Encuesta Latinoamericana de Seguridad (ELSI 2025)

Madurez de la ciberseguridad organizacional en América Latina

DOI: 10.29236/sistemas.n175a4

Resumen
Este artículo presenta los resultados del Estudio Latinoamericano sobre Seguridad de la Información (ELSI) 2025, basado en una encuesta aplicada a organizaciones de diversos sectores económicos en América Latina. El objetivo principal es analizar el nivel de madurez en ciberseguridad, evaluando variables clave como presupuesto, frecuencia y tipos de incidentes, mecanismos implementados, perfil del CISO, conciencia y participación de la alta dirección. A través de un enfoque exploratorio multivariable, se identifican patrones relevantes: una alta concentración de incidentes en sectores críticos, una brecha importante entre pequeñas y medianas empresas en capacidades de gestión, y una correlación positiva entre liderazgo consciente y mejores resultados en ciberseguridad. Los hallazgos se contrastan con estudios internacionales, aportando evidencia contextualizada para fortalecer la gobernanza y la resiliencia digital en la región. El estudio busca contribuir al desarrollo de estrategias de ciberseguridad más integradas y adaptativas para el contexto latinoamericano.

Palabras clave: ciberseguridad, madurez organizacional, alta dirección, América Latina, resiliencia digital.

Introducción

La ciberseguridad se ha convertido en un componente esencial de la resiliencia organizacional en la era digital. Los crecientes riesgos derivados de la hiperconectividad, la transformación digital acelerada y el sofisticado ecosistema de amenazas exigen que las organizaciones adopten estrategias integrales de protección, detección y respuesta.

Según el *World Economic Forum* (2025), el panorama de amenazas cibernéticas continúa evolucionando a gran velocidad, impulsado por el avance de tecnologías como la inteligencia artificial y el machine learning, que son utilizadas tanto por los defensores como por los atacantes. El informe destaca que ninguna organización, independientemente de su tamaño o sector, está exenta de riesgos cibernéticos. Por su parte, *ENISA* (2024) enfatiza la creciente importancia de los factores organizativos y culturales en la madurez cibernética, subrayando que la tecnología por sí sola no garantiza una postura de seguridad robusta.

Estudios como los de *ISACA* (2024) y *IBM* (2024) han evidenciado que, a pesar del incremento en las inversiones en ciberseguridad, muchas organizaciones siguen enfrentando incidentes significativos, lo que sugiere la necesidad de fortalecer aspectos como la gobernanza, la cultura de seguridad y la alineación estratégica.

En este contexto, la presente investigación busca aportar una visión actualizada sobre la madurez de la ciberseguridad organizacional en América Latina, a partir del análisis exploratorio de la encuesta ELSI 2025 (*datos propios*). Se examinan variables clave como el perfil del CISO, los presupuestos asignados, los incidentes sufridos, los mecanismos implementados, los principales obstáculos percibidos y las prioridades estratégicas para el próximo año.

Este artículo se basa en un análisis riguroso de datos primarios y literatura internacional, apoyado en herramientas de análisis de datos avanzadas, manteniendo una perspectiva humanizada en la interpretación de los hallazgos. En este documento se usa el término ciberseguridad como concepto paraguas que incluye seguridad de la información, seguridad digital y protección de activos digitales.

Este trabajo aporta evidencia empírica actualizada sobre el estado de madurez de la ciberseguridad organizacional en América Latina, un campo donde la literatura regional sigue siendo escasa.

A través de un enfoque multivariable, se pretende identificar patrones y correlaciones que contribuyan a una mejor comprensión de los desafíos y oportunidades en la gestión de la ciberseguridad en la región, ofreciendo así insumos relevantes para la toma de decisiones tanto a nivel estratégico como operativo.

Metodología

La presente investigación se basa en el análisis de los resultados de la encuesta **ELSI 2025** (*datos propios*), diseñada para explorar el estado de madurez de la ciberseguridad organizacional en diversas industrias de América Latina.

Diseño de la encuesta

La encuesta fue estructurada en torno a siete bloques temáticos:

1. **Demografía organizacional**
2. **Presupuestos de ciberseguridad**
3. **Experiencia en incidentes de seguridad**
4. **Mecanismos de protección implementados**
5. **Función ejecutiva del CISO**
6. **Conciencia y apoyo de la alta dirección**
7. **Prioridades estratégicas para 2025**

El cuestionario incluyó preguntas de opción única, opción múltiple y escalas ordinales, que permitieron capturar tanto percepciones como métricas cuantificables.

Población y muestra

La encuesta fue distribuida de manera dirigida a profesionales de ciberseguridad, TI y gestión de riesgos en organizaciones de diferen-

tes tamaños y sectores en América Latina. Se recibieron un total de 180 respuestas válidas, que conforman la muestra analizada.

