Encuesta latinoamericana de seguridad de la información 2026.

Resultados y revelaciones estratégicas

DOI: 10.29236/sistemas.n179a4

Jeimy J. Cano M.

Andrés R. Almanza J.

Gabriela M. Saucedo M.

Resumen

El presente estudio analiza el estado de la seguridad de la información de 115 organizaciones participantes de Latinoamérica, con el objetivo de caracterizar el estado de su gobierno de ciberseguridad y de identificar las relaciones de mayor valor entre sector económico, capacidad presupuestal, exposición a incidentes y prioridades temáticas para 2026. Los resultados muestran que el 74.1% de las organizaciones dispone de rubro presupuestal para 2026, con una marcada asimetría sectorial: los sectores regulados presentan una probabilidad ocho veces mayor de contar con presupuesto. No obstante, la existencia de presupuesto se desacopla de su magnitud, y el costo de los incidentes se asocia más con la exposición sectorial y el tamaño organizacional, que con el nivel de inversión. La agenda 2026 está dominada por la inteligencia artificial, la fuga de información y las amenazas persistentes avanzadas.

Palabras clave

Seguridad de la información, ciberseguridad, gobierno de seguridad, gestión de riesgos, madurez organizacional

Introducción

La transformación digital ha situado a la seguridad de la información en el centro de la gestión del riesgo empresarial. La creciente sofisticación de las amenazas, impulsada por tecnologías emergentes y por un entorno geopolítico inestable, ha ampliado la superficie de ataque de las organizaciones y ha tensionado su capacidad de respuesta.

En este contexto, anticipar las amenazas cibernéticas dejó de ser una función exclusivamente técnica para convertirse en una decisión estratégica que compromete a la alta dirección, al presupuesto y a la cultura organizacional.

A pesar de la abundante evidencia internacional sobre costos de las brechas y tendencias de amenazas, persiste un vacío en la comprensión de cómo se distribuyen, a escala sectorial, las capacidades de gobierno, inversión y prevención dentro de un mismo ecosistema regional. Comprender estas asimetrías es indispensable para diseñar intervenciones que eleven la resiliencia cibernética colectiva.

Este estudio aborda dicho vacío mediante el análisis de los datos de la Encuesta Latinoamericana de Seguridad de la Información 2026 (ELSI 2026). El estudio prioriza, por su valor accionable, los cruces entre sector económico, capacidad presupuestal, costo de los incidentes y temas clave para 2026.

Metodología

Diseño y muestra

Se empleó un diseño cuantitativo, observacional y de corte transversal. La muestra estuvo conformada por 115 respuestas válidas obtenidas mediante un cuestionario autoadministrado de 22 ítems, distribuido entre responsables y profesionales de seguridad de la información de organizaciones de diversos sectores en Latinoamérica. El muestreo fue no probabilístico por autoselección, condición que delimita el alcance inferencial de los hallazgos a la población participante.

Técnicas estadísticas

El análisis descriptivo empleó distribuciones de frecuencia y, para las variables de respuesta múltiple, conjuntos de respuesta múltiple expresados como porcentaje de casos. Para las asociaciones nominales se utilizó la prueba chi-cuadrado de independencia de Pearson, acompañada del tamaño del efecto V de Cramér; cuando las frecuencias esperadas fueron reducidas se recurrió a la prueba exacta de Fisher. Las asociaciones entre variables ordinales se evaluaron con el coeficiente tau-b de Kendall, y la presencia de tendencias monótonas de prevalencia a través de niveles ordinales de presupuesto se contrastó con la prueba de Cochran-Armitage (Agresti, 2019). El procesamiento se realizó con el apoyo de inteligencia artificial gene-

rativa avanzada, validando cada una de sus respuestas contra los datos originales.

A continuación se detallan las técnicas estadísticas aplicadas: (Agresti, 2019).

