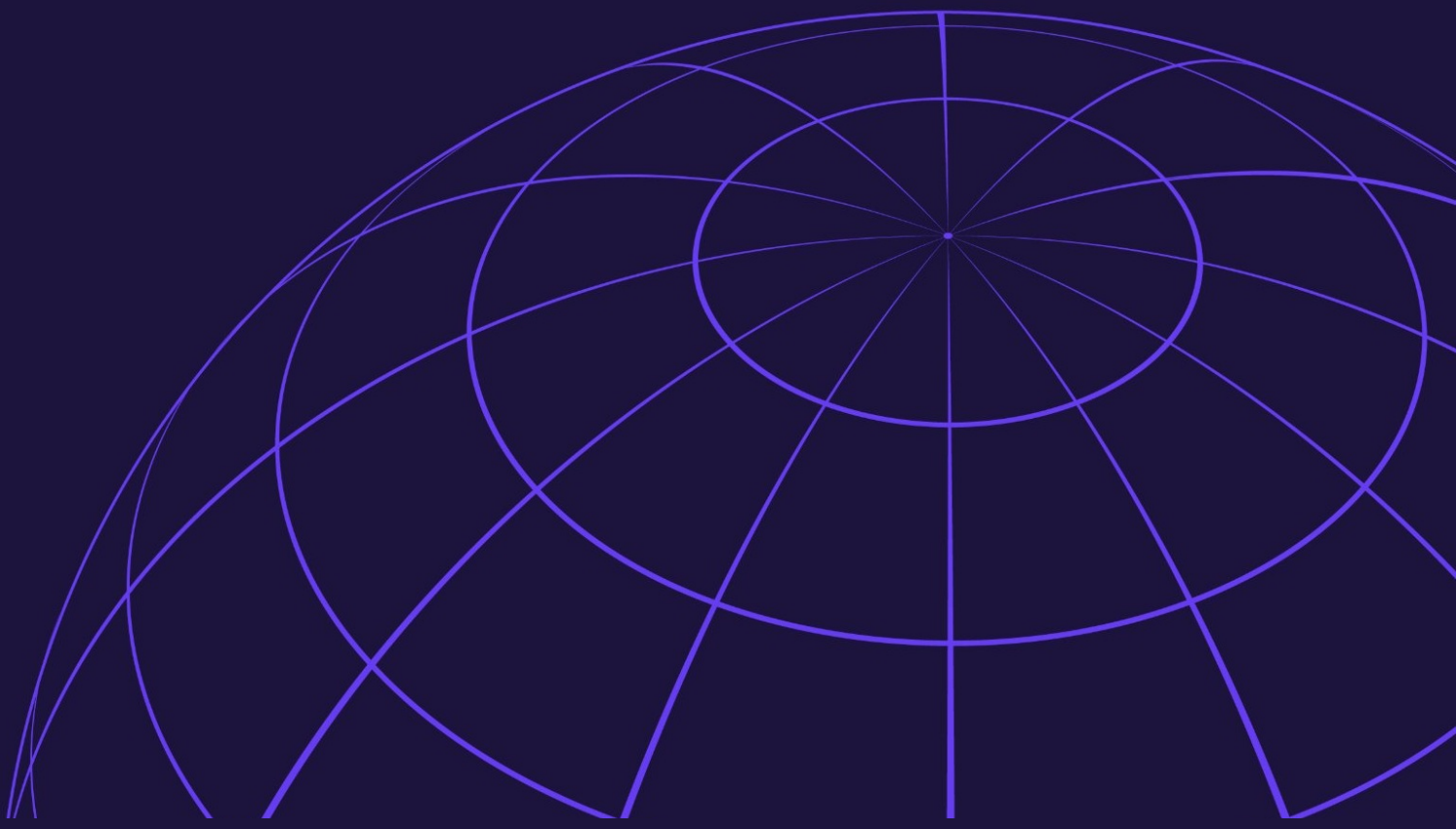
SecurityScorecard

INFORME | NOVIEMBRE DE 2026

Ciberseguridad en las mayores empresas de América Latina

Benchmark por país e industria: LATAM 500

500	19	16	75,1
EMPRESAS	PAÍSES	INDUSTRIAS	SCORE MEDIO



Datos del 8 de noviembre de 2026 | Fuentes: SecurityScorecard y Driftnet

Resumen ejecutivo

Las 500 mayores empresas de América Latina, por país y por industria

EMPRESAS ANALIZADAS	SCORE MEDIO	NOTA A O B	POR DEBAJO DE 70
500	75,1	48%	37%
19 países, 16 industrias	nota C	de las empresas	nota F: 22%

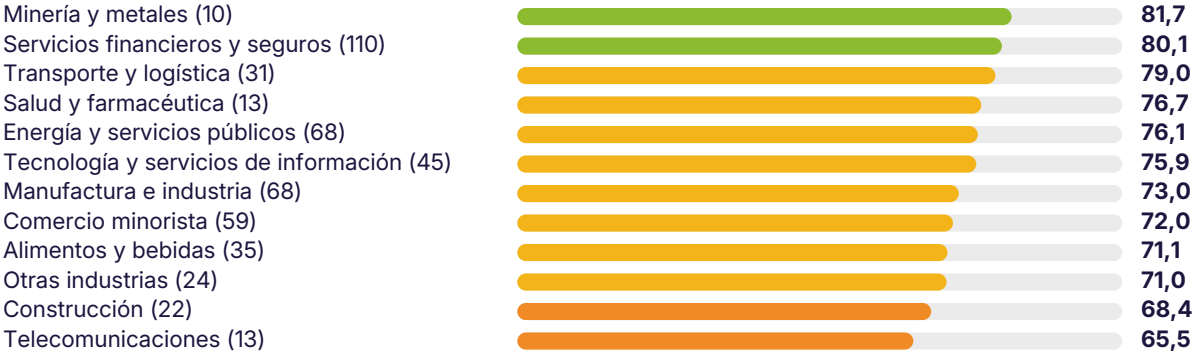
Principales conclusiones

- **País:** Colombia lidera, con una media de 78,2, y México cierra el ranking, con 72,1: una diferencia de 6,1 puntos entre los extremos.
- **Industria:** Minería y metales tiene la mejor media (81,7) y Telecomunicaciones la peor (65,5), una diferencia de 16,2 puntos.
- **Mezcla sectorial:** parte de las diferencias entre países proviene de qué industrias concentra cada uno. Tras ajustar por la composición por industria, 2 de los 6 países cambian de posición en el ranking.
- **Cola de riesgo:** el 37% de las empresas queda por debajo de 70. La proporción es mayor en Construcción (59%) y en México (49%).
- **Exposición crítica:** el 52% de las empresas expone al menos una vulnerabilidad del catálogo de explotación activa de la CISA (KEV) y el 24% tiene una CVE KEV asociada a ransomware. El pico por industria es Telecomunicaciones (100%).
- **Tendencia:** el score medio del conjunto cayó 0,8 puntos en 12 meses (75,9 a 75,1). La mayor caída por industria fue en Construcción y, por país, en Colombia.
- **Tamaño:** entre las empresas con tamaño informado, las de más de 10.000 empleados tienen una media de 78,6 y las de 1.001 a 5.000, 78,6. El tamaño solo se conoce para el 44% de la muestra.

Media por país

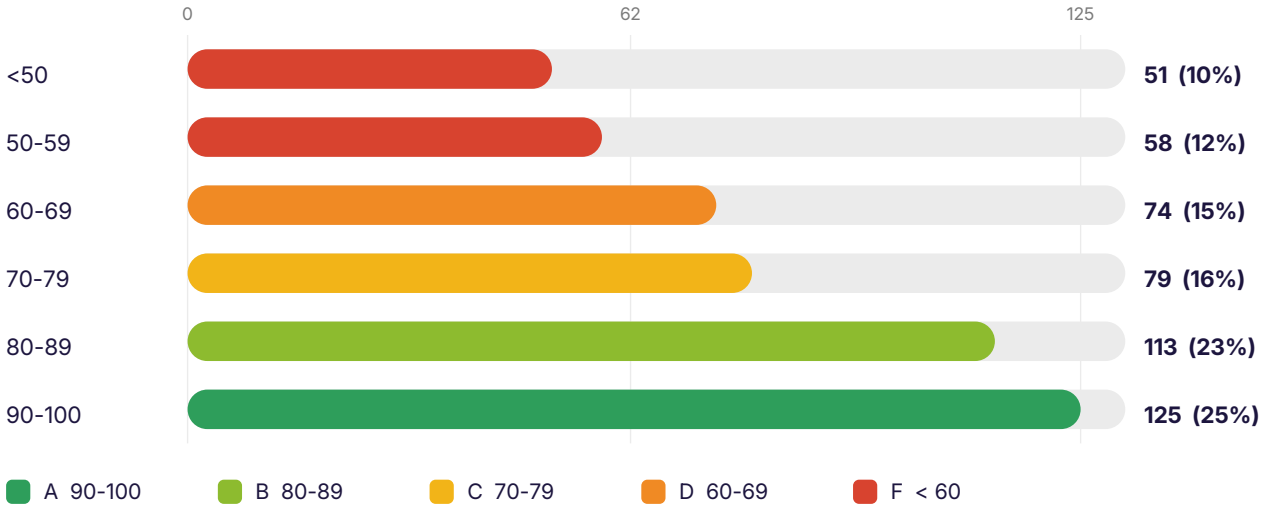


Media por industria



Panorama general

Distribución de los scores de las empresas analizadas



Medidas de posición y dispersión

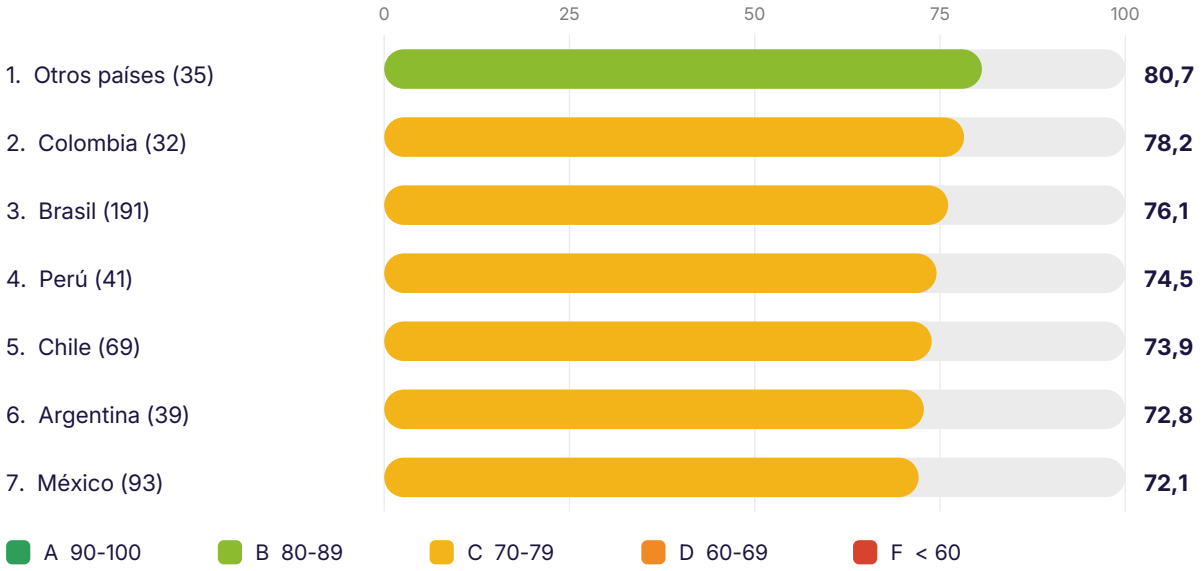
Medida	Valor
Media	75,1
Mediana	78,0
1.er cuartil	62,8
3.er cuartil	89,2
Mínimo	19
Máximo	100
Rango intercuartílico	26,5

Lectura

- La mediana (78,0) queda por encima de la media (75,1): la cola de empresas con score bajo arrastra la media hacia abajo.
- La mitad de las empresas está entre 62,8 y 89,2 puntos, un rango de 26,5: la postura de ciberseguridad es muy heterogénea incluso entre las mayores empresas de la región.
- El 22% de las empresas tiene nota F (por debajo de 60) y el 25% tiene nota A (90 o más).