La composición sectorial de la muestra incluye organizaciones de consultoría especializada, educación, fuerzas armadas, alimentos y bebidas, construcción/ingeniería, gobierno, salud, servicios financieros, entre otros sectores emergentes.

Procesamiento de los datos

Se aplicaron técnicas de limpieza y codificación para asegurar la consistencia de las respuestas. En el caso de las preguntas de opción múltiple, se procedió a la expansión de columnas para permitir el análisis cruzado.

Para explorar las relaciones entre variables ordinales y no paramétricas, se utilizó el coeficiente de correlación de Spearman (ρ), el cual es adecuado para detectar asociaciones monotónicas sin requerir distribución normal de los datos (*Gauthier, 2001*).

Adicionalmente, se construyeron matrices de correlación y análisis multivariables para identificar patrones significativos.

Limitaciones

Cabe señalar que algunas variables, como los costos de los incidentes, presentaron una tasa de respuesta más baja en la muestra analizada. Este fenómeno ha sido identificado en estudios previos (*IBM, 2024; Verizon 2025*), debido a la sensibilidad de este tipo de información.

Demografía

La muestra analizada (n=180) está compuesta por organizaciones de diferentes tamaños y sectores.

Tamaño de la organización

La distribución según tamaño muestra que:

- Empresas de 1-50 empleados: 32%
- Empresas de 51-200 empleados: 20%
- Empresas de 201-500 empleados: 15%
- Empresas de 501-1000 empleados: 12%
- Empresas de 1001-5000 empleados: 13%
- Empresas de más de 5000 empleados: 8%

Este perfil refleja una representación equilibrada entre pequeñas, medianas y grandes organizaciones.

Sectores representados

Los principales sectores de actividad representados en la muestra son:

- Consultoría especializada
- Educación
- Fuerzas Armadas
- Alimentos y Bebidas
- Construcción e Ingeniería
- Gobierno
- Salud
- Servicios financieros
- Otros sectores emergentes.

Presupuestos

El análisis de los presupuestos de ciberseguridad revela una diversidad significativa en los niveles de inversión.

Porcentaje del presupuesto global destinado a ciberseguridad

- La mayoría de las organizaciones destina entre **5% y 15%** de su presupuesto global de TI a ciberseguridad.
- Un porcentaje menor (alrededor del **10%**) reporta una inversión superior al **15%**.
- Otro segmento relevante destina menos del **5%**.

Presupuesto en términos absolutos (USD)

- **Menos de USD $50,000** anuales: 65%
- **USD $50,001 - $100,000**: 20%
- **USD $100,001 - $150,000**: 10%
- **Más de USD $150,000**: 5%

Este patrón sugiere que, si bien la ciberseguridad es reconocida como prioridad estratégica, persisten limitaciones presupuestales en muchos segmentos, especialmente fuera de los sectores más regulados (banca, gobierno, salud).

Cruce: Presupuesto ↔ Sector

El cruce entre nivel de presupuesto e industria muestra que (tabla 1).

Este patrón refuerza los hallazgos de (ISACA, 2024; LastPass, 2024; IANS, 2024), que destacan los in-

Sector	Nivel de inversión predominante
Consultoría especializada	Medio – Alto
Educación	Bajo
Fuerzas Armadas	Alto
Gobierno	Alto
Alimentos y Bebidas	Bajo
Construcción/Ingeniería	Bajo – Medio
Salud	Medio
Servicios financieros	Alto

Tabla 1 Sectores por nivel de inversión

crementos continuos en los presupuestos, aún en las pequeñas empresas, que no siempre se traducen en mejorías en la protección de la información.

Nota: Los niveles *Alto*, *Medio*, *Bajo* se derivan de la distribución de respuestas sobre el porcentaje del presupuesto global destinado a ciberseguridad y el presupuesto en USD reportado por sector:

- *Alto*: mayoría de las organizaciones del sector reportan inversiones superiores al 10-15% del presupuesto de TI, o más de USD $100,000 anuales.
- *Medio*: predominan inversiones en el rango de 5%-15% o entre USD $50,000 - $100,000 anuales.
- *Bajo*: predominan inversiones menores al 5% o menos de USD $50,000 anuales.
- La categoría *"Medio-Alto"* se emplea para sectores con distribución bimodal en la muestra (subgrupos significativos con inversión Alta y Media).

En definitiva, las inversiones en seguridad, aunque los sectores y el tamaño son factores fundamentales, tienen sus dinámicas propias que hacen que estos presupuestos siempre sean cambiantes, lo cierto para todas las empresas es que hay inversiones, los retos de la inversión siempre existirán, pero los datos pueden ser la clave para hacer cada vez más eficiente ese proceso (Marsh, 2025).