- *Prueba chi-cuadrado de independencia de Pearson*: Compara las frecuencias observadas en cada celda de la tabla con las frecuencias que se esperarían si las variables fueran totalmente independientes. Un valor de X^2 elevado, con un p-valor pequeño, sugiere que la asociación observada es poco probable que ocurra por puro azar.

- *Prueba exacta de Fisher*: Es una prueba de independencia diseñada específicamente para tablas de contingencia (originalmente de 2×2) que no depende de aproximaciones para muestras grandes. Es la opción preferida cuando el tamaño de la muestra es pequeño o cuando los datos están muy desequilibrados.

- *Prueba de Cochran-Armitage*: En lugar de buscar cualquier tipo de asociación, esta prueba detecta específicamente si existe una tendencia lineal (aumento o disminución) en la proporción de éxitos a medida que aumenta el nivel de la variable ordinal.

- *Coeficiente tau-b de Kendall*: Evalúa la fuerza y la dirección de la asociación basándose en la concordancia y discordancia de los pares de observaciones.

- *Efecto V de Cramér*: Mientras que la prueba Chi-cuadrado solo indica si hay una asociación significativa (p-valor), la V de Cramér escala ese resultado entre 0 (independencia total) y 1 (asociación perfecta), permitiendo comparar la magnitud del efecto independientemente del tamaño de la muestra.

Resultados

Análisis descriptivo

La muestra refleja una fuerte presencia de los sectores de consultoría especializada, gobierno y servicios financieros, seguidos por educación (Figura 1). En conjunto, el 74.1% de las organizaciones declara contar con un rubro presupuestal para seguridad de la información en 2026, mientras que el 25.9% carece de él. El número medio de mecanismos de protección implementados es de 9.8. En el plano del gobierno, el 27% de las organizaciones no cuenta con un CISO y el 32% no realiza ejercicios de análisis de escenarios de riesgo, lo que evidencia una base de gestión todavía incipiente en una porción relevante de la muestra. Se destaca dentro de los resultados que 55 organizaciones reportan la gestión de incidentes a sus equipos ejecutivos o junta directiva, en tanto que 19 no presentan informe alguno.

Figura 1
Distribución de la muestra por sector económico

Nota. Frecuencia de organizaciones por sector tras la normalización de la variable (n = 115). Elaboración propia.

Análisis exploratorio: cruces de mayor valor

Sector y presupuesto. La existencia de rubro presupuestal varía significativamente entre grupos sectoriales (Tabla 1). La prueba chi-cuadrado resultó estadísticamente significativa ($\chi^2 = 11.137$; gl = 5; p = 0.0487) con un tamaño del efecto moderado (V de Cramér = 0.23). Dado que el 41.7% de las celdas presentó frecuencias esperadas inferiores a cinco, se complementó con una prueba exacta de Fisher sobre la dicotomía regulados frente a no regulados, que confirmó una asociación robusta: las organizaciones de sectores regulados (finanzas y gobierno) tienen una probabilidad cerca de ocho veces mayor de contar con presupuesto (OR = 8.3; p = 0.001).

Presupuesto, costo de incidentes y tamaño. La existencia de presupuesto se desacopla de su magnitud: sectores como gobierno presentan alta cobertura presupuestal, pero montos comparativamente bajos, mientras que manufactura y servicios financieros concentran los presupuestos totales más elevados. El costo de los incidentes, por su parte, no se asocia de forma significativa con el nivel de inversión (tau-b costo–presupuesto total = 0.204, p = 0.11), sino que sigue un

Tabla 1

Existencia de presupuesto de seguridad por grupo sectorial

Grupo sectorial	Sí	No	Total	% Sí
Consultoría	20	11	31	65%
Educación	7	5	12	58%
Finanzas	15	0	15	100%
Gobierno	17	2	19	89%
Otros	23	10	33	70%
Salud	4	2	6	67%

Nota. $\chi^2(5) = 11.137$, $p = 0.0487$, V de Cramér = 0.23. Prueba exacta de Fisher (regulados vs. no regulados): OR = 8.3, $p = 0.001$.

