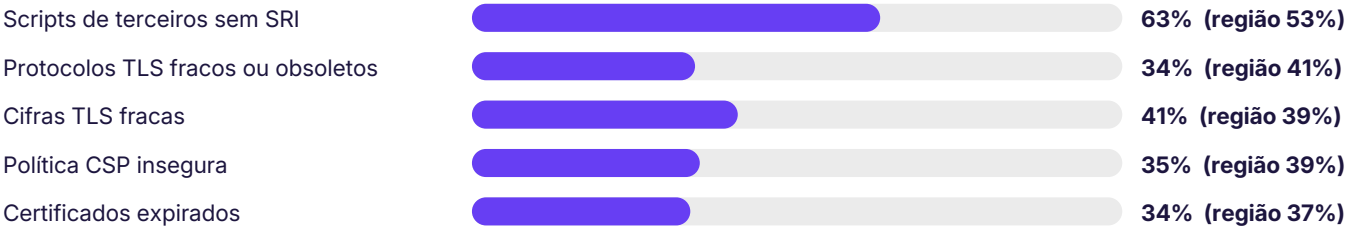
SCORE MÉDIO	MEDIANA	ABAIXO DE 70	VARIAÇÃO 12M
80,8	86,0	22%	-1,8
grade B	mín 33 | máx 100	região 21%	pontos de score



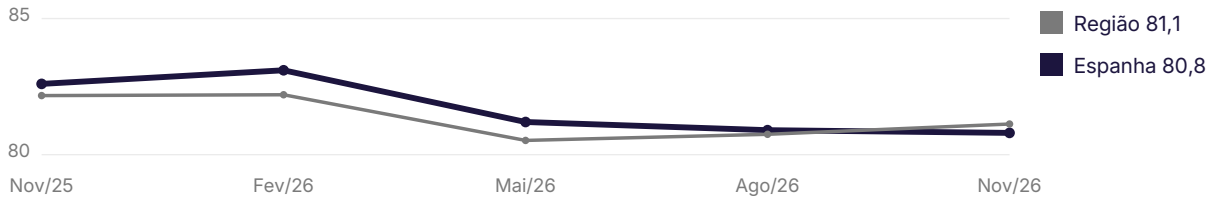
Score por fator (país vs região)



Problemas mais comuns (% de instituições afetadas)



Evolução do score médio



Análise

A Espanha ocupa o 5.º lugar entre 11 países, com score médio de 80,8, 0,3 pontos abaixo da média regional de 81,1. Das instituições do país, 63% têm grade A ou B e 22% ficam abaixo de 70.

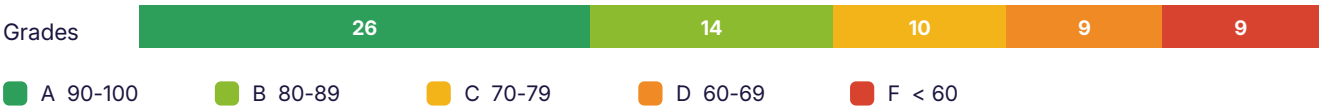
Em relação à região, o fator mais forte é **segurança de rede** (+1,3) e o mais fraco é **segurança aplicacional** (-2,5). O problema mais acima da média regional é **scripts de terceiros sem SRI** (63% das instituições, contra 53% na região).

Nos últimos 12 meses, o score médio caiu 1,8 pontos, de 82,6 para 80,8. Na exposição crítica, 26% das instituições têm CVE do catálogo KEV (média regional: 26%) e 8% têm uma CVE KEV associada a ransomware (média regional: 10%).