Incidentes

Frecuencia de incidentes

- La mayoría de las organizaciones reporta haber enfrentado **entre 1 y 5 incidentes** durante el año.
- Un 15% reporta **más de 5 incidentes**.
- Un 20% indicó **no haber registrado incidentes**.

Estos resultados son consistentes con el enfoque actual de la industria, que señala que **la ocurrencia de incidentes es inevitable** en un entorno de amenazas dinámicas (*Gartner, 2025; WEF, 2025a; WEF 2025b; Gartner, 2025).*

Costos de los incidentes

- **Menos de USD $50,000**: mayoría de los casos.
- **USD $50,001 - $100,000**: segmento relevante.
- **Más de USD $150,000**: minoría.

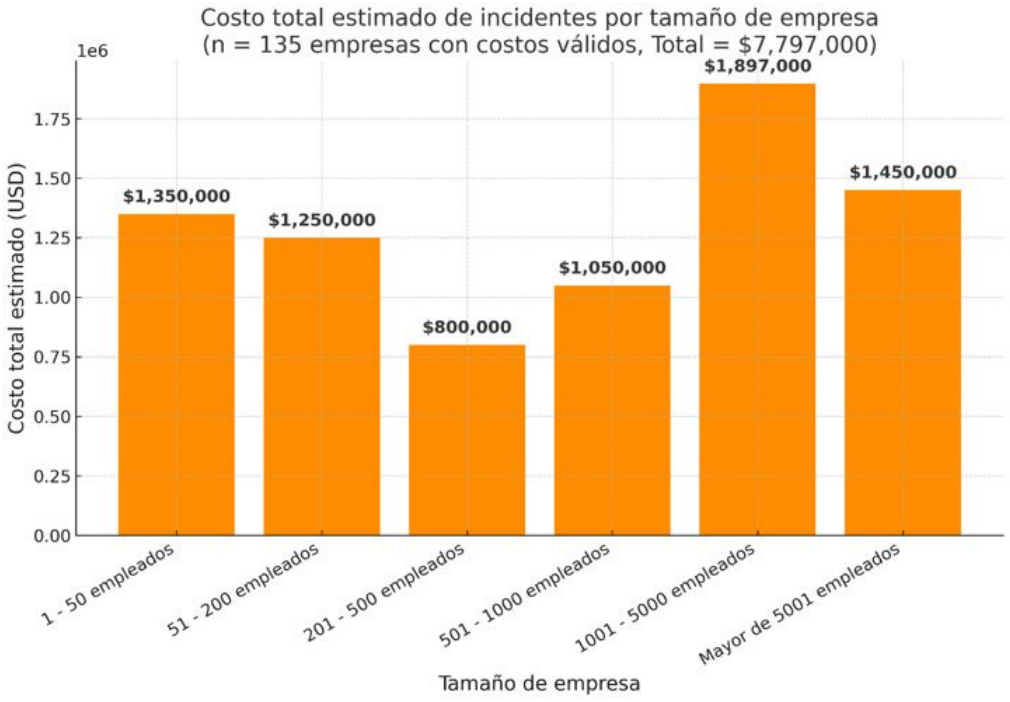
La dificultad para cuantificar con precisión estos costos refuerza la necesidad de desarrollar mejores prácticas de **cuantificación de riesgos cibernéticos** (*IBM, 2024; ENISA, 2025; FBI 2025*), sin embargo, se ha avanzado en usar métodos que al menos ayuden a las empresas a poder hacer la labor de cuantificar los incidentes cibernéticos (ThreatConnect, 2024), y viene en continuo crecimiento la práctica de hacerlo, la tasa aún sigue siendo baja de aquellos que lo hacen, solo

un 15% según PwC (2024) realiza cuantificación.

Al revisar por sectores los costos de los incidentes y hacer cálculos estimativos por tamaños de las empresas, se tiene la gráfica 1.

Impacto económico general de los incidentes

El costo total estimado de los incidentes reportados por las organizaciones que entregaron información válida asciende a aproximadamente **USD $7.8 millones**. Al analizar la distribución por tamaño de empresa (gráfica 1), se observa que las organizaciones de mayor tamaño concentran los costos más elevados. Este patrón puede estar influenciado por múltiples factores, incluyendo una **mayor exposición a riesgos**, **mayor complejidad operativa** y, posiblemente, una **mayor capacidad para identificar y cuantificar los costos asociados a los incidentes**. Estos hallazgos coinciden con tendencias observadas en estudios internacionales recientes (Verizon, 2025; IBM, 2024; WEF, 2025b;TrendMicro, 2025), que señalan que las organizaciones con mayor madurez tienden a tener una mejor visibilidad sobre el impacto económico de los incidentes de ciberseguridad.