Ranking por país

Score medio de las mayores empresas, por país de la sede o de la operación principal



Valores por segmento

País	Empresas	Media	Mediana	Q1-Q3	% A o B	% por debajo de 70	Var. 12m	Efecto comp.
Otros países	35	80,7	84,0	73-94	63%	23%	-0,2	+2,9
Colombia	32	78,2	79,5	68-90	50%	34%	-4,8	+1,9
Brasil	191	76,1	78,0	64-90	48%	32%	+0,2	+1,2
Perú	41	74,5	78,0	64-88	46%	32%	+1,0	-1,1
Chile	69	73,9	77,0	58-86	46%	38%	-1,2	-0,7
Argentina	39	72,8	77,0	58-90	46%	44%	+0,7	-2,2
México	93	72,1	71,0	58-87	42%	49%	-2,8	-2,3

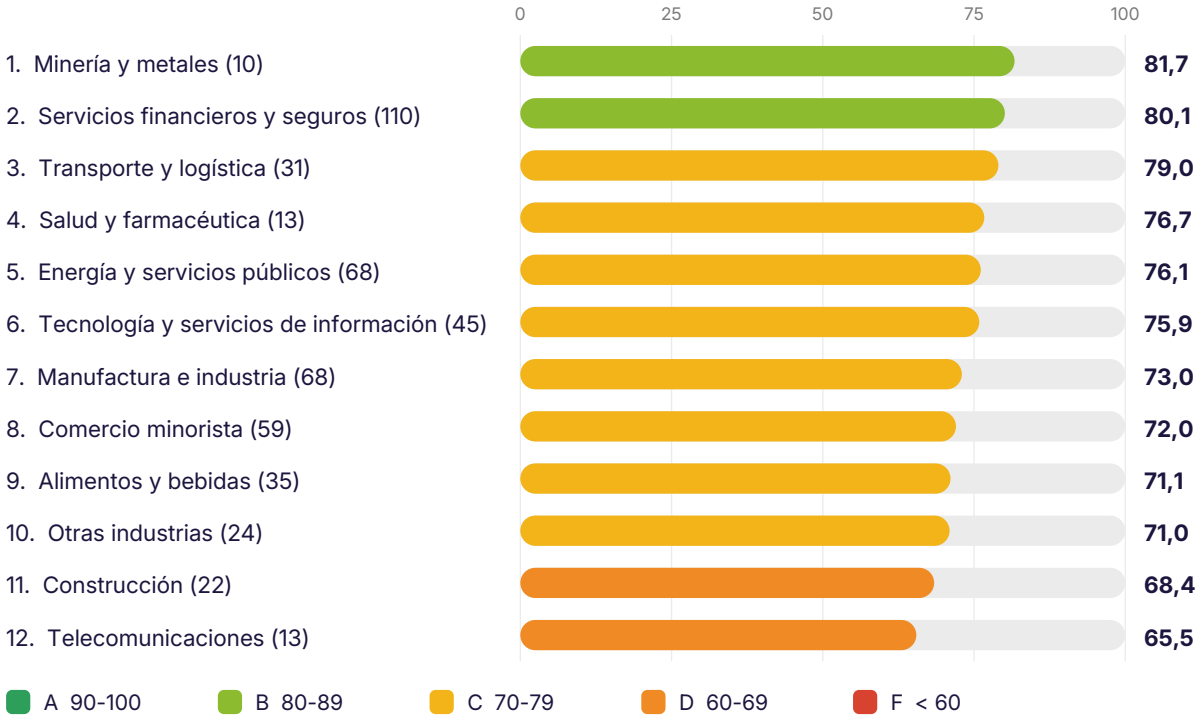
Efecto comp.: diferencia entre la media observada y la esperada por la mezcla del otro eje (industrias en el ranking por país, países en el ranking por industria), en puntos. Var. 12m: variación del score medio de las mismas empresas.

Lectura

- Colombia y Brasil lideran, con 78,2 y 76,1. En el otro extremo, México tiene 72,1.
- La proporción de empresas por debajo de 70 va del 32% (Perú) al 49% (México).

Ranking por industria

Score medio de las mayores empresas, por industria (clasificación de SecurityScorecard)



Valores por segmento

Industria	Empresas	Media	Mediana	Q1-Q3	% A o B	% por debajo de 70	Var. 12m	Efecto comp.
Minería y metales	10	81,7	82,5	74-88	60%	10%	-0,6	+7,6
Servicios financieros y seguros	110	80,1	83,5	70-92	63%	25%	-0,2	+4,2
Transporte y logística	31	79,0	83,0	70-90	55%	26%	+1,4	+4,0
Salud y farmacéutica	13	76,7	74,0	68-93	38%	31%	+4,2	+0,7
Energía y servicios públicos	68	76,1	79,5	63-89	50%	31%	-2,2	+0,8
Tecnología y servicios de información	45	75,9	80,0	67-90	51%	42%	-0,3	+0,9
Manufactura e industria	68	73,0	76,5	58-88	40%	40%	-1,8	-1,8
Comercio minorista	59	72,0	72,0	58-86	41%	47%	-2,9	-2,7
Alimentos y bebidas	35	71,1	72,0	56-84	40%	46%	+0,8	-4,0
Otras industrias	24	71,0	71,0	55-83	46%	50%	-0,3	-3,7
Construcción	22	68,4	67,0	55-80	27%	59%	-3,4	-6,1
Telecomunicaciones	13	65,5	71,0	57-74	8%	38%	+3,7	-8,3

Efecto comp.: diferencia entre la media observada y la esperada por la mezcla del otro eje (industrias en el ranking por país, países en el ranking por industria), en puntos. Var. 12m: variación del score medio de las mismas empresas.

Lectura

- Minería y metales (81,7) y Servicios financieros y seguros (80,1) tienen las mejores medias; Telecomunicaciones (65,5) y Construcción (68,4) las peores.
- La industria con mayor proporción de empresas con nota F es Alimentos y bebidas (34%); la menor es Minería y metales (0%).

País × industria

Score medio por combinación (celdas con 3 o más empresas; entre paréntesis cuando hay menos de 5)

	Brasil (191)	México (93)	Chile (69)	Perú (41)	Argentina (39)	Colombia (32)	Otros países (35)	Total
Minería y metales (10)	-	-	(76)	(86)	-	-	-	**82**
Servicios financieros y seguros (110)	82	74	89	79	73	89	76	**80**
Transporte y logística (31)	81	75	-	-	-	-	-	**79**
Salud y farmacéutica (13)	76	-	-	-	-	-	-	**77**
Energía y servicios públicos (68)	79	-	75	60	78	68	-	**76**
Tecnología y servicios de información (45)	73	67	85	(85)	70	-	(89)	**76**
Manufactura e industria (68)	75	74	66	(70)	(74)	(72)	-	**73**
Comercio minorista (59)	73	67	71	-	-	-	-	**72**
Alimentos y bebidas (35)	74	(68)	65	(87)	(62)	(71)	(80)	**71**
Otras industrias (24)	68	76	-	-	-	-	-	**71**
Construcción (22)	75	67	(66)	(60)	-	-	-	**68**
Telecomunicaciones (13)	(70)	72	-	-	-	-	-	**65**
Total	**76**	**72**	**74**	**75**	**73**	**78**	**81**	**75**

Número de empresas por combinación

	Brasil	México	Chile	Perú	Argentina	Colombia	Otros países
Minería y metales	1	1	3	4	1	-	-
Servicios financieros y seguros	30	20	10	12	6	13	19
Transporte y logística	16	9	2	-	1	1	2
Salud y farmacéutica	11	1	-	-	-	1	-
Energía y servicios públicos	33	2	10	5	11	6	1
Tecnología y servicios de información	16	7	7	4	6	1	4
Manufactura e industria	31	16	9	4	4	3	1
Comercio minorista	24	14	13	2	2	2	2
Alimentos y bebidas	8	3	10	4	4	3	3
Otras industrias	10	9	1	1	1	-	2
Construcción	6	6	3	4	1	2	-
Telecomunicaciones	4	5	1	1	2	-	-

Coloreadas según las notas A a F. Las celdas entre paréntesis tienen 3 o 4 empresas y son poco robustas: una sola empresa cambia la media en muchos puntos. "-" indica menos de 3 empresas (no se muestra). Las columnas y filas de total usan todas las empresas del segmento.

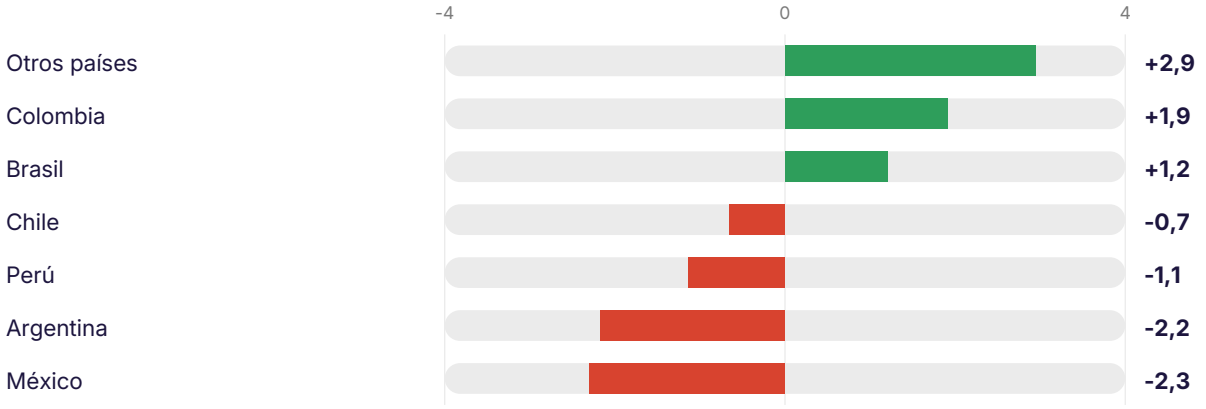
Lectura

- Las combinaciones con mejor score son Servicios financieros y seguros en Colombia (89, 13 empresas); Servicios financieros y seguros en Chile (89, 10 empresas); Tecnología y servicios de información en Chile (85, 7 empresas).
- Las peores son Energía y servicios públicos en Perú (60, 5 empresas); Alimentos y bebidas en Chile (65, 10 empresas); Manufactura e industria en Chile (66, 9 empresas).
- Una misma industria varía mucho entre países: la mayor amplitud entre países dentro de una industria es de 19 puntos.

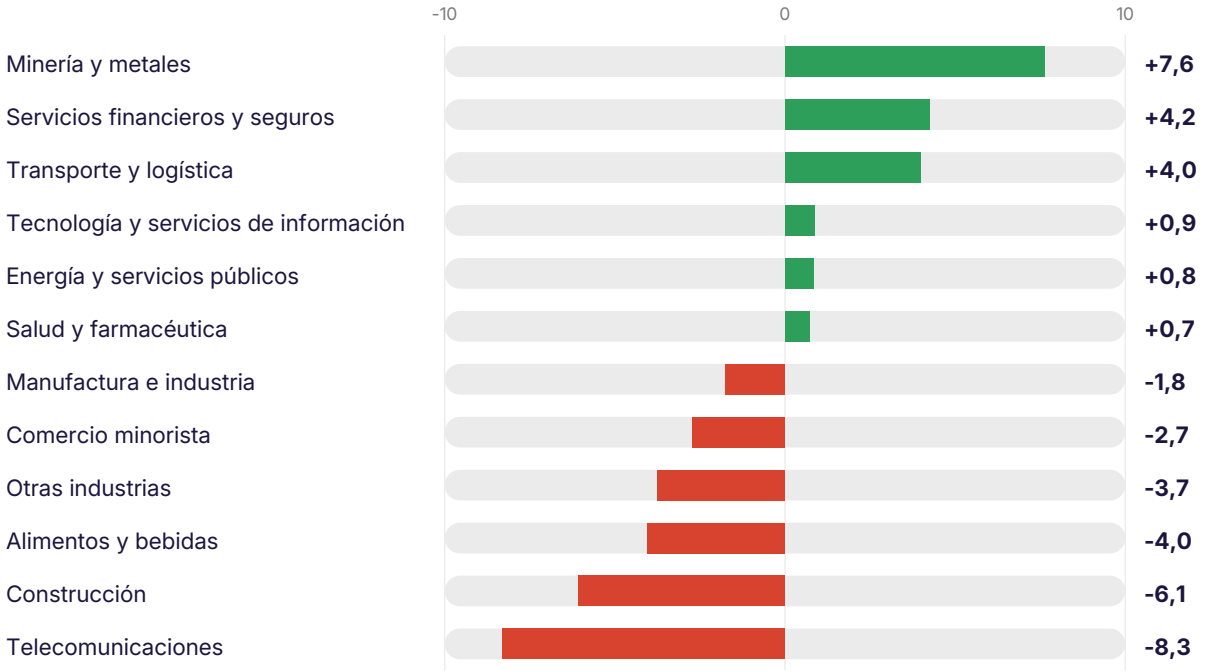
Efecto de composición

Cuánto se aleja cada país y cada industria de lo esperado por la mezcla del otro eje

Países: media observada menos la media esperada por la mezcla de industrias (puntos)



Industrias: media observada menos la esperada por la mezcla de países (puntos)

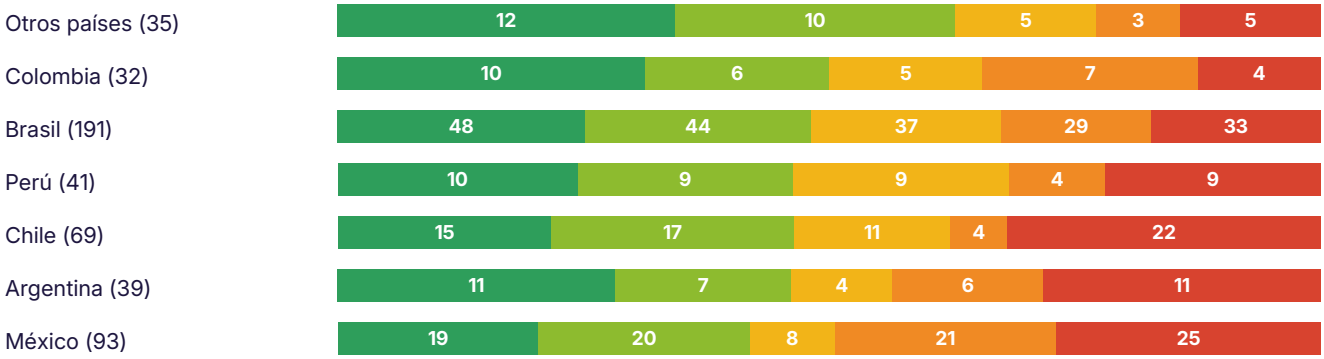


- Un efecto positivo significa que el país tiene un score superior al que tendría si cada una de sus industrias tuviera el score medio regional de esa industria: es desempeño propio del país, independiente de qué industrias concentre. Colombia tiene el mayor efecto (+1,9) y México el menor (-2,3).
- El ajuste cambia la posición de 2 de los 6 países. La comparación entre países debe mirar el ranking bruto y el efecto conjuntamente.
- En las industrias, el mayor efecto es Minería y metales (+7,6) y el menor, Telecomunicaciones (-8,3).