6. Peru

6.º lugar entre 11 países | 68 instituições analisadas

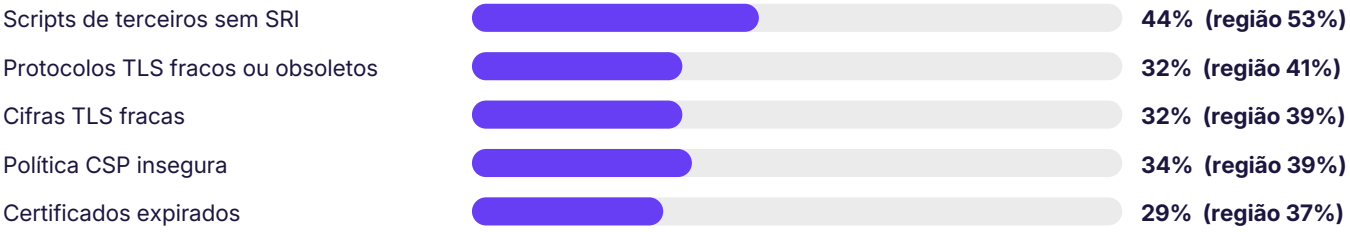
SCORE MÉDIO	MEDIANA	ABAIXO DE 70	VARIAÇÃO 12M
80,8	83,5	26%	-0,4
grade B	mín 49 | máx 100	região 21%	pontos de score



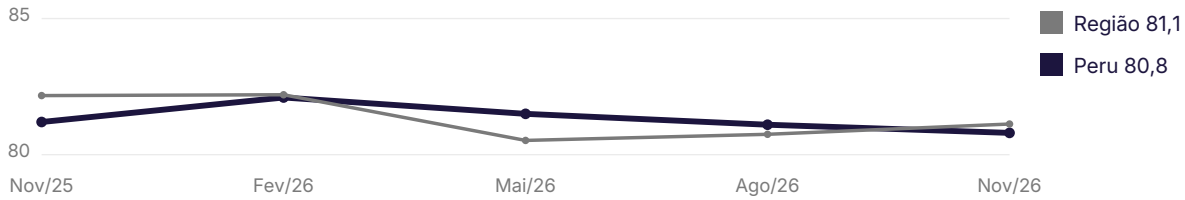
Score por fator (país vs região)



Problemas mais comuns (% de instituições afetadas)



Evolução do score médio



Análise

O Peru ocupa o 6.º lugar entre 11 países, com score médio de 80,8, 0,3 pontos abaixo da média regional de 81,1. Das instituições do país, 59% têm grade A ou B e 26% ficam abaixo de 70.

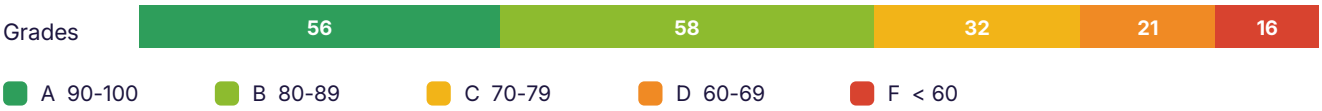
Em relação à região, o fator mais forte é **segurança de rede** (+1,5) e o mais fraco é **cadência de patching** (-0,2). O problema mais acima da média regional é **cookies sem HttpOnly** (9% das instituições, contra 8% na região).

Nos últimos 12 meses, o score médio caiu 0,4 pontos, de 81,2 para 80,8. Na exposição crítica, 21% das instituições têm CVE do catálogo KEV (média regional: 26%) e 6% têm uma CVE KEV associada a ransomware (média regional: 10%).

7. Brasil

7.º lugar entre 11 países | 183 instituições analisadas

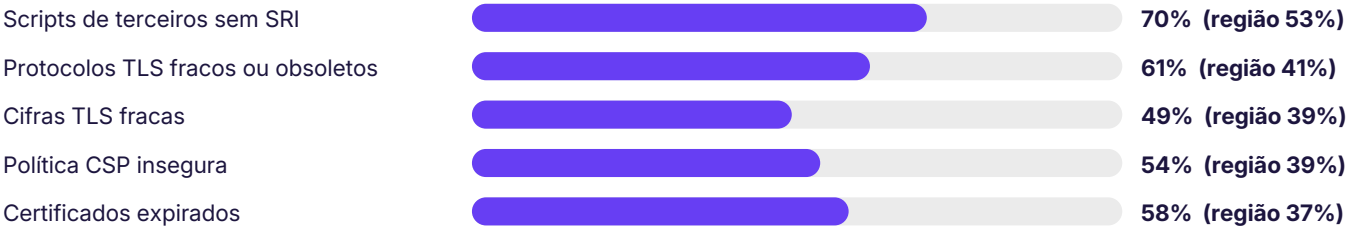
SCORE MÉDIO	MEDIANA	ABAIXO DE 70	VARIAÇÃO 12M
80,7	84,0	20%	-0,7
grade B	mín 41 | máx 100	região 21%	pontos de score