Gráfica 1 Costos de incidentes x tamaños de empresa

Tipos de incidentes más frecuentes

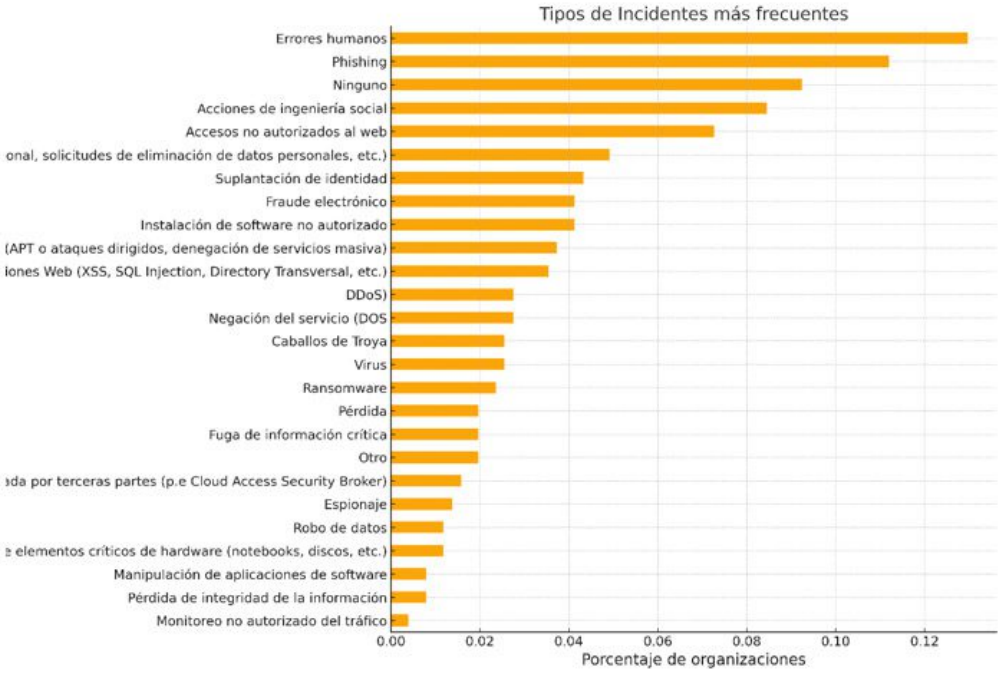
Se listan los más representativos, Tabla 2.

Estos resultados son coherentes con las tendencias globales reportadas por *Verizon* (2025). Al revisar todos los incidentes de los datos tenemos la gráfica 2.

El análisis de los mecanismos de ciberseguridad implementados proporciona una visión sobre la madurez técnica de las organizaciones encuestadas.

Tipo de incidente	Frecuencia relativa
Errores humanos	Muy alta
Fugas de información sensible	Alta
Ransomware	Moderada
Ataques de denegación de servicio (DDoS)	Menor
Compromiso de cuentas de usuario	Menor

Tabla 2 Tipo de incidentes y frecuencias



Gráfica 2 Total de tipos de incidentes

Nota: Las categorías *Muy alta*, *Alta*, *Moderada* y *Menor* se derivan del conteo relativo de respuestas para cada tipo de incidente:

- *Muy alta*: incidente más frecuente en la muestra (reportado por más del 70% de las organizaciones que reportaron incidentes).
- *Alta*: reportado por entre 50% y 70%.
- *Moderada*: reportado por entre 25% y 49%.
- *Menor*: reportado por menos del 25%.

Tipos de incidentes y sus impactos económicos

Al revisar, los detalles de cuánto cuestan los incidentes de seguridad, tenemos la gráfica 3.