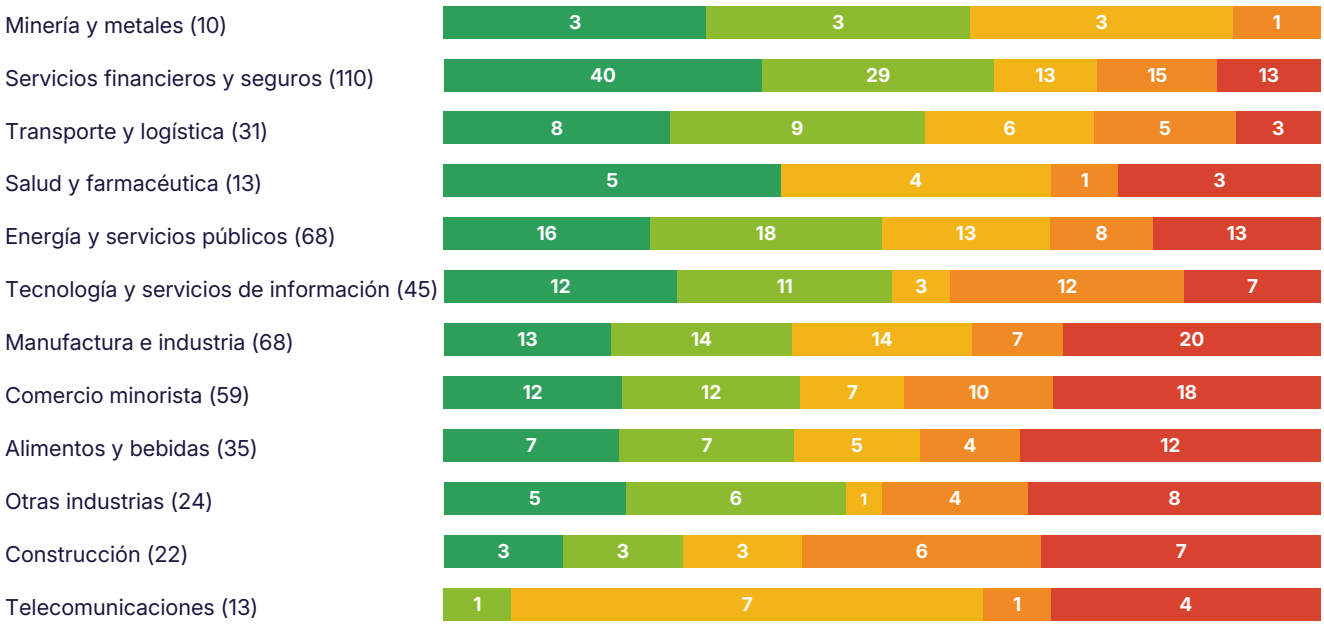
Distribución de notas

Número de empresas en cada franja de nota, por país y por industria

Por país



Por industria



A 90-100 B 80-89 C 70-79 D 60-69 F < 60

Cada barra suma el 100% de las empresas del segmento; los números muestran la cantidad de empresas en cada nota.

Factores de riesgo

Score medio por factor de SecurityScorecard, por industria y por país

Por industria

	Red	Aplicaciones	Patching	Info. expuesta	DNS	Endpoints
Minería y metales	80,7	88,8	91,4	99,1	99,5	100,0
Servicios financieros y seguros	82,0	84,6	85,1	91,2	90,9	97,1
Transporte y logística	79,0	86,3	84,9	93,5	96,2	98,5
Salud y farmacéutica	77,2	83,5	79,7	90,8	87,8	92,4
Energía y servicios públicos	79,1	83,3	78,9	93,2	92,8	96,8
Tecnología y servicios de información	79,0	79,7	86,1	95,3	91,6	99,0
Manufactura e industria	75,5	82,4	79,9	98,8	92,9	97,2
Comercio minorista	73,9	80,1	77,3	92,3	90,6	97,6
Alimentos y bebidas	75,2	80,3	76,9	95,9	89,2	95,6
Otras industrias	70,9	83,6	79,4	92,8	86,8	91,3
Construcción	69,7	81,1	80,5	97,0	95,8	99,5
Telecomunicaciones	66,4	78,2	63,2	73,2	81,8	57,8

Por país

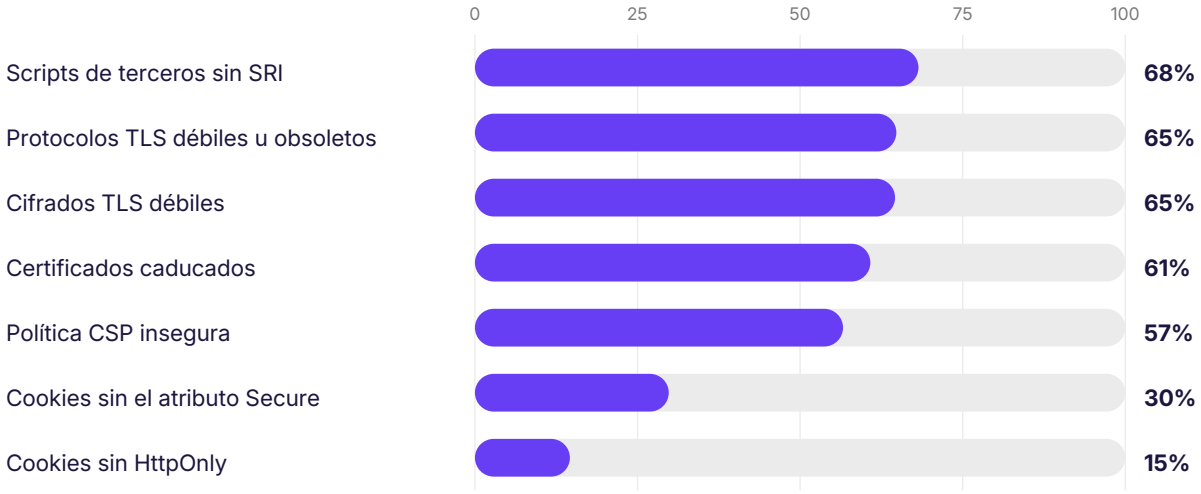
	Red	Aplicaciones	Patching	Info. expuesta	DNS	Endpoints
Otros países	84,3	83,0	87,6	95,8	97,7	99,4
Colombia	80,5	86,2	81,1	93,3	99,1	97,4
Brasil	77,2	82,6	80,5	90,7	86,4	94,5
Perú	78,3	80,5	82,1	96,2	95,3	97,4
Chile	76,1	84,8	80,3	96,3	95,9	98,2
Argentina	76,7	80,2	81,3	92,5	90,7	93,2
México	74,0	81,7	79,5	95,7	92,8	96,4

Lectura

- Los factores más frágiles en el conjunto son seguridad de red (77,2), cadencia de parcheo (81,0) y seguridad de aplicaciones (82,6).
- La seguridad de red es el factor más débil en 10 de las 12 industrias y en 6 de los 7 países.
- La peor seguridad de red está en Telecomunicaciones (66,4) y la peor cadencia de parcheo en Telecomunicaciones (63,2).

Vulnerabilidades más comunes

Porcentaje de empresas con al menos una ocurrencia de cada problema



Por industria (% de empresas afectadas)

	Sin SRI	TLS débil	Cifrados débiles	Cert. caducado	CSP insegura	Cookie sin Secure
Minería y metales	40%	40%	50%	60%	30%	10%
Servicios financieros y seguros	62%	57%	53%	65%	65%	23%
Transporte y logística	71%	61%	71%	61%	71%	26%
Salud y farmacéutica	77%	77%	77%	77%	77%	38%
Energía y servicios públicos	69%	59%	62%	56%	63%	28%
Tecnología y servicios de información	62%	64%	62%	53%	44%	42%
Manufactura e industria	69%	69%	60%	60%	50%	28%
Comercio minorista	71%	69%	75%	68%	54%	32%
Alimentos y bebidas	74%	66%	63%	54%	54%	29%
Otras industrias	71%	71%	79%	50%	38%	29%
Construcción	73%	77%	82%	45%	45%	27%
Telecomunicaciones	92%	100%	100%	92%	77%	85%

Por país (% de empresas afectadas)

	Sin SRI	TLS débil	Cifrados débiles	Cert. caducado	CSP insegura	Cookie sin Secure
Otros países	71%	51%	54%	57%	60%	23%
Colombia	53%	47%	53%	59%	50%	25%
Brasil	76%	72%	73%	69%	66%	34%
Perú	56%	51%	56%	54%	61%	39%
Chile	62%	65%	65%	54%	45%	19%
Argentina	59%	64%	56%	56%	51%	31%
México	69%	67%	61%	57%	47%	30%

Qué son y por qué importan

Lectura de los problemas más comunes

- **Scripts de terceros sin SRI (68%):** páginas que cargan JavaScript externo sin verificación de integridad. Si el proveedor es comprometido, el código malicioso se ejecuta en el sitio de la empresa, vector típico de los ataques a la cadena de suministro y del skimming web.
- **TLS débil y cifrados débiles (65% y 65%):** servidores que aún aceptan versiones antiguas del protocolo, exponiendo las conexiones a degradación de versión e interceptación.
- **Cookies sin Secure (30%) o HttpOnly (15%):** facilitan el robo de sesión en canales autenticados.
- **Certificados caducados (61%) y CSP insegura (57%):** de severidad baja, pero muy extendidos e indicativos de fallos de inventario y de proceso.
- Para el problema más común (scripts de terceros sin SRI), la prevalencia va del 40% en Minería y metales al 92% en Telecomunicaciones.

Vulnerabilidades más críticas

Exposición a fallos ya explotados activamente, no solo a fallos con puntuación CVSS alta

CON CVE ALTA O CRÍTICA
67%
de las empresas

CON CVE DEL CATÁLOGO KEV
52%
explotación activa (CISA)

KEV LIGADA A RANSOMWARE
24%
campañas conocidas

EPSS SUPERIOR AL 90%
58%
alta probabilidad

Por industria (% de empresas)

Segmento	CVE alta/crítica	CVE en KEV	KEV + ransomware	EPSS superior al 90%
Minería y metales	30%	30%	0%	20%
Servicios financieros y seguros	60%	48%	21%	53%
Transporte y logística	71%	52%	13%	58%
Salud y farmacéutica	77%	62%	54%	77%
Energía y servicios públicos	74%	56%	31%	63%
Tecnología y servicios de información	58%	42%	16%	49%
Manufactura e industria	71%	50%	26%	57%
Comercio minorista	64%	54%	24%	59%
Alimentos y bebidas	74%	57%	17%	66%
Otras industrias	75%	50%	21%	54%
Construcción	68%	50%	18%	59%
Telecomunicaciones	100%	100%	92%	100%

Por país (% de empresas)

Segmento	CVE alta/crítica	CVE en KEV	KEV + ransomware	EPSS superior al 90%
Otros países	51%	43%	11%	46%
Colombia	66%	34%	12%	47%
Brasil	74%	58%	29%	64%
Perú	66%	41%	22%	49%
Chile	61%	55%	19%	59%
Argentina	67%	51%	26%	56%
México	65%	52%	28%	57%

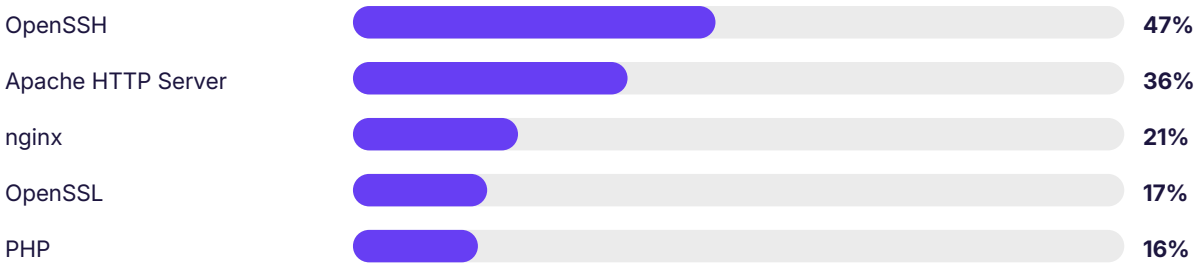
- La exposición a KEV es mayor en Telecomunicaciones (100%) y menor en Minería y metales (30%); por país, va del 34% (Colombia) al 58% (Brasil).

Vulnerabilidades más extendidas

Fallos del catálogo KEV encontrados en más empresas

CVE	Producto	% empresas	EPSS	Ransomware
CVE-2023-44487	IETF HTTP/2	33%	100,0%	No
CVE-2024-38475	Apache HTTP Server	25%	100,0%	No
CVE-2021-40438	Apache Apache	20%	100,0%	Sí
CVE-2025-24813	Apache Tomcat	12%	99,9%	No
CVE-2026-109619	PHP Group PHP	10%	100,0%	No
CVE-2019-0211	Apache HTTP Server	9%	65,0%	No
CVE-2026-31431	Linux Kernel	7%	98,1%	No
CVE-2023-4863	Google Chromium WebP	7%	100,0%	No

Familias de software más expuestas (CVE alta o crítica)

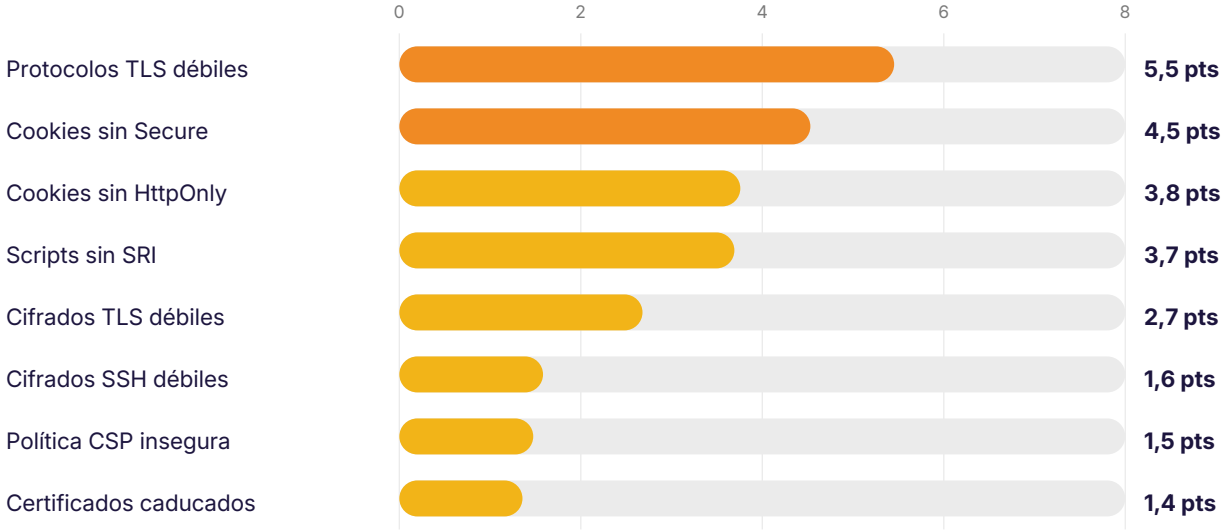


SecurityScorecard infiere las versiones de software a partir de señales externas (banners). Parte de los hallazgos puede estar corregida mediante backports y debe validarse internamente.