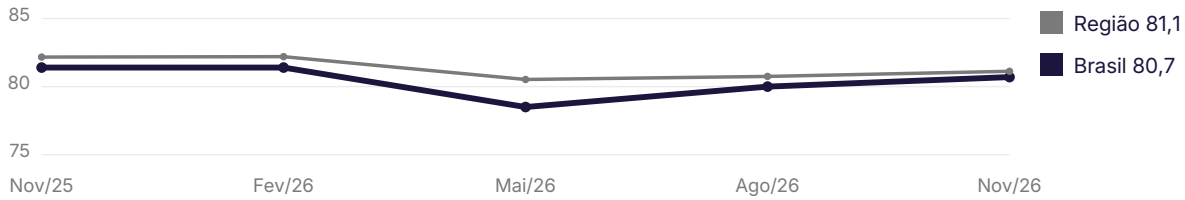
Score por fator (país vs região)



Problemas mais comuns (% de instituições afetadas)



Evolução do score médio



Análise

O Brasil ocupa o 7.º lugar entre 11 países, com score médio de 80,7, 0,5 pontos abaixo da média regional de 81,1. Das instituições do país, 62% têm grade A ou B e 20% ficam abaixo de 70.

Em relação à região, o fator mais forte é **segurança de endpoints** (-0,6) e o mais fraco é **saúde do DNS** (-5,1). O problema mais acima da média regional é **certificados expirados** (58% das instituições, contra 37% na região).

Nos últimos 12 meses, o score médio caiu 0,7 pontos, de 81,4 para 80,7. Na exposição crítica, 39% das instituições têm CVE do catálogo KEV (média regional: 26%) e 16% têm uma CVE KEV associada a ransomware (média regional: 10%).

8. Uruguai

8.º lugar entre 11 países | 70 instituições analisadas

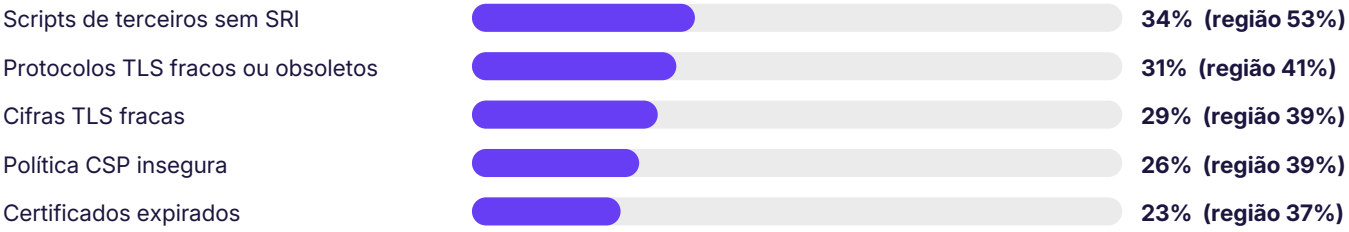
SCORE MÉDIO	MEDIANA	ABAIXO DE 70	VARIAÇÃO 12M
79,8	84,5	26%	-2,7
grade C	mín 33 | máx 100	região 21%	pontos de score



Score por fator (país vs região)



Problemas mais comuns (% de instituições afetadas)



Evolução do score médio



Análise

O Uruguai ocupa o 8.º lugar entre 11 países, com score médio de 79,8, 1,4 pontos abaixo da média regional de 81,1. Das instituições do país, 59% têm grade A ou B e 26% ficam abaixo de 70.

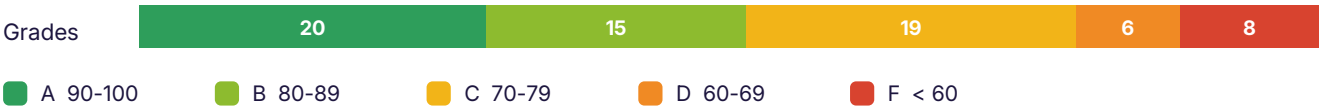
Em relação à região, o fator mais forte é **saúde do DNS** (+2,1) e o de menor vantagem é **segurança de endpoints** (+0,5). O problema mais próximo da média regional é **cookies sem HttpOnly** (7% das instituições, contra 8% na região).