Nota. $\chi^2(5) = 11.137$, $p = 0.0487$, V de Cramér = 0.23. Prueba exacta de Fisher (regulados vs. no regulados): OR = 8.3, $p = 0.001$.

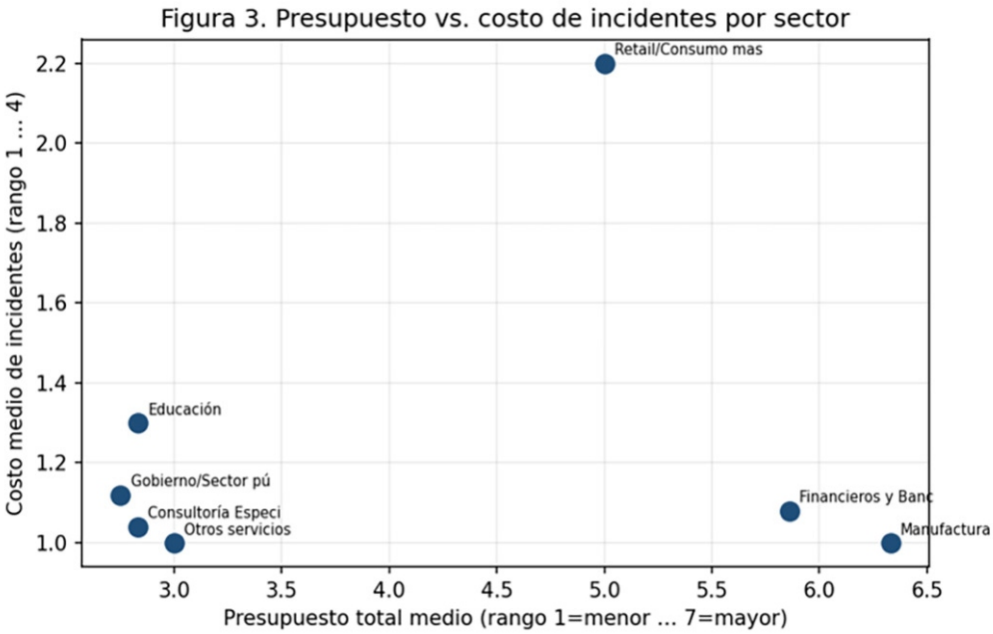
patrón de exposición sectorial: retail y telecomunicaciones reportan los costos medios más altos (Figura 2). El costo muestra además una tendencia ascendente con el tamaño organizacional (tau-b = 0.177, p = 0.0518), consistente con una mayor superficie de ataque y mayores activos en riesgo en las organizaciones grandes.

Sector, presupuesto y agenda 2026. La agenda temática para 2026 está dominada por la inteligencia artificial y las amenazas basadas en IA, seguidas por la fuga de información sensible y las amenazas persistentes avanzadas (Tabla 2 y Figura 3). El análisis de tendencia muestra matices según la capacidad presupuestal: las organizaciones con menor presupuesto enfatizan temas defensivos fundamentales, fuga de información e inteligencia de amenazas, mientras que las de mayor presupuesto incorporan con más frecuencia la protección de infraestructuras críticas y el internet de las cosas (Tabla 3).

Incidentes y obstáculos. Entre las organizaciones que experimentaron incidentes en 2025, predominan los originados en el factor humano: errores humanos (60.2%) y phishing (51.8%), seguidos de la ingeniería social (36.1%). De manera coherente, el obstáculo principal percibido para una adecuada postura de seguridad es la ausencia de una cultura de seguridad (44.7%), seguida por la falta de apoyo directivo (32.5%) y la complejidad tecnológica (30.7%). El factor humano y el gobierno, más que la tecnología, emergen como los determinantes críticos (Figura 5).