Vulnerabilidades de mayor impacto

Impacto en el score y coste potencial de un incidente

Puntos de score perdidos por empresa afectada (media)



Contexto económico

COSTE MEDIO GLOBAL DE UNA BRECHA
USD 4,99 M
IBM 2026

SECTOR FINANCIERO
USD 6,29 M
IBM 2026, frente a 5,56 M en 2025

ATAQUES CON IA
+1 M USD
coste adicional medio por brecha

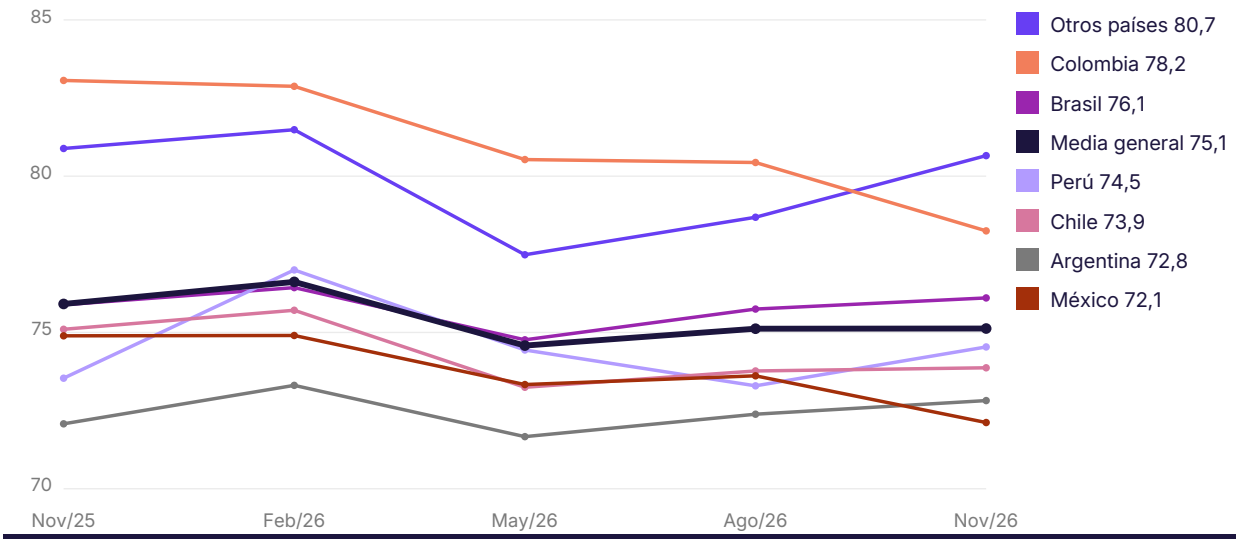
El coste medio varía según la industria; el informe de IBM destaca el sector financiero como uno de los más caros. Las cifras son medias globales y no miden las empresas de este informe.

Lectura

- Los fallos que más puntos cuestan son de configuración sencilla: protocolos TLS débiles (5,5 puntos por empresa afectada), cookies sin Secure (4,5) y cookies sin HttpOnly (3,8). Corregirlos es barato y tiene un retorno inmediato en el score.
- Los problemas de menor severidad individual (CSP, certificados caducados) pesan por su escala: aparecen en la mitad o más de las empresas.
- En cuanto al riesgo real, el mayor impacto procede de las vulnerabilidades KEV vinculadas a ransomware y de los incidentes en la cadena de proveedores: el informe Verizon DBIR 2026 indica que la participación de terceros en las brechas subió hasta el 48%, frente al 30% del año anterior.

Tendencia por país

Evolución del score medio en los últimos 12 meses



Segmento	Nov/25	Feb/26	May/26	Ago/26	Nov/26	Var. 12m
Otros países	80,9	81,5	77,5	78,7	80,7	-0,2
Colombia	83,1	82,9	80,5	80,4	78,2	-4,8
Brasil	75,9	76,4	74,8	75,7	76,1	+0,2
Perú	73,5	77,0	74,4	73,3	74,5	+1,0
Chile	75,1	75,7	73,2	73,8	73,9	-1,2
Argentina	72,1	73,3	71,7	72,4	72,8	+0,7
México	74,9	74,9	73,3	73,6	72,1	-2,8
Media general	**75,9**	**76,6**	**74,6**	**75,1**	**75,1**	**-0,8**

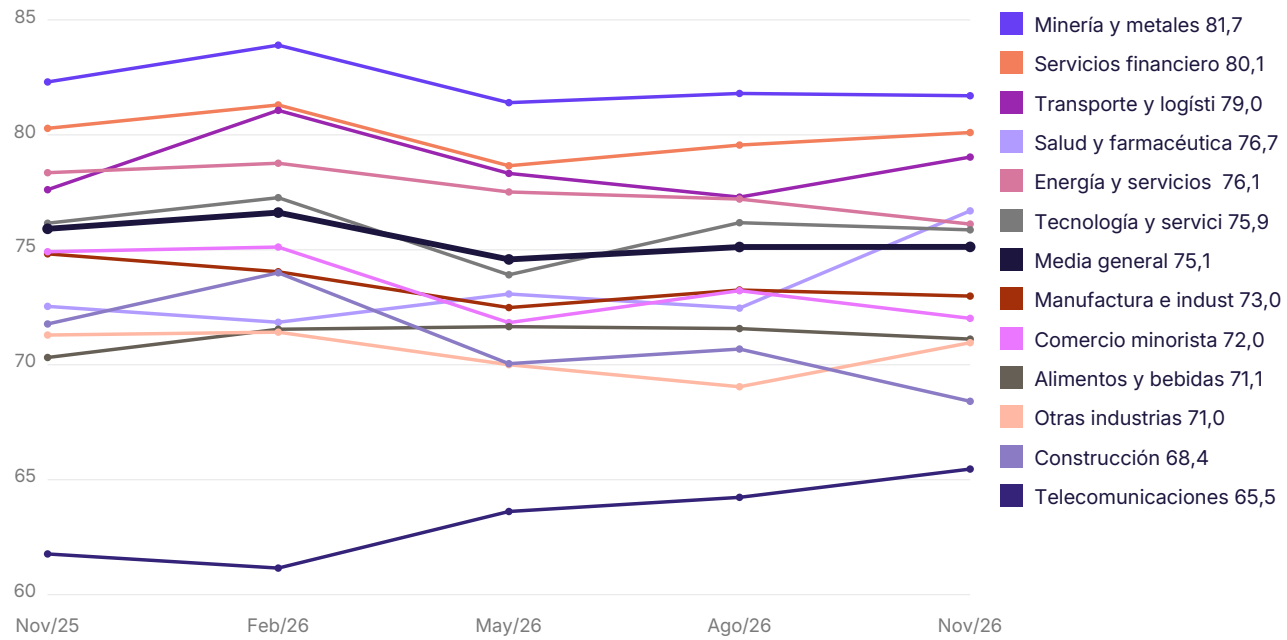
Media de las mismas empresas a lo largo del tiempo (solo empresas con historial completo en las cinco fechas).

Lectura

- 4 de los 7 países perdieron puntos en 12 meses, desde 1,0 (Perú, mejor desempeño) hasta 4,8 (Colombia, mayor caída).
- En conjunto, el score medio pasó de 75,9 a 75,1 (-0,8).

Tendencia por industria

Evolución del score medio en los últimos 12 meses



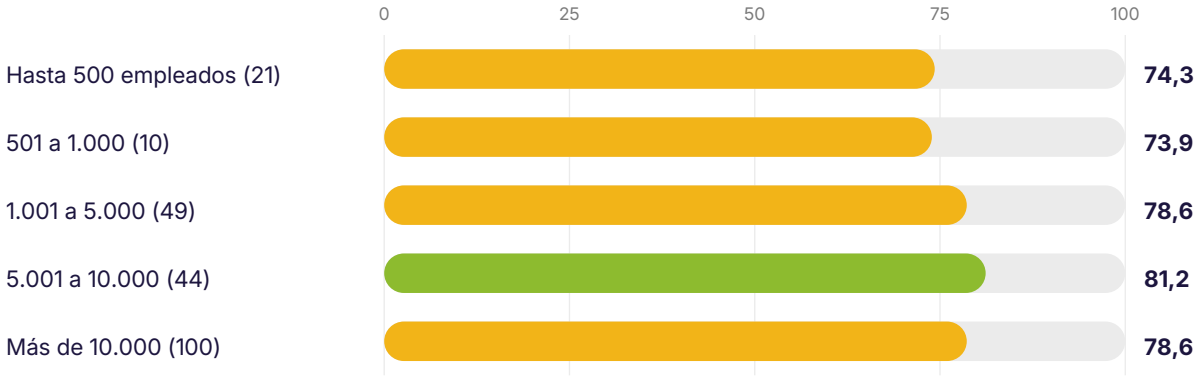
Segmento	Nov/25	Feb/26	May/26	Ago/26	Nov/26	Var. 12m
Minería y metales	82,3	83,9	81,4	81,8	81,7	-0,6
Servicios financieros y seguros	80,3	81,3	78,7	79,6	80,1	-0,2
Transporte y logística	77,6	81,1	78,3	77,3	79,0	+1,4
Salud y farmacéutica	72,5	71,8	73,1	72,5	76,7	+4,2
Energía y servicios públicos	78,4	78,8	77,5	77,2	76,1	-2,2
Tecnología y servicios de información	76,2	77,3	73,9	76,2	75,9	-0,3
Manufactura e industria	74,8	74,0	72,5	73,2	73,0	-1,8
Comercio minorista	74,9	75,1	71,8	73,2	72,0	-2,9
Alimentos y bebidas	70,3	71,5	71,7	71,6	71,1	+0,8
Otras industrias	71,3	71,4	70,0	69,0	71,0	-0,3
Construcción	71,8	74,0	70,0	70,7	68,4	-3,4
Telecomunicaciones	61,8	61,2	63,6	64,2	65,5	+3,7
Media general	**75,9**	**76,6**	**74,6**	**75,1**	**75,1**	**-0,8**

Media de las mismas empresas a lo largo del tiempo (solo empresas con historial completo en las cinco fechas).

- 8 de las 12 industrias perdieron puntos en 12 meses. La mayor caída fue en Construcción (-3,4); el mejor desempeño, en Salud y farmacéutica (+4,2).

Tamaño de la empresa

Score por franja de empleados (tamaño informado para 224 de las 500 empresas, 44%)



Franja	Empresas	Media	Mediana	% por debajo de 70	% KEV
Hasta 500 empleados	21	74,3	76,0	43%	57%
501 a 1.000	10	73,9	64,5	60%	40%
1.001 a 5.000	49	78,6	80,0	29%	47%
5.001 a 10.000	44	81,2	85,5	20%	43%
Más de 10.000	100	78,6	81,5	27%	57%

SecurityScorecard no informa el tamaño de más de la mitad de las empresas; las conclusiones valen solo para las que tienen tamaño conocido.

Lectura

- La mejor media está en la franja 5.001 a 10.000 (81,2) y la peor en 501 a 1.000 (73,9).
- Las empresas mayores tienen más superficie expuesta (más dominios, proveedores y sistemas), lo que tiende a pesar en el score; los tamaños menores tienen menos observaciones y mayor variabilidad.

Exposición de la infraestructura propia

Lente Driftnet: servicios expuestos y vulnerabilidades en las IP registradas a nombre de las empresas

CON INFRA PROPIA
167 de 500
33% de las empresas

SERVICIO SENSIBLE EXPUESTO
34%
FTP, admin. remota, SMB o BD

CVE KEV (DRIFTNET)
29%
en las IP propias

CVE KEV (SECURITYSCORECARD)
60%
mismas empresas

Por industria

Segmento	Con infra	Servicio sensible	FTP	Admin. remota	KEV (Driftnet)	KEV (SSC)
Minería y metales	2 / 10	-	-	-	-	-
Servicios financieros y seguros	37 / 110	22%	19%	14%	35%	54%
Transporte y logística	13 / 31	8%	0%	0%	15%	46%
Salud y farmacéutica	6 / 13	50%	17%	0%	33%	67%
Energía y servicios públicos	34 / 68	38%	21%	21%	29%	56%
Tecnología y servicios de información	7 / 45	29%	14%	29%	14%	86%
Manufactura e industria	19 / 68	26%	16%	11%	16%	58%
Comercio minorista	22 / 59	45%	18%	36%	45%	64%
Alimentos y bebidas	12 / 35	50%	17%	33%	8%	75%
Otras industrias	4 / 24	-	-	-	-	-
Construcción	9 / 22	33%	11%	22%	33%	78%
Telecomunicaciones	2 / 13	-	-	-	-	-

Por país

Segmento	Con infra	Servicio sensible	FTP	Admin. remota	KEV (Driftnet)	KEV (SSC)
Otros países	9 / 35	0%	0%	0%	11%	44%
Colombia	12 / 32	58%	42%	33%	50%	58%
Brasil	84 / 191	39%	20%	21%	31%	63%
Perú	11 / 41	18%	18%	18%	18%	64%
Chile	22 / 69	36%	9%	32%	23%	68%
Argentina	15 / 39	20%	13%	7%	33%	53%
México	14 / 93	21%	14%	21%	21%	50%

Porcentajes sobre las empresas con infraestructura propia identificada en cada segmento (mínimo de 5). KEV (SSC): lente SecurityScorecard sobre las mismas empresas. 8 empresas con espacio de direcciones de escala de proveedor (más de 20.000 IP) fueron excluidas. por no representar infraestructura corporativa.