Nos últimos 12 meses, o score médio caiu 2,7 pontos, de 82,5 para 79,8. Na exposição crítica, 19% das instituições têm CVE do catálogo KEV (média regional: 26%) e 7% têm uma CVE KEV associada a ransomware (média regional: 10%).

9. Portugal

9.º lugar entre 11 países | 68 instituições analisadas

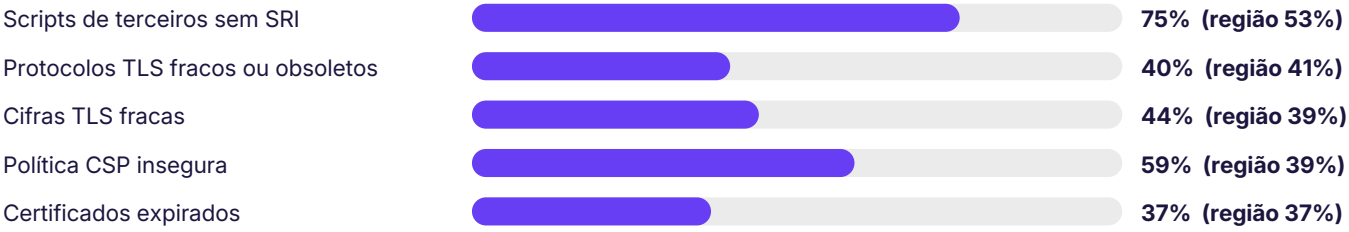
SCORE MÉDIO	MEDIANA	ABAIXO DE 70	VARIAÇÃO 12M
78,6	80,0	21%	-3,7
grade C	mín 42 | máx 100	região 21%	pontos de score



Score por fator (país vs região)



Problemas mais comuns (% de instituições afetadas)



Evolução do score médio



Análise

Portugal ocupa o 9.º lugar entre 11 países, com score médio de 78,6, 2,5 pontos abaixo da média regional de 81,1. Das instituições do país, 51% têm grade A ou B e 21% ficam abaixo de 70.

Em relação à região, o fator mais forte é **informação exposta** (+2,7) e o mais fraco é **segurança aplicacional** (-5,1). O problema mais acima da média regional é **scripts de terceiros sem SRI** (75% das instituições, contra 53% na região).

Nos últimos 12 meses, o score médio caiu 3,7 pontos, de 82,3 para 78,6. Na exposição crítica, 29% das instituições têm CVE do catálogo KEV (média regional: 26%) e 15% têm uma CVE KEV associada a ransomware (média regional: 10%).

10. Argentina

10.º lugar entre 11 países | 123 instituições analisadas

SCORE MÉDIO	MEDIANA	ABAIXO DE 70	VARIAÇÃO 12M
76,2	77,0	31%	-0,2
grade C	mín 32 | máx 100	região 21%	pontos de score



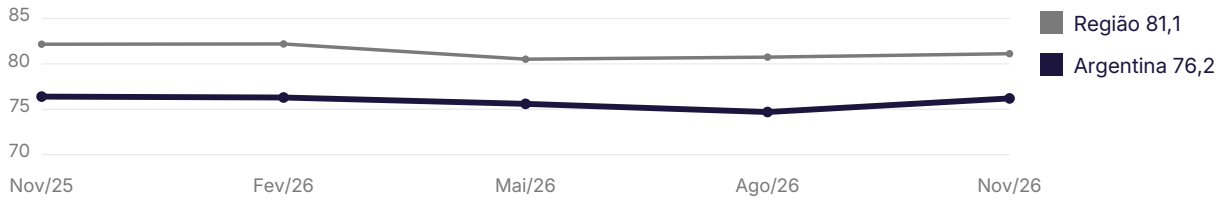
Score por fator (país vs região)



Problemas mais comuns (% de instituições afetadas)



Evolução do score médio



Análise

A Argentina ocupa o 10.º lugar entre 11 países, com score médio de 76,2, 4,9 pontos abaixo da média regional de 81,1. Das instituições do país, 46% têm grade A ou B e 31% ficam abaixo de 70.