Gráfica 3 Tipos de incidentes y costos

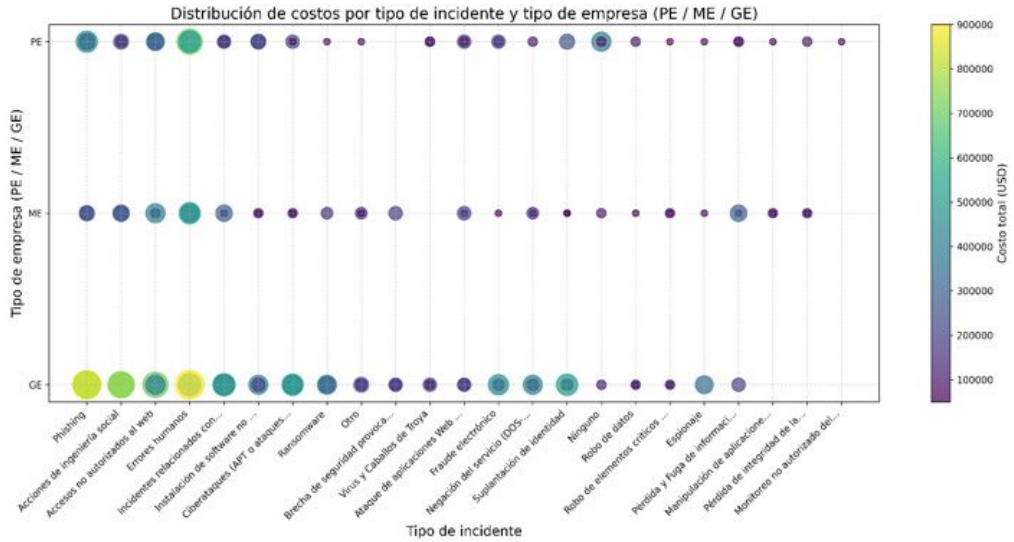
Impacto económico por tipo de incidente

Además del análisis global de los costos, se realizó un cruce específico para identificar el impacto económico asociado a los distintos tipos de incidentes reportados. Los resultados muestran que los **errores humanos** representan el tipo de incidente con mayor costo agregado en la muestra, seguido por incidentes de **phishing** y **acciones de ingeniería social** (Gráfica 3). Este patrón coincide con tendencias internacionales, que señalan que los factores humanos siguen siendo una de las principales fuentes de riesgo en ciberseguridad (Verizon, 2025; IBM, 2024; Verizon, 2025).

Cabe señalar que, en este análisis, una misma organización puede contribuir al costo total de múltiples tipos de incidente, en línea con la naturaleza multifacética de los ataques contemporáneos (ENISA, 2024). Por este motivo, el costo agregado por tipo de incidente no es mutuamente excluyente y puede superar el costo total consolidado a nivel empresa, así mismo los costos ocultos que pueden llegar a tener los incidentes, pueden no siempre ser tasados, y mucho menos estimados, lo que hace mas desafiante el poder saber realmente cuanto le cuesta alas empresas sus incidentes de manera general (Romanosky, 2016; Wolf, 2024; (IIA, 2017)

Distribución de costos por tipo de incidente y tipo de empresa

La gráfica 4, presenta la distribución de los costos totales estima-



Gráfica 4 Distribución de tipos de incidentes por tamaño de las empresas

dos de los distintos tipos de incidentes de ciberseguridad, segmentados por tamaño de empresa (PE: pequeñas empresas; ME: medianas empresas; GE: grandes empresas).

El análisis revela varios hallazgos relevantes:

Incidentes transversales: Ciertos tipos de incidentes —como errores humanos, phishing, acciones de ingeniería social y accesos no autorizados al web— afectan de manera significativa a los tres tipos de empresas, con costos considerables en todas las categorías.

Mayor concentración en grandes empresas: Se observa que las grandes empresas (GE) presentan, en términos absolutos, los costos más elevados en casi todas las categorías de incidentes. Este patrón puede asociarse tanto a una mayor exposición como a una mayor capacidad de reporte y cuantificación precisa de los incidentes.

Costos relativos en pequeñas empresas: Destaca que las pequeñas empresas (PE) también muestran costos significativos en incidentes como errores humanos, phishing y acciones de ingeniería social, lo que evidencia una vulnerabilidad relativa elevada frente a estos vectores de ataque.

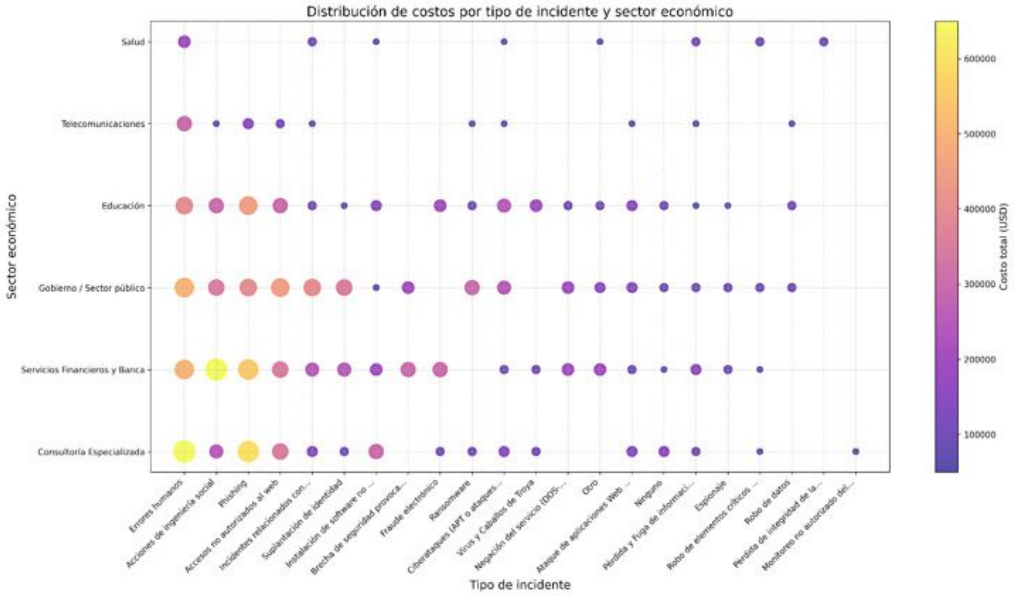
Menor presencia de incidentes complejos en medianas empresas: Se advierte que las medianas empresas (ME) registran, en esta muestra, menores costos relativos en categorías como ciberataques avanzados o ataques a aplicaciones web, lo que podría reflejar tanto diferencias en la madurez tecnológica como en los niveles de exposición.