Lectura

- El 33% de las empresas tiene infraestructura propia identificable; el resto publica sus servicios a través de cloud, CDN, WAF u operadores, lo que traslada parte del riesgo a terceros.
- En las 167 empresas con infraestructura propia, el 34% expone al menos un servicio sensible (FTP en el 18% y administración remota en el 21%).
- En las mismas empresas, SecurityScorecard señala KEV en el 60% y Driftnet en el 29%; juntas, el 68%, y ambas a la vez, el 21%. Las lentes tienen alcances distintos y se complementan: SecurityScorecard evalúa el dominio de la empresa y los activos que se le atribuyen, y Driftnet observa las direcciones IP registradas a nombre de la empresa.

Tendencias de amenazas en la región

Lo que indican las fuentes externas para las mayores empresas de América Latina

- **Región bajo presión.** El informe de Intel 471 para 2026 señala una media de 2.640 ataques semanales por organización en América Latina, un 35% por encima de la media global, y filtraciones por ransomware un 78% mayores en 2025 que en 2024 (de más de 250 a más de 450), con el número de variantes activas pasando de 48 a 79.

- **Industria e infraestructura crítica.** Según Kaspersky ICS CERT (julio de 2026), el 20,4% de los computadores de sistemas de control industrial de la región registró actividad maliciosa, la segunda región más expuesta del mundo. Por sector, las mayores tasas fueron construcción (21,9%), energía eléctrica (19%) y manufactura (15,7%).

- **Energía, logística y manufactura en la mira.** Un estudio de Kaspersky divulgado en julio de 2026 indica que petróleo, gas y energía concentran el 27% de los ataques contra empresas de la región, seguidos de transporte y logística (18%) y manufactura (15%). IBM X-Force ya señalaba la energía con el 20% de los incidentes regionales en 2024.

- **Ransomware como servicio.** Kaspersky describe el crecimiento del modelo RaaS, con kits desde US$ 40, lo que reduce la barrera de entrada. Un informe de abril de 2026 divulgado por la prensa regional cita servicios empresariales, bienes de consumo y manufactura industrial entre los objetivos preferidos.

- **IA ofensiva y automatización.** IBM estima que los ataques asistidos por IA añaden, de media, US$ 1 millón al coste de cada brecha.

- **Cadena de proveedores.** La participación de terceros en las brechas subió hasta el 48%, frente al 30% del año anterior, según el Verizon DBIR 2026. Los scripts externos sin SRI y los proveedores con score bajo son hoy una de las puertas de entrada más probables.

- **Monitorización continua.** La gestión de riesgos migra de los cuestionarios anuales a la monitorización externa continua, la priorización según la explotación real (KEV y EPSS) y métricas cuantitativas comparables entre empresas, sectores y países.

Prioridades recomendadas

- Corregir primero lo que está en KEV y tiene un EPSS alto, antes de ordenar por CVSS.
- Desactivar TLS antiguo y cifrados débiles y corregir los atributos de las cookies: es la mayor ganancia de score por esfuerzo.
- Aplicar SRI y CSP a todos los scripts de terceros.
- Segmentar rigurosamente las redes de TI y de tecnología operativa (OT) en las industrias de energía, manufactura y minería.
- Monitorizar de forma continua a los proveedores críticos y exigir niveles mínimos de score en contrato.

País: Colombia

puesto 2 de 7 segmentos | 32 empresas analizadas

SCORE MEDIO	MEDIANA	POR DEBAJO DE 70	VAR. 12M
78,2	79,5	34%	-4,8
nota C	Q1-Q3: 68-90	general 37%	puntos de score

Notas: 10 | 6 | 5 | 7 | 4

A 90-100 B 80-89 C 70-79 D 60-69 F < 60

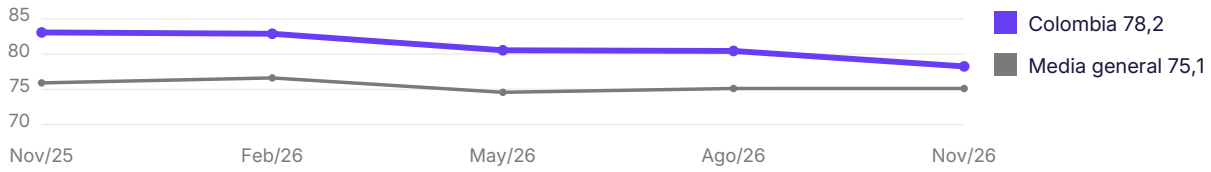
Score por factor (segmento vs general)

Red	80,5 (general 77,2)
Aplicaciones	86,2 (general 82,6)
Patching	81,1 (general 81,0)
Info. expuesta	93,3 (general 93,5)
DNS	99,1 (general 91,6)
Endpoints	97,4 (general 96,0)

Problemas más comunes (% de empresas afectadas)

Scripts de terceros sin SRI	53% (general 68%)
Protocolos TLS débiles u obsoletos	47% (general 65%)
Cifrados TLS débiles	53% (general 65%)
Certificados caducados	59% (general 61%)
Política CSP insegura	50% (general 57%)

Evolución del score medio



Análisis

Colombia ocupa el puesto 2 entre 7 segmentos, con un score medio de 78,2, que es 3,1 puntos superior a la media general de 75,1. De sus empresas, el 50% tiene nota A o B y el 34% queda por debajo de 70. Tras ajustar por la mezcla de industrias, el efecto país es de +1,9 puntos: el país tiene un desempeño superior al esperado para su composición sectorial. Entre las industrias con 5 o más empresas en el país, la mejor es Servicios financieros y seguros (89, 13 empresas) y la peor, Energía y servicios públicos (68, 6 empresas).

Frente al conjunto, el factor más fuerte es salud del DNS (+7,5) y el más débil es información expuesta (-0,2). Ninguno de los problemas más comunes ocurre por encima de la media general.

En los últimos 12 meses, el score medio cayó 4,8 puntos, de 83,1 a 78,2. En la exposición crítica, el 34% de las empresas tiene una CVE del catálogo KEV (media general: 52%) y el 12% tiene una CVE KEV asociada a ransomware (media general: 24%).

País: Brasil

puesto 3 de 7 segmentos | 191 empresas analizadas

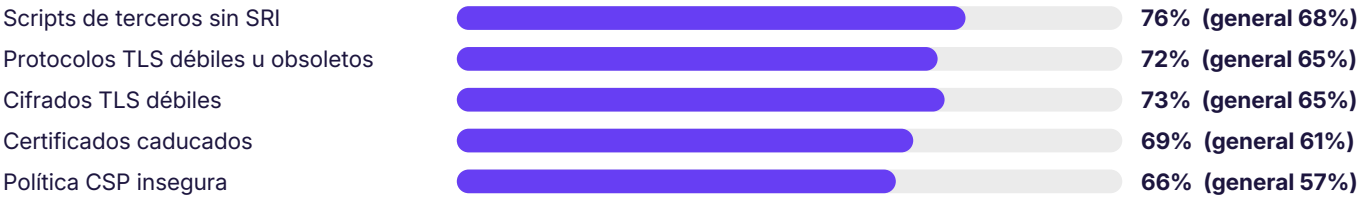
SCORE MEDIO	MEDIANA	POR DEBAJO DE 70	VAR. 12M
76,1	78,0	32%	+0,2
nota C	Q1-Q3: 64-90	general 37%	puntos de score



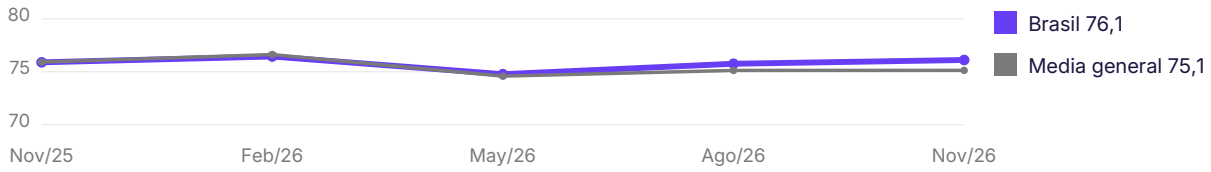
Score por factor (segmento vs general)



Problemas más comunes (% de empresas afectadas)



Evolución del score medio



Análisis

Brasil ocupa el puesto 3 entre 7 segmentos, con un score medio de 76,1, que es 1,0 puntos superior a la media general de 75,1. De sus empresas, el 48% tiene nota A o B y el 32% queda por debajo de 70. Tras ajustar por la mezcla de industrias, el efecto país es de +1,2 puntos: el país tiene un desempeño superior al esperado para su composición sectorial. Entre las industrias con 5 o más empresas en el país, la mejor es Servicios financieros y seguros (82, 30 empresas) y la peor, Otras industrias (68, 10 empresas).

Frente al conjunto, el factor más fuerte es seguridad de red (+0,0) y el más débil es salud del DNS (-5,2). El problema más por encima de la media general es política CSP insegura (66% de las empresas, frente al 57% del conjunto).

En los últimos 12 meses, el score medio subió 0,2 puntos, de 75,9 a 76,1. En la exposición crítica, el 58% de las empresas tiene una CVE del catálogo KEV (media general: 52%) y el 29% tiene una CVE KEV asociada a ransomware (media general: 24%).

País: Perú

puesto 4 de 7 segmentos | 41 empresas analizadas

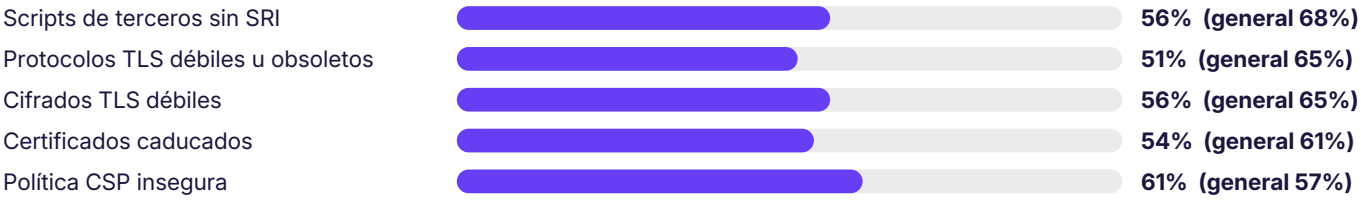
SCORE MEDIO	MEDIANA	POR DEBAJO DE 70	VAR. 12M
74,5	78,0	32%	+1,0
nota C	Q1-Q3: 64-88	general 37%	puntos de score



Score por factor (segmento vs general)



Problemas más comunes (% de empresas afectadas)



Evolución del score medio



Análisis

Perú ocupa el puesto 4 entre 7 segmentos, con un score medio de 74,5, que es 0,6 puntos inferior a la media general de 75,1. De sus empresas, el 46% tiene nota A o B y el 32% queda por debajo de 70. Tras ajustar por la mezcla de industrias, el efecto país es de -1,1 puntos: el país tiene un desempeño inferior al esperado para su composición sectorial. Entre las industrias con 5 o más empresas en el país, la mejor es Servicios financieros y seguros (79, 12 empresas) y la peor, Energía y servicios públicos (60, 5 empresas).

Frente al conjunto, el factor más fuerte es salud del DNS (+3,7) y el más débil es seguridad de aplicaciones (-2,1). El problema más por encima de la media general es cookies sin el atributo Secure (39% de las empresas, frente al 30% del conjunto).

En los últimos 12 meses, el score medio subió 1,0 puntos, de 73,5 a 74,5. En la exposición crítica, el 41% de las empresas tiene una CVE del catálogo KEV (media general: 52%) y el 22% tiene una CVE KEV asociada a ransomware (media general: 24%).

País: Chile

puesto 5 de 7 segmentos | 69 empresas analizadas

SCORE MEDIO	MEDIANA	POR DEBAJO DE 70	VAR. 12M
73,9	77,0	38%	-1,2
nota C	Q1-Q3: 58-86	general 37%	puntos de score



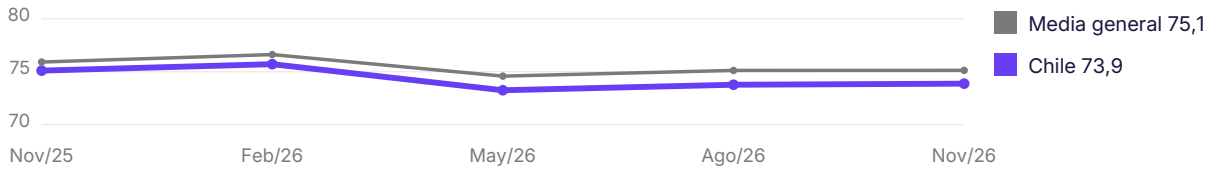
Score por factor (segmento vs general)



Problemas más comunes (% de empresas afectadas)



Evolución del score medio



Análisis

Chile ocupa el puesto 5 entre 7 segmentos, con un score medio de 73,9, que es 1,3 puntos inferior a la media general de 75,1. De sus empresas, el 46% tiene nota A o B y el 38% queda por debajo de 70. Tras ajustar por la mezcla de industrias, el efecto país es de -0,7 puntos: el país tiene un desempeño inferior al esperado para su composición sectorial. Entre las industrias con 5 o más empresas en el país, la mejor es Servicios financieros y seguros (89, 10 empresas) y la peor, Alimentos y bebidas (65, 10 empresas).

Frente al conjunto, el factor más fuerte es salud del DNS (+4,4) y el más débil es seguridad de red (-1,2). El problema más por encima de la media general es cifrados TLS débiles (65% de las empresas, frente al 65% del conjunto).

En los últimos 12 meses, el score medio cayó 1,2 puntos, de 75,1 a 73,9. En la exposición crítica, el 55% de las empresas tiene una CVE del catálogo KEV (media general: 52%) y el 19% tiene una CVE KEV asociada a ransomware (media general: 24%).