Figura 2

Relación entre presupuesto total medio y costo de incidentes por sector



Nota. Cada punto representa un sector; los ejes expresan rangos ordinales medios. La ausencia de una pendiente clara ilustra el desacople entre inversión y costo de incidentes. Elaboración propia.

Tabla 2

Temas clave priorizados para 2026 (diez principales)

Tema	n	% de casos
Inteligencia Artificial	88	76.5%
Amenazas basadas en IA	79	68.7%
Fuga de información sensible	78	67.8%
Amenazas persistentes avanzadas	70	60.9%
Ataques a infraestructuras críticas	64	55.7%
Seguridad y control en la computación en la nube	54	47%
Inteligencia de amenazas	53	46.1%
Talento Humano de Seguridad	45	39.1%
CyberRisk Quantification	44	38.3%
Ransomware de las Cosas	42	36.5%

Nota. Porcentaje calculado sobre las organizaciones que respondieron el ítem (base = 115). Pregunta de respuesta múltiple. Elaboración propia.

Nota. Porcentaje calculado sobre las organizaciones que respondieron el ítem (base = 115). Pregunta de respuesta múltiple. Elaboración propia.

Figura 3

Prevalencia de los temas clave priorizados para 2026

Nota. Porcentaje de organizaciones que seleccionó cada tema (respuesta múltiple). Elaboración propia.

Tabla 3

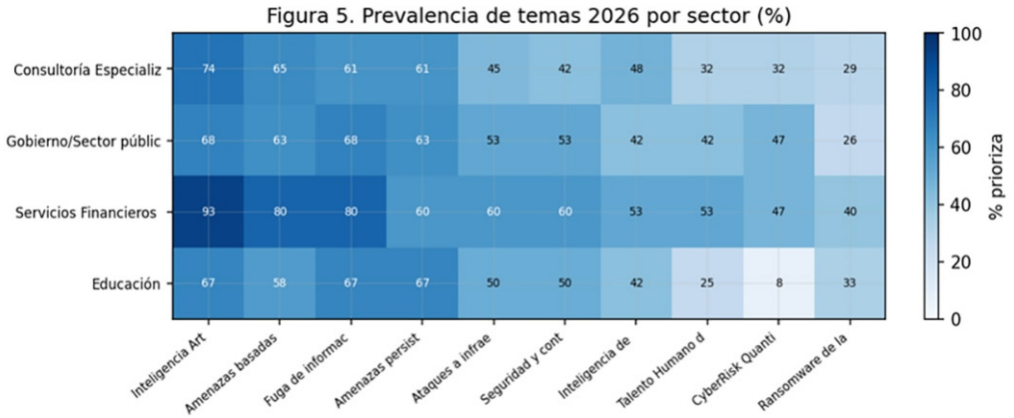
Tendencia de priorización temática según nivel de presupuesto

Tema	z	p	% PP bajo	% PP alto
Fuga de información sensible	-1.697	0.0897	80%	43%
Inteligencia de amenazas	-1.674	0.0941	70%	43%
Ataques a infraestructuras críticas	1.56	0.1187	45%	71%
Amenazas persistentes avanzadas	-1.536	0.1245	80%	57%
Internet de las cosas	1.351	0.1766	20%	43%
CyberRisk Quantification	1.219	0.2228	40%	71%

Nota. Prueba de tendencia de Cochran-Armitage. “% PP bajo” y “% PP alto” indican la prevalencia del tema en el nivel presupuestal más bajo y más alto, respectivamente. Ningún contraste alcanza $p < .05$. Elaboración propia.