Estos hallazgos sugieren que la naturaleza y el impacto económico de los incidentes de ciberseguridad no son homogéneos entre los distintos tamaños de empresa. Por el contrario, la distribución de costos evidencia patrones diferenciados que deben ser considerados en el diseño de estrategias de protección digital y en la asignación de recursos (CISA, 2020; Romanosky, 2016; IMF, 2025; Petrosyan, 2025; Check Point Research, 2025)

Esta gráfica también pone de manifiesto que incluso incidentes considerados “básicos” como errores humanos y phishing generan impactos económicos relevantes en todos los segmentos empresariales, lo cual subraya la importancia de fortalecer las capacidades humanas y de concienciación en ciberseguridad.

Distribución de costos por tipo de incidente y sector económico

La gráfica 5, muestra la distribución de los costos totales estimados por tipo de incidente de ciberseguridad, segmentados por sector económico. El tamaño y color de los círculos



Gráfica 5 Distribución de los tipos de incidentes x sector económico

es proporcional al costo total reportado en la muestra para cada combinación de incidente y sector.

El análisis evidencia patrones diferenciados entre los sectores:

Patrones transversales: Incidentes como errores humanos, phishing y acciones de ingeniería social representan los costos más significativos de manera transversal en la mayoría de los sectores analizados.

Sectores con alta concentración de costos: En consultoría especializada y servicios financieros y banca, los incidentes asociados a phishing y acciones de ingeniería social concentran los mayores costos. En el sector gobierno / sector público, destacan los costos asociados a errores humanos, phishing y accesos no autorizados al web. En el sector educación, phishing y acciones de ingeniería social representan las categorías más costosas. El sector salud presenta una menor concentración, aunque los errores humanos generan un impacto económico relevante.

Relación con el perfil del sector: Estos hallazgos sugieren que los sectores más orientados a la gestión de información y servicios (consultoría, banca, gobierno) tienden a ser más sensibles a incidentes relacionados con la explotación del factor humano (phishing e ingeniería social). Por su parte, sectores como salud o educación también muestran vulnerabilidad en incidentes básicos, lo que podría reflejar desafíos en términos de ca-

pacitación y cultura organizacional en ciberseguridad.

Importancia de estrategias sectoriales: Los resultados refuerzan la necesidad de diseñar estrategias de protección digital adaptadas a la naturaleza y perfil de cada sector, priorizando medidas preventivas frente a los tipos de incidentes que históricamente generan mayores costos en cada industria.

Este análisis confirma que la ciberseguridad no es un fenómeno homogéneo entre industrias. Los patrones de riesgo y sus impactos económicos son sectoriales, lo cual debe ser considerado en políticas públicas y en la gestión estratégica de ciberseguridad en las organizaciones. (Petrosyan, 2025; Check Point Research, 2025).

Herramientas

Cantidad de mecanismos implementados

El conteo revela:

- **Organizaciones grandes** (más de 1000 empleados) implementan en promedio **11 a 14 mecanismos**.
- **Organizaciones pequeñas** (1-50 empleados) implementan en promedio **4 a 6 mecanismos**.