País: Argentina

puesto 6 de 7 segmentos | 39 empresas analizadas

SCORE MEDIO	MEDIANA	POR DEBAJO DE 70	VAR. 12M
72,8	77,0	44%	+0,7
nota C	Q1-Q3: 58-90	general 37%	puntos de score

Notas: 11 | 7 | 4 | 6 | 11

A 90-100 B 80-89 C 70-79 D 60-69 F < 60

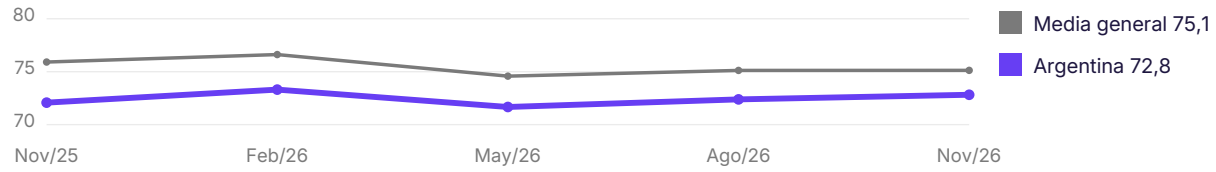
Score por factor (segmento vs general)

Red	76,7 (general 77,2)
Aplicaciones	80,2 (general 82,6)
Patching	81,3 (general 81,0)
Info. expuesta	92,5 (general 93,5)
DNS	90,7 (general 91,6)
Endpoints	93,2 (general 96,0)

Problemas más comunes (% de empresas afectadas)

Scripts de terceros sin SRI	59% (general 68%)
Protocolos TLS débiles u obsoletos	64% (general 65%)
Cifrados TLS débiles	56% (general 65%)
Certificados caducados	56% (general 61%)
Política CSP insegura	51% (general 57%)

Evolución del score medio



Análisis

Argentina ocupa el puesto 6 entre 7 segmentos, con un score medio de 72,8, que es 2,3 puntos inferior a la media general de 75,1. De sus empresas, el 46% tiene nota A o B y el 44% queda por debajo de 70. Tras ajustar por la mezcla de industrias, el efecto país es de -2,2 puntos: el país tiene un desempeño inferior al esperado para su composición sectorial. Entre las industrias con 5 o más empresas en el país, la mejor es Energía y servicios públicos (78, 11 empresas) y la peor, Tecnología y servicios de información (70, 6 empresas).

Frente al conjunto, el factor más fuerte es cadencia de parcheo (+0,3) y el más débil es seguridad de endpoints (-2,8). El problema más por encima de la media general es cookies sin HttpOnly (21% de las empresas, frente al 15% del conjunto).

En los últimos 12 meses, el score medio subió 0,7 puntos, de 72,1 a 72,8. En la exposición crítica, el 51% de las empresas tiene una CVE del catálogo KEV (media general: 52%) y el 26% tiene una CVE KEV asociada a ransomware (media general: 24%).

País: México

puesto 7 de 7 segmentos | 93 empresas analizadas

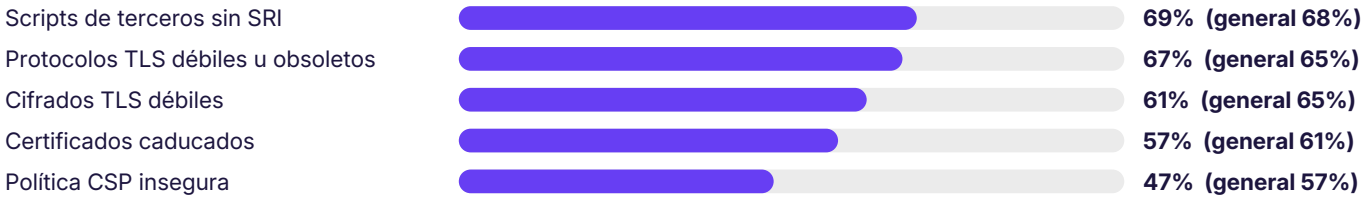
SCORE MEDIO	MEDIANA	POR DEBAJO DE 70	VAR. 12M
72,1	71,0	49%	-2,8
nota C	Q1-Q3: 58-87	general 37%	puntos de score



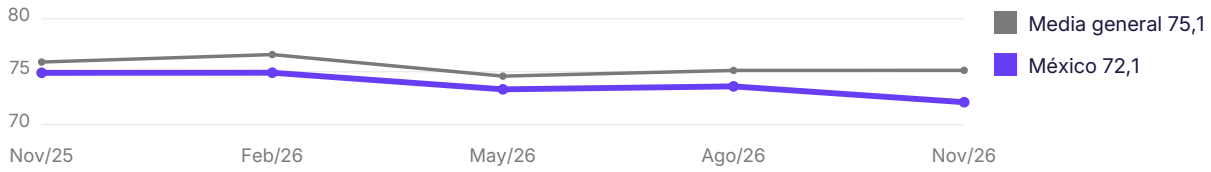
Score por factor (segmento vs general)



Problemas más comunes (% de empresas afectadas)



Evolución del score medio



Análisis

México ocupa el puesto 7 entre 7 segmentos, con un score medio de 72,1, que es 3,0 puntos inferior a la media general de 75,1. De sus empresas, el 42% tiene nota A o B y el 49% queda por debajo de 70. Tras ajustar por la mezcla de industrias, el efecto país es de -2,3 puntos: el país tiene un desempeño inferior al esperado para su composición sectorial. Entre las industrias con 5 o más empresas en el país, la mejor es Otras industrias (76, 9 empresas) y la peor, Construcción (67, 6 empresas).

Frente al conjunto, el factor más fuerte es información expuesta (+2,2) y el más débil es seguridad de red (-3,3). El problema más por encima de la media general es protocolos TLS débiles u obsoletos (67% de las empresas, frente al 65% del conjunto).

En los últimos 12 meses, el score medio cayó 2,8 puntos, de 74,9 a 72,1. En la exposición crítica, el 52% de las empresas tiene una CVE del catálogo KEV (media general: 52%) y el 28% tiene una CVE KEV asociada a ransomware (media general: 24%).

Industria: Minería y metales

puesto 1 de 12 segmentos | 10 empresas analizadas

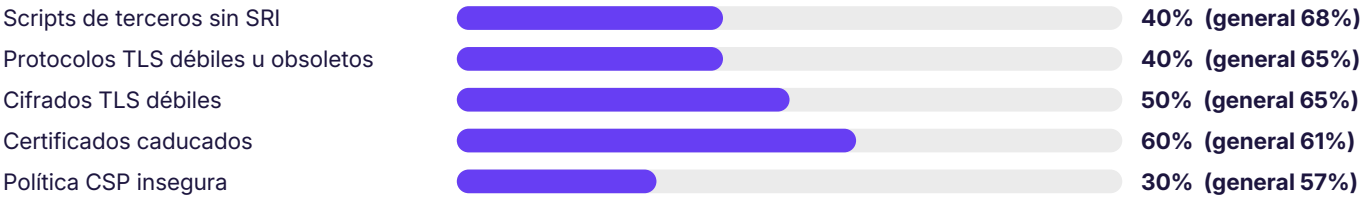
SCORE MEDIO	MEDIANA	POR DEBAJO DE 70	VAR. 12M
81,7	82,5	10%	-0,6
nota B	Q1-Q3: 74-88	general 37%	puntos de score



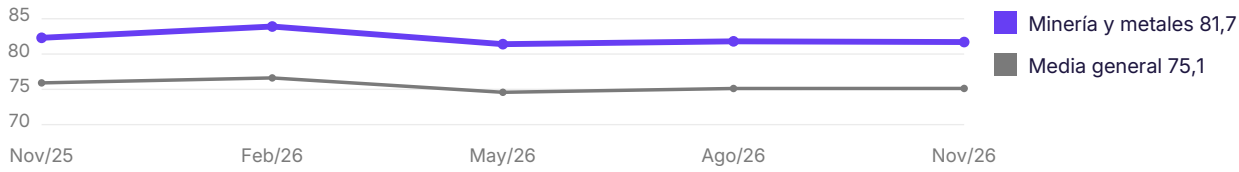
Score por factor (segmento vs general)



Problemas más comunes (% de empresas afectadas)



Evolución del score medio



Análisis

Minería y metales ocupa el primer puesto entre 12 segmentos, con un score medio de 81,7, que es 6,6 puntos superior a la media general de 75,1. De sus empresas, el 60% tiene nota A o B y el 10% queda por debajo de 70. Tras ajustar por la mezcla de países, el efecto industria es de +7,6 puntos: la industria tiene un desempeño superior al esperado para su distribución geográfica.

Frente al conjunto, el factor más fuerte es cadencia de parcheo (+10,4) y el más débil es seguridad de red (+3,5). Ninguno de los problemas más comunes ocurre por encima de la media general.

En los últimos 12 meses, el score medio cayó 0,6 puntos, de 82,3 a 81,7. En la exposición crítica, el 30% de las empresas tiene una CVE del catálogo KEV (media general: 52%) y ninguna tiene una CVE asociada a ransomware (media general: 24%).

Industria: Servicios financieros y seguros

puesto 2 de 12 segmentos | 110 empresas analizadas

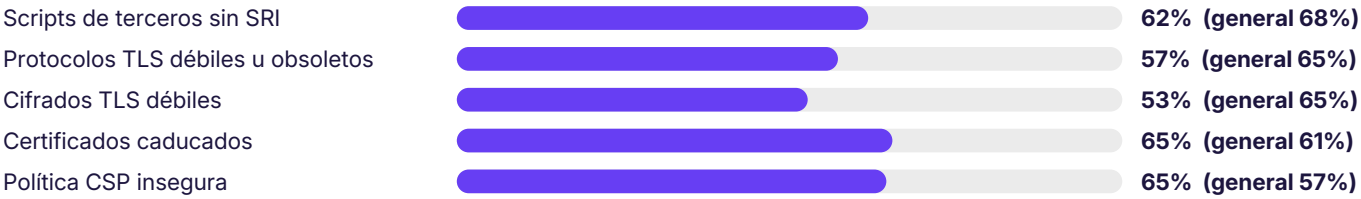
SCORE MEDIO	MEDIANA	POR DEBAJO DE 70	VAR. 12M
80,1	83,5	25%	-0,2
nota B	Q1-Q3: 70-92	general 37%	puntos de score



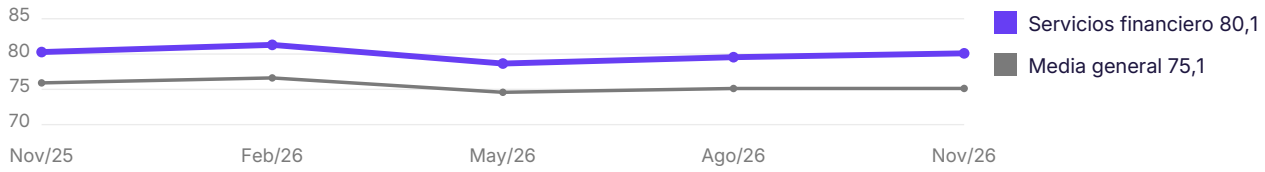
Score por factor (segmento vs general)



Problemas más comunes (% de empresas afectadas)



Evolución del score medio



Análisis

Servicios financieros y seguros ocupa el puesto 2 entre 12 segmentos, con un score medio de 80,1, que es 5,0 puntos superior a la media general de 75,1. De sus empresas, el 63% tiene nota A o B y el 25% queda por debajo de 70. Tras ajustar por la mezcla de países, el efecto industria es de +4,2 puntos: la industria tiene un desempeño superior al esperado para su distribución geográfica. Entre los países con 5 o más empresas en esta industria, el mejor es Colombia (89, 13 empresas) y el peor, Argentina (73, 6 empresas).

Frente al conjunto, el factor más fuerte es seguridad de red (+4,8) y el más débil es información expuesta (-2,3). El problema más por encima de la media general es política CSP insegura (65% de las empresas, frente al 57% del conjunto).

En los últimos 12 meses, el score medio cayó 0,2 puntos, de 80,3 a 80,1. En la exposición crítica, el 48% de las empresas tiene una CVE del catálogo KEV (media general: 52%) y el 21% tiene una CVE KEV asociada a ransomware (media general: 24%).

Industria: Transporte y logística

puesto 3 de 12 segmentos | 31 empresas analizadas

SCORE MEDIO	MEDIANA	POR DEBAJO DE 70	VAR. 12M
79,0	83,0	26%	+1,4
nota C	Q1-Q3: 70-90	general 37%	puntos de score

Notas: 8 | 9 | 6 | 5 | 3

A 90-100 B 80-89 C 70-79 D 60-69 F < 60

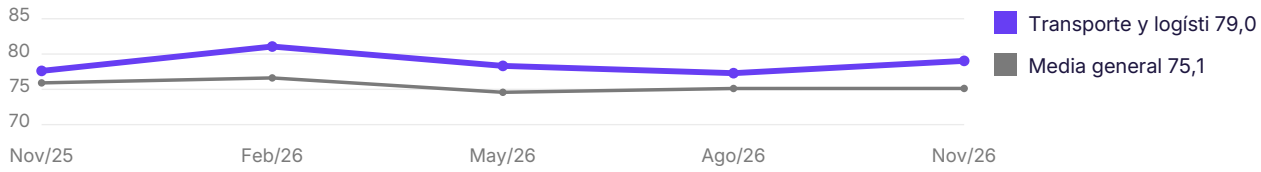
Score por factor (segmento vs general)

Red	79,0 (general 77,2)
Aplicaciones	86,3 (general 82,6)
Patching	84,9 (general 81,0)
Info. expuesta	93,5 (general 93,5)
DNS	96,2 (general 91,6)
Endpoints	98,5 (general 96,0)

Problemas más comunes (% de empresas afectadas)

Scripts de terceros sin SRI	71% (general 68%)
Protocolos TLS débiles u obsoletos	61% (general 65%)
Cifrados TLS débiles	71% (general 65%)
Certificados caducados	61% (general 61%)
Política CSP insegura	71% (general 57%)

Evolución del score medio



Análisis

Transporte y logística ocupa el puesto 3 entre 12 segmentos, con un score medio de 79,0, que es 3,9 puntos superior a la media general de 75,1. De sus empresas, el 55% tiene nota A o B y el 26% queda por debajo de 70. Tras ajustar por la mezcla de países, el efecto industria es de +4,0 puntos: la industria tiene un desempeño superior al esperado para su distribución geográfica. Entre los países con 5 o más empresas en esta industria, el mejor es Brasil (81, 16 empresas) y el peor, México (75, 9 empresas).