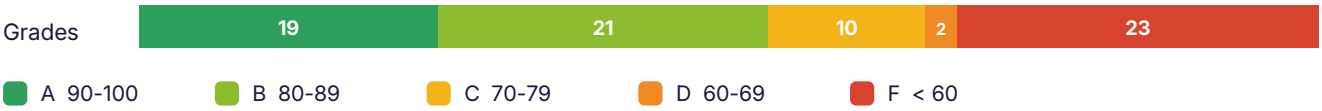
Em relação à região, o fator mais forte é **segurança aplicacional** (-0,9) e o mais fraco é **segurança de rede** (-7,0). O problema mais acima da média regional é **protocolos TLS fracos ou obsoletos** (56% das instituições, contra 41% na região).

Nos últimos 12 meses, o score médio caiu 0,2 pontos, de 76,4 para 76,2. Na exposição crítica, 36% das instituições têm CVE do catálogo KEV (média regional: 26%) e 20% têm uma CVE KEV associada a ransomware (média regional: 10%).

11. Equador

11.º lugar entre 11 países | 75 instituições analisadas

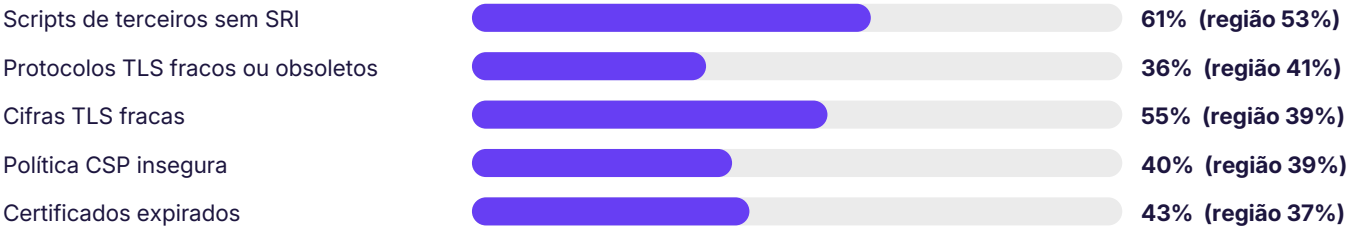
SCORE MÉDIO	MEDIANA	ABAIXO DE 70	VARIAÇÃO 12M
74,9	81,0	33%	-3,2
grade C	mín 39 | máx 100	região 21%	pontos de score



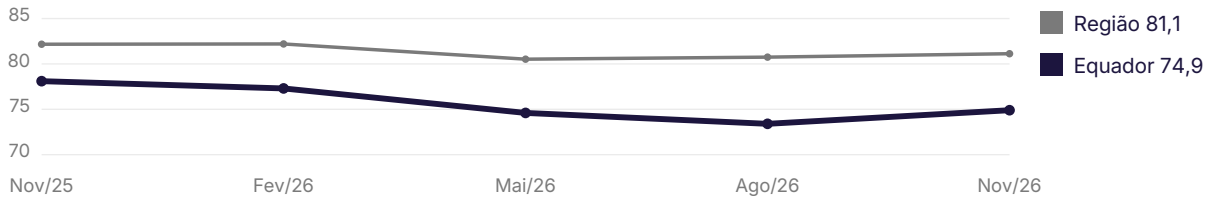
Score por fator (país vs região)



Problemas mais comuns (% de instituições afetadas)



Evolução do score médio



Análise

O Equador ocupa o 11.º lugar entre 11 países, com score médio de 74,9, 6,2 pontos abaixo da média regional de 81,1. Das instituições do país, 53% têm grade A ou B e 33% ficam abaixo de 70.

Em relação à região, o fator mais forte é **informação exposta** (+1,1) e o mais fraco é **segurança aplicacional** (-4,5). O problema mais acima da média regional é **cifras TLS fracas** (55% das instituições, contra 39% na região).