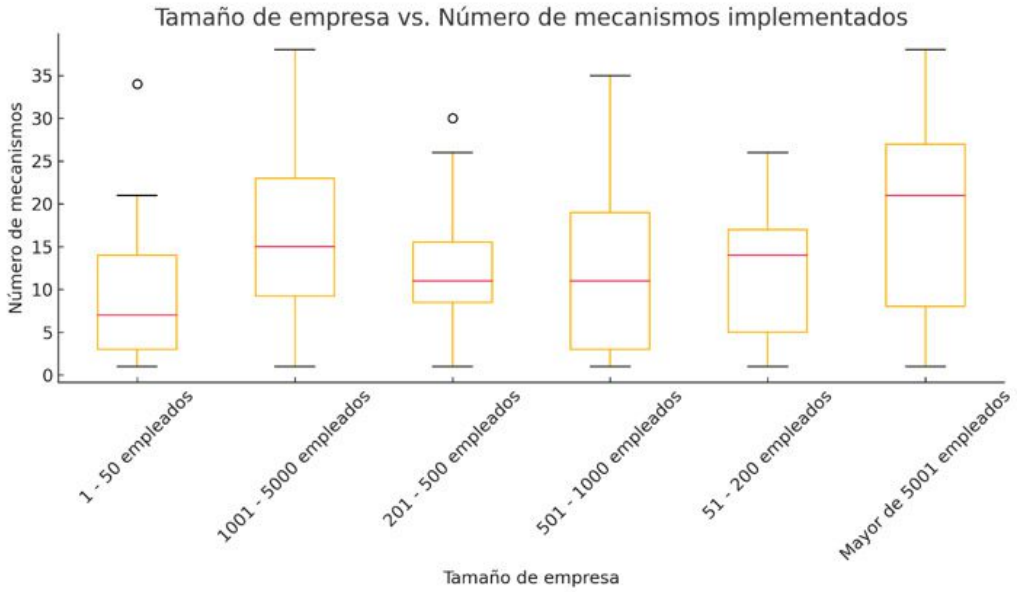
Mecanismos más usados por tipo de empresa

La tabla 3, lo que muestra es como existe una generalidad en la distribución de los mecanismos y herramientas de protección, mientras las empresas grandes se orientan a usar herramientas más sofisticadas, las pequeñas usan los mecanismos tradicionales. Este patrón es consistente con estudios de **ISACA** (2024) y **ENISA** (2024).

La gráfica 6, muestra la distribución del número de mecanismos implementados por cada categoría de tamaño de empresa. Empresas más grandes (por ejemplo, Más de 5000 empleados, 1001-5000, 501-1000) tienden a tener un mayor número de mecanismos (distribución más alta). Empresas más pequeñas (1-50, 51-200) muestran una menor cantidad de mecanismos (mediana y rangos más bajos).

Tipo de empresa	Mecanismos más usados
Grandes empresas	EDR, SIEM, MFA (Multi-Factor Authentication), Gestión de vulnerabilidades, Seguridad en la nube
Pequeñas empresas	Antivirus tradicional, Firewall perimetral, Backups básicos, Gestión de contraseñas

Tabla 3 Uso de mecanismos y herramientas de protección



Gráfica 6 distribución de mecanismos por tamaños de empresa

Sin embargo, la mera disponibilidad de herramientas no es suficiente si persisten barreras culturales y organizativas, como se analiza a continuación.

Obstáculos percibidos para la ciberseguridad

La seguridad digital, ciberseguridad y seguridad de la información, se abre camino dentro de las empresas, eso es una realidad, que se ve reflejada en los reportes de industria, sin embargo, hay obstáculos que marcan el desarrollo de esta, al indagar por cuales son los obstáculos y sobre todo sectorizarlos por el tamaño de la industria, obtenemos la tabla 4.

Interpretación:

- Estos resultados refuerzan lo planteado por el **Foro Económico Mundial en sus recientes**

Tamaño de empresa	Obstáculos predominantes
1-50 empleados	Falta de cultura de seguridad, falta de formación, falta de apoyo directivo
1001-5000 empleados	Falta de colaboración entre áreas, complejidad tecnológica, falta de apoyo directivo

Tabla 4 Obstáculos de la seguridad por tamaña de las empresas

reportes (2025a; 2025b), que subrayan que el avance en tecnología debe estar acompañado por una evolución en **gobernanza** y **cultura organizativa**.

- La falta de apoyo de la alta dirección es un desafío **transversal**, presente tanto en pequeñas como en grandes organizaciones.
- Este hallazgo es consistente con el enfoque de **ENISA** (2024), que subraya que los desafíos evolucionan a medida que la organización crece en complejidad. De igual manera que las medidas de defensa son esenciales y más allá de las evoluciones naturales, las empresas las deben usar, y estar en la dinámica de poder saber cuales son las más adecuados para sus entornos organizacionales (CyberEdge, 2025; Microsoft, 2024).

Función ejecutiva del CISO

El análisis del perfil del CISO en las organizaciones encuestadas muestra una amplia diversidad en cuanto al nivel de madurez de esta función.

Presencia formal de la figura de CISO

- **30%** tiene un CISO formalmente nombrado.
- **40%**: función liderada por responsable informal.
- **30%**: sin figura formal.