Frente al conjunto, el factor más fuerte es salud del DNS (+4,6) y el más débil es información expuesta (+0,0). El problema más por encima de la media general es política CSP insegura (71% de las empresas, frente al 57% del conjunto).

En los últimos 12 meses, el score medio subió 1,4 puntos, de 77,6 a 79,0. En la exposición crítica, el 52% de las empresas tiene una CVE del catálogo KEV (media general: 52%) y el 13% tiene una CVE KEV asociada a ransomware (media general: 24%).

Industria: Salud y farmacéutica

puesto 4 de 12 segmentos | 13 empresas analizadas

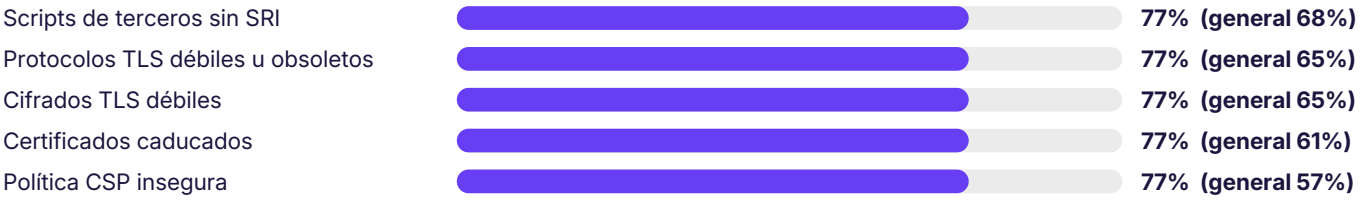
SCORE MEDIO	MEDIANA	POR DEBAJO DE 70	VAR. 12M
76,7	74,0	31%	+4,2
nota C	Q1-Q3: 68-93	general 37%	puntos de score



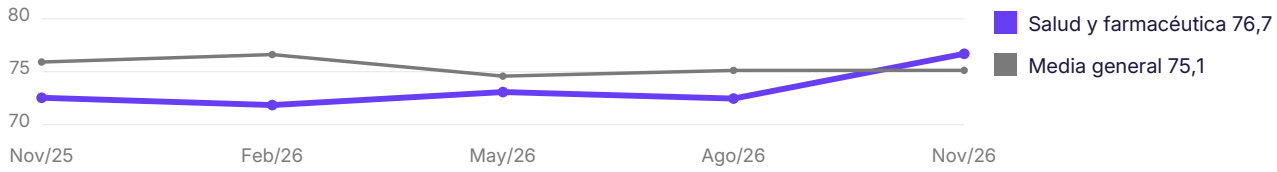
Score por factor (segmento vs general)



Problemas más comunes (% de empresas afectadas)



Evolución del score medio



Análisis

Salud y farmacéutica ocupa el puesto 4 entre 12 segmentos, con un score medio de 76,7, que es 1,6 puntos superior a la media general de 75,1. De sus empresas, el 38% tiene nota A o B y el 31% queda por debajo de 70. Tras ajustar por la mezcla de países, el efecto industria es de +0,7 puntos: la industria tiene un desempeño superior al esperado para su distribución geográfica.

Frente al conjunto, el factor más fuerte es seguridad de aplicaciones (+0,8) y el más débil es salud del DNS (-3,8). El problema más por encima de la media general es política CSP insegura (77% de las empresas, frente al 57% del conjunto).

En los últimos 12 meses, el score medio subió 4,2 puntos, de 72,5 a 76,7. En la exposición crítica, el 62% de las empresas tiene una CVE del catálogo KEV (media general: 52%) y el 54% tiene una CVE KEV asociada a ransomware (media general: 24%).

Industria: Energía y servicios públicos

puesto 5 de 12 segmentos | 68 empresas analizadas

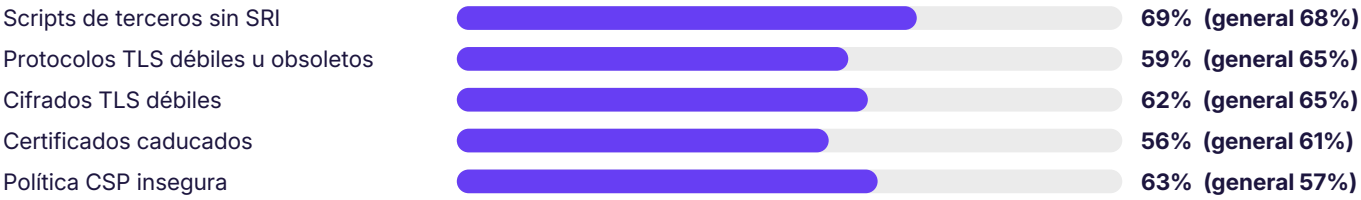
SCORE MEDIO	MEDIANA	POR DEBAJO DE 70	VAR. 12M
76,1	79,5	31%	-2,2
nota C	Q1-Q3: 63-89	general 37%	puntos de score



Score por factor (segmento vs general)



Problemas más comunes (% de empresas afectadas)



Evolución del score medio



Análisis

Energía y servicios públicos ocupa el puesto 5 entre 12 segmentos, con un score medio de 76,1, que es 1,0 puntos superior a la media general de 75,1. De sus empresas, el 50% tiene nota A o B y el 31% queda por debajo de 70. Tras ajustar por la mezcla de países, el efecto industria es de +0,8 puntos: la industria tiene un desempeño superior al esperado para su distribución geográfica. Entre los países con 5 o más empresas en esta industria, el mejor es Brasil (79, 33 empresas) y el peor, Perú (60, 5 empresas).

Frente al conjunto, el factor más fuerte es seguridad de red (+1,9) y el más débil es cadencia de parcheo (-2,1). El problema más por encima de la media general es política CSP insegura (63% de las empresas, frente al 57% del conjunto).

En los últimos 12 meses, el score medio cayó 2,2 puntos, de 78,4 a 76,1. En la exposición crítica, el 56% de las empresas tiene una CVE del catálogo KEV (media general: 52%) y el 31% tiene una CVE KEV asociada a ransomware (media general: 24%).

Industria: Tecnología y servicios de información

puesto 6 de 12 segmentos | 45 empresas analizadas

SCORE MEDIO	MEDIANA	POR DEBAJO DE 70	VAR. 12M
75,9	80,0	42%	-0,3
nota C	Q1-Q3: 67-90	general 37%	puntos de score



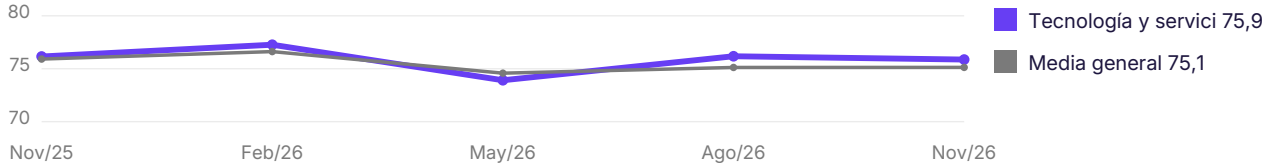
Score por factor (segmento vs general)



Problemas más comunes (% de empresas afectadas)



Evolución del score medio



Análisis

Tecnología y servicios de información ocupa el puesto 6 entre 12 segmentos, con un score medio de 75,9, que es 0,7 puntos superior a la media general de 75,1. De sus empresas, el 51% tiene nota A o B y el 42% queda por debajo de 70. Tras ajustar por la mezcla de países, el efecto industria es de +0,9 puntos: la industria tiene un desempeño superior al esperado para su distribución geográfica. Entre los países con 5 o más empresas en esta industria, el mejor es Chile (85, 7 empresas) y el peor, México (67, 7 empresas).

Frente al conjunto, el factor más fuerte es cadencia de parcheo (+5,0) y el más débil es seguridad de aplicaciones (-2,9). El problema más por encima de la media general es cookies sin el atributo Secure (42% de las empresas, frente al 30% del conjunto).

En los últimos 12 meses, el score medio cayó 0,3 puntos, de 76,2 a 75,9. En la exposición crítica, el 42% de las empresas tiene una CVE del catálogo KEV (media general: 52%) y el 16% tiene una CVE KEV asociada a ransomware (media general: 24%).

Industria: Manufactura e industria

puesto 7 de 12 segmentos | 68 empresas analizadas

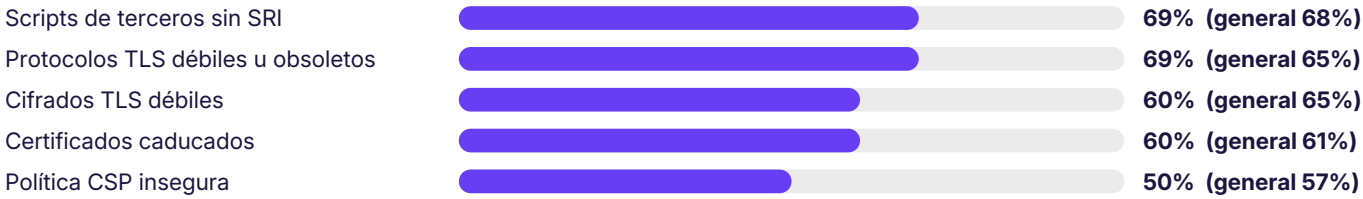
SCORE MEDIO	MEDIANA	POR DEBAJO DE 70	VAR. 12M
73,0	76,5	40%	-1,8
nota C	Q1-Q3: 58-88	general 37%	puntos de score



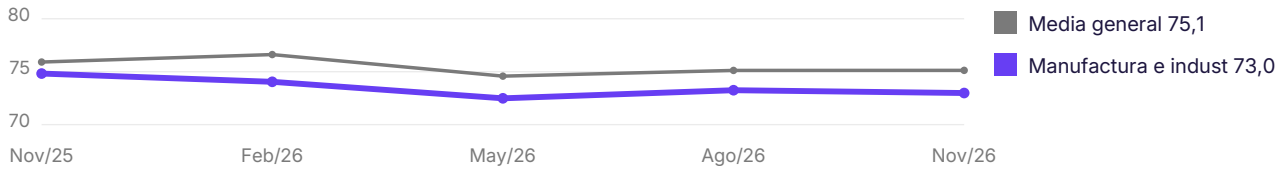
Score por factor (segmento vs general)



Problemas más comunes (% de empresas afectadas)



Evolución del score medio



Análisis

Manufactura e industria ocupa el puesto 7 entre 12 segmentos, con un score medio de 73,0, que es 2,1 puntos inferior a la media general de 75,1. De sus empresas, el 40% tiene nota A o B y el 40% queda por debajo de 70. Tras ajustar por la mezcla de países, el efecto industria es de -1,8 puntos: la industria tiene un desempeño inferior al esperado para su distribución geográfica. Entre los países con 5 o más empresas en esta industria, el mejor es Brasil (75, 31 empresas) y el peor, Chile (66, 9 empresas).

Frente al conjunto, el factor más fuerte es información expuesta (+5,3) y el más débil es seguridad de red (-1,7). El problema más por encima de la media general es protocolos TLS débiles u obsoletos (69% de las empresas, frente al 65% del conjunto).

En los últimos 12 meses, el score medio cayó 1,8 puntos, de 74,8 a 73,0. En la exposición crítica, el 50% de las empresas tiene una CVE del catálogo KEV (media general: 52%) y el 26% tiene una CVE KEV asociada a ransomware (media general: 24%).

Industria: Comercio minorista

puesto 8 de 12 segmentos | 59 empresas analizadas

SCORE MEDIO	MEDIANA	POR DEBAJO DE 70	VAR. 12M
72,0	72,0	47%	-2,9
nota C	Q1-Q3: 58-86	general 37%	puntos de score

Notas: 12 | 12 | 7 | 10 | 18

A 90-100 B 80-89 C 70-79 D 60-69 F < 60

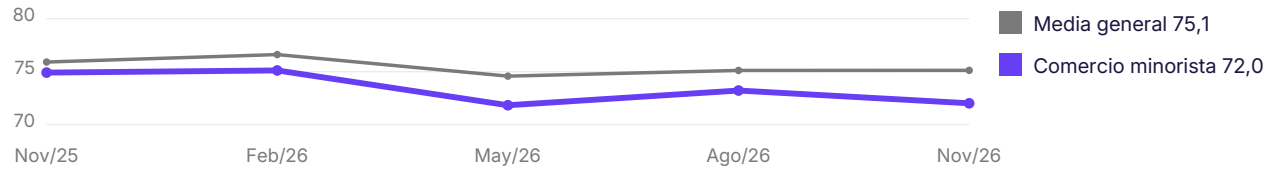
Score por factor (segmento vs general)

Red	73,9 (general 77,2)
Aplicaciones	80,1 (general 82,6)
Patching	77,3 (general 81,0)
Info. expuesta	92,3 (general 93,5)
DNS	90,6 (general 91,6)
Endpoints	97,6 (general 96,0)

Problemas más comunes (% de empresas afectadas)

Scripts de terceros sin SRI	71% (general 68%)
Protocolos TLS débiles u obsoletos	69% (general 65%)
Cifrados TLS débiles	75% (general 65%)
Certificados caducados	68% (general 61%)
Política CSP insegura	54% (general 57%)

Evolución del score medio



Análisis

Comercio minorista ocupa el puesto 8 entre 12 segmentos, con un score medio de 72,0, que es 3,1 puntos inferior a la media general de 75,1. De sus empresas, el 41% tiene nota A o B y el 47% queda por debajo de 70. Tras ajustar por la mezcla de países, el efecto industria es de -2,7 puntos: la industria tiene un desempeño inferior al esperado para su distribución geográfica. Entre los países con 5 o más empresas en esta industria, el mejor es Brasil (73, 24 empresas) y el peor, México (67, 14 empresas).