Nos últimos 12 meses, o score médio caiu 3,2 pontos, de 78,1 para 74,9. Na exposição crítica, 21% das instituições têm CVE do catálogo KEV (média regional: 26%) e 15% têm uma CVE KEV associada a ransomware (média regional: 10%).

Metodologia e notas

Como os números foram calculados

- **Amostra:** 1195 instituições financeiras de 11 países, extraídas dos portfolios “Banks” da conta SecurityScorecard. As instituições incluem bancos, bancos públicos e de desenvolvimento, financeiras, cooperativas, fintechs e filiais de grupos globais. A amostra não cobre todo o sistema financeiro de cada país.
- **Score:** os scores da SecurityScorecard vão de 0 a 100 e correspondem às grades da seguinte forma: A (90 a 100), B (80 a 89), C (70 a 79), D (60 a 69) e F (abaixo de 60). A média por país é a média simples dos scores de suas instituições.
- **Prevalência de problemas:** porcentagem de instituições com pelo menos uma ocorrência do problema nos fatores avaliados pela plataforma, a partir dos dados de 08/11/2026.
- **Vulnerabilidades críticas:** CVE de severidade alta ou crítica detectadas pela plataforma, cruzadas com o catálogo KEV da CISA (atualizado em 06/11/2026) e com o EPSS (probabilidade de exploração nos 30 dias seguintes).
- **Tendências:** evolução do score médio das mesmas instituições nos últimos 12 meses (histórico diário da plataforma, de 08/11/2025 a 07/11/2026).
- **Exposição da infraestrutura própria:** dados da Driftnet (scans de internet) atribuídos às instituições pelo nome da entidade no registro de IPs, validado por regras de nomenclatura. Inclui serviços TCP sensíveis e CVE mapeadas (NVD), cruzadas com KEV. Os indicadores de TLS vêm da SecurityScorecard.
- **Limitações:** a SecurityScorecard mede a exposição visível de fora para dentro, não substitui uma auditoria interna. Versões de software são inferidas por sinais externos e podem incluir falsos positivos por backport. Este relatório apresenta apenas valores agregados por país.
- **Cores das tabelas:** faixas fixas, do verde (melhor) ao vermelho (pior). Nos scores, as faixas coincidem com as grades A a F. Nas porcentagens de exposição, verde até 10%, verde-claro até 25%, amarelo até 40%, laranja até 60% e o vermelho fica acima de 60%. Em porcentagens em que mais é melhor (% A ou B), os limites são 90%, 75%, 60% e 45%. Nos indicadores Sim/Não (KEV, ransomware), vermelho indica presença e verde ausência, e o EPSS usa as mesmas faixas das porcentagens de exposição.

Fontes externas

- IBM, Cost of a Data Breach Report 2026 (custo, tempo de identificação, ataques com IA).
- Verizon, 2026 Data Breach Investigations Report (envolvimento de terceiros).
- CISA, Known Exploited Vulnerabilities Catalog; FIRST/Empirical Security, EPSS.
- Análises setoriais de tendências 2026 para a América Latina (ESET, entre outras) e imprensa especializada.

Sobre a SecurityScorecard

A SecurityScorecard é a líder global em gestão de risco de terceiros (TPRM) baseada em inteligência de ameaças, protegendo as cadeias de suprimentos do mundo. A empresa oferece uma abordagem de TPRM baseada em inteligência de ameaças que permite às organizações eliminar o risco na origem. A plataforma usa visibilidade contínua e fluxos de trabalho acelerados por IA para ajudar as organizações a reduzir o risco de terceiros antes que ocorram incidentes e a responder com confiança quando eles acontecem.

Com a confiança de 3.000 organizações, incluindo mais de 70% da Fortune 100, e reconhecida como uma fonte confiável pela Agência de Segurança Cibernética e de Infraestrutura dos EUA (CISA). Apoiada pela Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, Google Ventures e Riverwood Capital, a SecurityScorecard oferece segurança cibernética de cadeia de suprimentos de ponta a ponta, que protege a continuidade dos negócios.

Proteja a cadeia de suprimentos por trás do seu negócio. Saiba mais em securityscorecard.com.