Figura 4

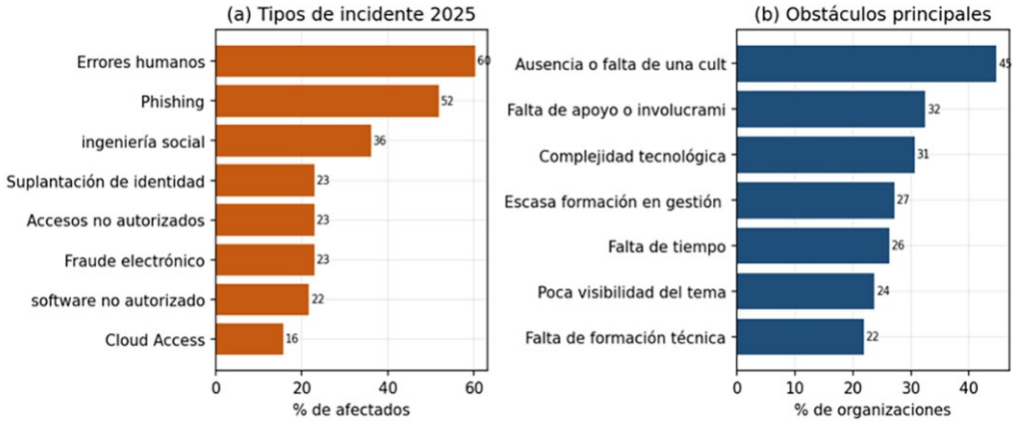
Prevalencia de temas 2026 por sector



Nota. Intensidad de color proporcional al porcentaje de organizaciones del sector que prioriza cada tema. Elaboración propia.

Figura 5

Tipos de incidente en 2025 y obstáculos percibidos



Nota. (a) Incidentes reportados por las organizaciones afectadas; (b) obstáculos principales percibidos. Respuestas múltiples. Elaboración propia.

Análisis de resultados

Convergencias. Los resultados convergen con la evidencia internacional más reciente en tres frentes. Primero, el protagonismo de la inteligencia artificial en la agenda 2026 coincide con el *Global Cybersecurity Outlook 2026*, en el que el 94% de los líderes encuestados identifica a la IA como el principal motor de cambio en ciberseguridad para el año y el 87% considera las vulnerabilidades asociadas a la IA como el riesgo de más rápido crecimiento (WEF, 2026). Esta convergencia se ve amplificada por Deloitte (2026), que pronostica que hasta el 75% de las empresas invertirá en IA agéntica hacia el cierre de 2026, intensificando el carácter dual de la IA como amenaza y como herramienta.

Segundo, el predominio del factor humano, errores humanos y phishing, como origen de los incidentes coincide con el *Cost of a Data Breach Report*, que atribuye al error humano una cuarta parte de las brechas y sitúa al phishing como vector inicial más frecuente (IBM, 2025).

Tercero, la fuerte asimetría presupuestal entre sectores regulados y no regulados refleja la inequidad cibernética descrita por el WEF (2026): mientras un 19% de las organizaciones ya supera los requisitos de resiliencia (frente al 9% del año anterior), las de menor tamaño tienen 2,5 veces más probabilidad de declarar una resiliencia insuficiente, profundizando una brecha estructural análoga a la observada entre los sectores regulados y no regulados.

Divergencias y matices. El estudio aporta matices que enriquecen la literatura. A diferencia de la narrativa habitual que vincula linealmente inversión y protección, los datos no evidencian un efecto protección significativo: el costo de los incidentes se explica mejor por la exposición sectorial y el tamaño que por el nivel de presupuesto. Esta divergencia, lejos de contradecir la importancia de invertir, sugiere que la eficacia depende de la calidad del gobierno y no solo del monto, en línea con el énfasis de NIST (2024) en la función Gobernar.

Asimismo, la posición rezagada del sector salud en madurez contrasta con su reconocido estatus como el sector de mayor costo de brecha a escala global (IBM, 2025), configurando un perfil de riesgo elevado que merece atención prioritaria. Finalmente, la baja conciencia directiva observada en parte de la muestra resuena con la divergencia de prioridades documentada por el WEF (2026), donde los directores ejecutivos ya sitúan el fraude habilitado por medios cibernéticos como su principal preocupación: el 73% reportó haber sido afectado por este fenómeno en 2025, mientras los CISO siguen centrados en el ransomware y la cadena de suministro.