Frente al conjunto, el factor más fuerte es seguridad de endpoints (+1,5) y el más débil es cadencia de parcheo (-3,8). El problema más por encima de la media general es cifrados TLS débiles (75% de las empresas, frente al 65% del conjunto).

En los últimos 12 meses, el score medio cayó 2,9 puntos, de 74,9 a 72,0. En la exposición crítica, el 54% de las empresas tiene una CVE del catálogo KEV (media general: 52%) y el 24% tiene una CVE KEV asociada a ransomware (media general: 24%).

Industria: Alimentos y bebidas

puesto 9 de 12 segmentos | 35 empresas analizadas

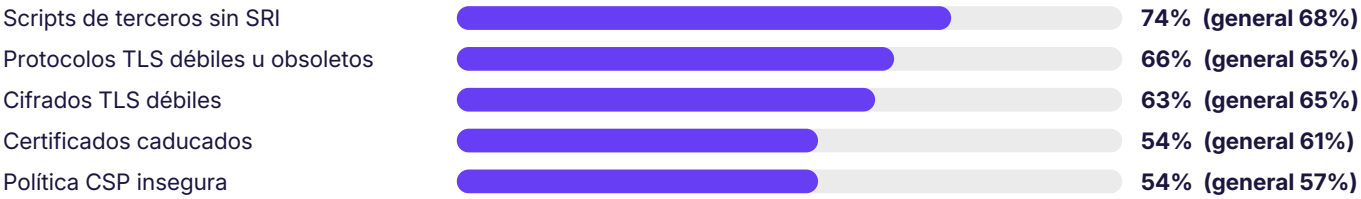
SCORE MEDIO	MEDIANA	POR DEBAJO DE 70	VAR. 12M
71,1	72,0	46%	+0,8
nota C	Q1-Q3: 56-84	general 37%	puntos de score



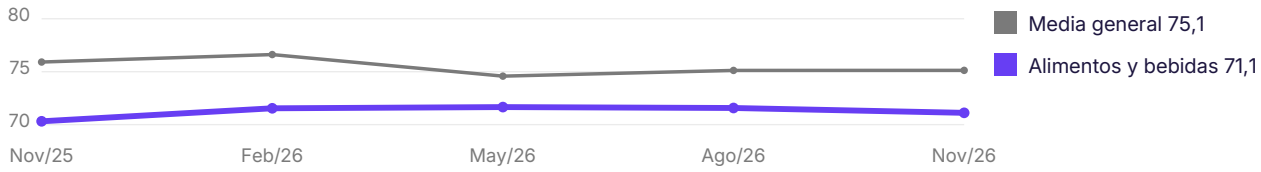
Score por factor (segmento vs general)



Problemas más comunes (% de empresas afectadas)



Evolución del score medio



Análisis

Alimentos y bebidas ocupa el puesto 9 entre 12 segmentos, con un score medio de 71,1, que es 4,0 puntos inferior a la media general de 75,1. De sus empresas, el 40% tiene nota A o B y el 46% queda por debajo de 70. Tras ajustar por la mezcla de países, el efecto industria es de -4,0 puntos: la industria tiene un desempeño inferior al esperado para su distribución geográfica. Entre los países con 5 o más empresas en esta industria, el mejor es Brasil (74, 8 empresas) y el peor, Chile (65, 10 empresas).

Frente al conjunto, el factor más fuerte es información expuesta (+2,4) y el más débil es cadencia de parcheo (-4,2). El problema más por encima de la media general es scripts de terceros sin SRI (74% de las empresas, frente al 68% del conjunto).

En los últimos 12 meses, el score medio subió 0,8 puntos, de 70,3 a 71,1. En la exposición crítica, el 57% de las empresas tiene una CVE del catálogo KEV (media general: 52%) y el 17% tiene una CVE KEV asociada a ransomware (media general: 24%).

Industria: Construcción

puesto 11 de 12 segmentos | 22 empresas analizadas

SCORE MEDIO	MEDIANA	POR DEBAJO DE 70	VAR. 12M
68,4	67,0	59%	-3,4
nota D	Q1-Q3: 55-80	general 37%	puntos de score

Notas: 3 | 3 | 3 | 6 | 7

A 90-100 | B 80-89 | C 70-79 | D 60-69 | F < 60

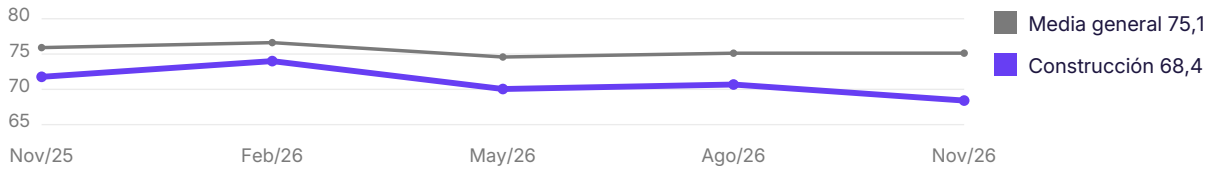
Score por factor (segmento vs general)



Problemas más comunes (% de empresas afectadas)



Evolución del score medio



Análisis

Construcción ocupa el puesto 11 entre 12 segmentos, con un score medio de 68,4, que es 6,7 puntos inferior a la media general de 75,1. De sus empresas, el 27% tiene nota A o B y el 59% queda por debajo de 70. Tras ajustar por la mezcla de países, el efecto industria es de -6,1 puntos: la industria tiene un desempeño inferior al esperado para su distribución geográfica. Entre los países con 5 o más empresas en esta industria, el mejor es Brasil (75, 6 empresas) y el peor, México (67, 6 empresas).

Frente al conjunto, el factor más fuerte es salud del DNS (+4,3) y el más débil es seguridad de red (-7,5). El problema más por encima de la media general es cifrados TLS débiles (82% de las empresas, frente al 65% del conjunto).

En los últimos 12 meses, el score medio cayó 3,4 puntos, de 71,8 a 68,4. En la exposición crítica, el 50% de las empresas tiene una CVE del catálogo KEV (media general: 52%) y el 18% tiene una CVE KEV asociada a ransomware (media general: 24%).

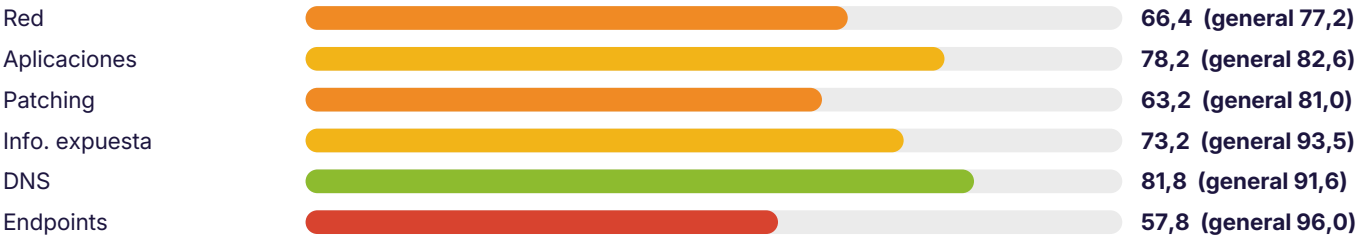
Industria: Telecomunicaciones

puesto 12 de 12 segmentos | 13 empresas analizadas

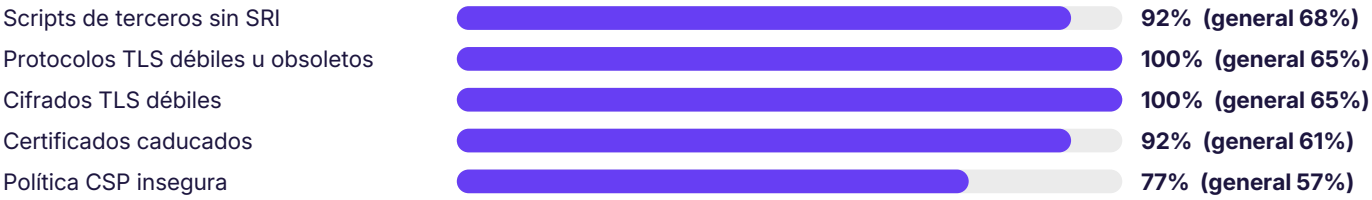
SCORE MEDIO	MEDIANA	POR DEBAJO DE 70	VAR. 12M
65,5	71,0	38%	+3,7
nota D	Q1-Q3: 57-74	general 37%	puntos de score



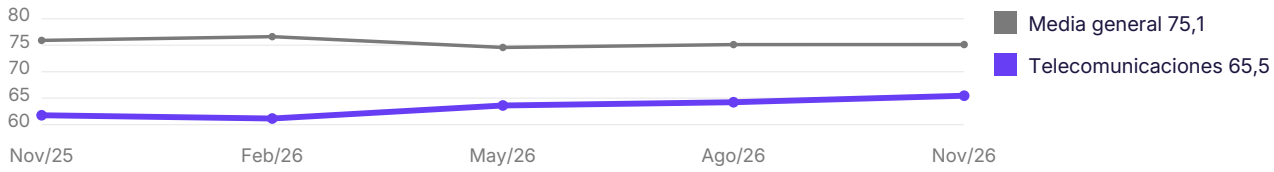
Score por factor (segmento vs general)



Problemas más comunes (% de empresas afectadas)



Evolución del score medio



Análisis

Telecomunicaciones ocupa el puesto 12 entre 12 segmentos, con un score medio de 65,5, que es 9,7 puntos inferior a la media general de 75,1. De sus empresas, el 8% tiene nota A o B y el 38% queda por debajo de 70. Tras ajustar por la mezcla de países, el efecto industria es de -8,3 puntos: la industria tiene un desempeño inferior al esperado para su distribución geográfica.

Frente al conjunto, el factor más fuerte es seguridad de aplicaciones (-4,4) y el más débil es seguridad de endpoints (-38,2). El problema más por encima de la media general es cookies sin el atributo Secure (85% de las empresas, frente al 30% del conjunto).

En los últimos 12 meses, el score medio subió 3,7 puntos, de 61,8 a 65,5. En la exposición crítica, el 100% de las empresas tiene una CVE del catálogo KEV (media general: 52%) y el 92% tiene una CVE KEV asociada a ransomware (media general: 24%).

Metodología y notas

Cómo se calcularon las cifras

- **Muestra:** 500 empresas del portfolio «LATAM 500» de SecurityScorecard, que reúne a las mayores empresas de América Latina.
- **Score:** los scores de SecurityScorecard van de 0 a 100 y se asocian a notas con letra así: A (90 a 100), B (80 a 89), C (70 a 79), D (60 a 69) y F (por debajo de 60). La media por segmento es la media simple de los scores de sus empresas, con mediana, cuartiles, mínimo y máximo. Tamaño: campo de empleados de la plataforma, informado para el 44% de la muestra.
- **Efecto de composición:** diferencia entre la media observada de un segmento y la esperada si cada empresa tuviera el score medio regional de su industria (efecto país) o de su país (efecto industria). La matriz país × industria muestra solo celdas con 5 o más empresas.
- **Prevalencia de problemas y CVE:** porcentaje de empresas con al menos una ocurrencia en los factores de la plataforma, cruzado con el catálogo KEV de la CISA (actualizado el 06/11/2026) y con el EPSS. Las versiones de software se infieren a partir de señales externas y pueden incluir falsos positivos por backports.
- **Tendencia:** evolución del score medio de las mismas empresas en los últimos 12 meses (histórico diario de la plataforma, del 08/11/2025 al 07/11/2026), considerando solo las que tienen historial completo.
- **Driftnet:** IP atribuidas a las empresas por el nombre de la entidad en el registro de IP (nombre igual a la marca, más sufijos societarios) y filtradas por país cuando se conoce; se excluyeron las empresas con espacio de direcciones de escala de proveedor. Cubre solo empresas con infraestructura propia identificable. El TLS lo evalúa solo SecurityScorecard: Driftnet registra la versión negociada, que no revela el soporte de versiones antiguas.
- **Colores de las tablas:** franjas fijas, del verde (mejor) al rojo (peor). En los scores coinciden con las notas A a F; en los porcentajes de exposición, verde hasta el 10%, verde claro hasta el 25%, amarillo hasta el 40%, naranja hasta el 60% y el rojo está por encima del 60%.
- **Limitaciones:** SecurityScorecard mide la exposición visible de fuera hacia dentro y no sustituye a una auditoría interna. Solo hay valores agregados; no se identifica a ninguna empresa.

Fuentes externas

- IBM, Cost of a Data Breach Report 2026; IBM X-Force Threat Intelligence Index 2025.
- Verizon, 2026 Data Breach Investigations Report.
- Kaspersky ICS CERT (julio de 2026) y Kaspersky (julio de 2026, vía EFE).
- Intel 471, panorama de amenazas cibernéticas en América Latina 2026.
- CISA, Known Exploited Vulnerabilities Catalog; FIRST/Empirical Security, EPSS.

Acerca de SecurityScorecard

SecurityScorecard es el líder mundial en gestión de riesgos de terceros (TPRM) basada en inteligencia de amenazas y protege las cadenas de suministro del mundo. La empresa ofrece un enfoque de TPRM basado en inteligencia de amenazas que permite a las organizaciones eliminar el riesgo en su origen. La plataforma utiliza visibilidad continua y flujos de trabajo acelerados por IA para ayudar a las organizaciones a reducir el riesgo de terceros antes de que se produzcan incidentes y a responder con confianza cuando ocurren.

Con la confianza de 3.000 organizaciones, entre ellas más del 70% de las Fortune 100, y reconocida como un recurso de confianza por la Agencia de Ciberseguridad y Seguridad de las Infraestructuras de EE. UU. (CISA). Respaldada por Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, Google Ventures y Riverwood Capital, SecurityScorecard ofrece ciberseguridad de la cadena de suministro de extremo a extremo que protege la continuidad del negocio.

Proteja la cadena de suministro que sustenta su negocio. Más información en securityscorecard.com.