Conclusiones

El estudio caracterizó la postura de seguridad de la información de 115 organizaciones y priorizó los cruces de mayor valor para la toma de decisiones. Tres conclusiones se destacan. Primera, la capacidad de gobierno y de inversión está distribuida de forma desigual: los sectores regulados lideran ampliamente la dotación presupuestal, lo que confirma una inequidad cibernética estructural. Segunda, el costo de los incidentes responde más a la exposición sectorial y al tamaño que al nivel de gasto, lo que desplaza el foco desde el cuánto se invierte hacia el cómo se gobierna la inversión. Tercera, la agenda 2026 está marcada por la inteligencia artificial y por amenazas que explotan el factor humano, lo que exige fortalecer simultáneamente la cultura, el gobierno y las capacidades analíticas en la gestión de riesgos.

Referencias

Agresti, A. (2019). *An introduction to categorical data analysis* (3rd ed.). Hoboken, NJ. USA: John Wiley & Sons.

Deloitte. (2026). *Technology, media & telecommunications predictions 2026: Narrowing the gap between the promise of AI and its reality.* Deloitte Center for Technology, Media & Telecommunications. https://www.deloitte.com/global/en/about/press-room/2026-tmt-predictions.html

International Business Machines Corporation (IBM). (2025). *Cost of a data breach report 2025.* IBM Security. https://www.ibm.com/reports/data-breach

National Institute of Standards and Technology (NIST). (2024). *The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29).* U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

World Economic Forum (WEF). (2026). *Global cybersecurity outlook 2026.* World Economic Forum. https://www.weforum.org/publications/global-cybersecurity-outlook-2026/

Jeimy J. Cano M., Ph.D, CFE, CICA. *Ingeniero y Magíster en Ingeniería de Sistemas y Computación, Universidad de los Andes. Especialista en Derecho Disciplinario, Universidad Externado de Colombia; Ph.D en Business Administration, Newport University, CA. USA. y Ph.D en Educación, Universidad Santo Tomás. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Internal Control Auditor (CICA) por The Institute of Internal Controls. Profesor Distinguido de la Facultad de Derecho, Universidad de los Andes. Es director de la Revista SISTEMAS de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.*

Andres R. Almanza J., Ms.C, CISM. *Chief Growth Officer en CISOS.CLUB, Investigador en Ciberseguridad SegInfo y Liderazgo. Executive Certificate in Cybersecurity Leadership & Strategy by FIU University. Certificado como ISO 27001 Lead Implementer and 27005 Lead Manager from PECB | CISM, ITILv3, LPI. Certificado como Coach Profesional Internacional, Master in Leadership and Organizational Development with Coaching, Executive Master's in Leadership Skills Developed in Harvard, & Coach Profesional avalado por International Coach Federation. Profesional en Ingeniería de Sistemas. Especialista en seguridad en redes y máster en seguridad de la información. Docente del programa de maestría de la Universidad Externado de Colombia y de la Universidad de las Américas en Ecuador. Creador de la Comunidad CISOS.CLUB, CISOS-COL y CISOS-LATAM (Linkedin) y Miembro del comité editorial de la revista sistemas de ACIS.*

Gabriela María Saucedo Meza, Ph.D. *Licenciado en Sistemas Computaciones y Maestría en Desarrollo Organizacional y Humano por la Universidad del Valle de Atemajac, México. Doctora en Educación por la Universidad Santo Tomás, Colombia. Certificada en Consultoría General por el Consejo Nacional de Normalización y Certificación de Competencia Laboral (CONOCER), México. Cuenta con más de 35 años de experiencia en gestión educativa, docencia e investigación en seguridad de la información, auditoría de TI, liderazgo educativo, cambio y cultura organizacional. Actualmente Coordinadora Académica de Posgrados de la Facultad de Contaduría Pública de la Universidad Externado de Colombia.*