Tipología del CISO (tabla 5)

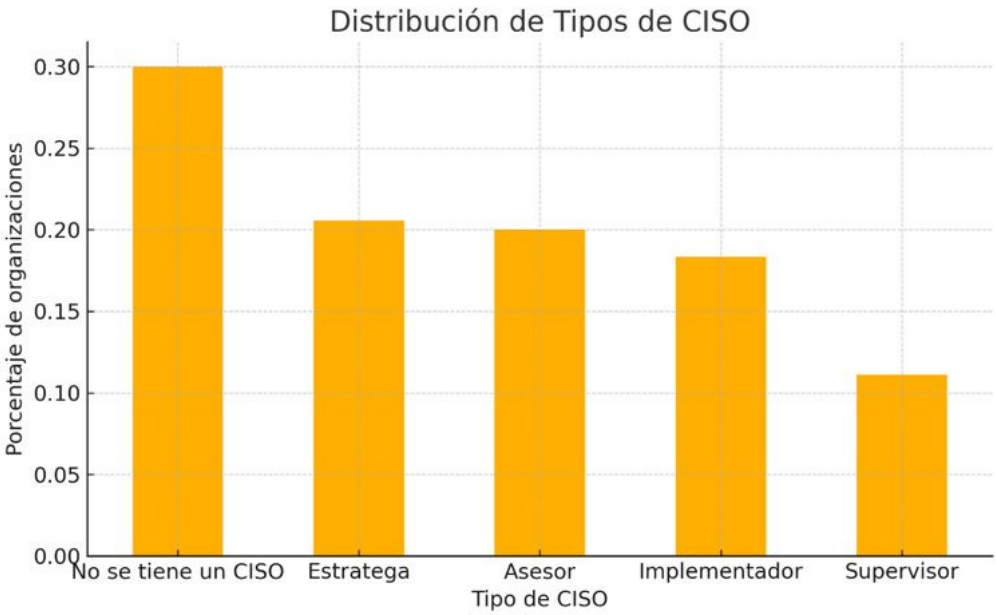
Predominan los perfiles tipo 3 (Asesor) y 4 (Estratega) en organizaciones de mayor tamaño y sectores regulados. En contraste, en pymes y sectores emergentes prevalecen los perfiles tipo 1 (Implementador) y 2 (Supervisor). Este patrón se evidencia en la gráfica 7.

Brechas identificadas

Aquí aplico el ajuste que sugeriste: Según la literatura especializada (FTI Consulting, 2024; IANS, 2025; Hitch Partners, 2025; Splunk, 2025), hay grandes avances en relación con la posición del CISO, su posicionamiento ejecutivo y su presencia como líder y estratega, aún con esos avances se mantienen en muchos contextos globales persisten brechas como:

Tipo de CISO	% de organizaciones
Implementador (operativo)	18 %
Supervisor	22 %
Asesor	34 %
Estratega	26 %

Tabla 5 Tipos de CISO



Gráfica 7 distribución de tipos de CISO

- Limitada participación del CISO en comités de dirección.
- Falta de alineación entre ciberseguridad y estrategia de negocio.
- Restricciones presupuestales que limitan la evolución del rol.

Esto se presenta como **tendencia de la literatura**, no como dato directo de esta encuesta, que destacan la necesidad de una mayor integración del CISO en los órganos de gobierno corporativo. El líder de seguridad digital en la región LATAM, como en el mundo basado en estos datos y correlacionados con reporte de la industria, sigue creciendo como rol, con más credibilidad, y retos importantes en relación con la responsabilidad, rendición de cuentas y carácter ejecutivo, que hoy más que nunca se demanda de ellos por parte de la dirección ejecutiva y de los cuerpos directivos (Diligent , 2025; Duncan, 2025)

Conciencia de la alta dirección

La conciencia y el apoyo de los niveles directivos constituye un factor crítico para la madurez en ciberseguridad (*WEF, 2025a; WEF, 2025b)*. En esta sección se analiza el nivel de consciencia y el grado de participación de la alta dirección en los procesos de ciberseguridad de sus organizaciones, utilizando un modelo conceptual basado en la Ventana de Johari.

Los datos generales sobre la consciencia en seguridad por parte de los directivos están relacionados de la siguiente manera.

Percepción sobre el nivel de conciencia

- **28%** percibe alto nivel de conciencia.
- **47%**: nivel moderado.
- **25%**: nivel bajo o muy bajo.

Factores que limitan el apoyo directivo

Según reportes de industria, aunque las directivas cada vez más están involucradas o su mesa de alguna manera toca los temas de ciberseguridad (*Diligent, 2025; Barsky & Pearlson, 2025; Morgan, 2024; ACC, 2025; IANS, 2023)*, aún existen factores que suelen limitar el apoyo incluyen:

- Percepción de la ciberseguridad como un centro de costos.
- Desconocimiento del impacto potencial de los incidentes.
- Desconexión entre discurso de negocio y discurso de ciberseguridad.

Estos hallazgos refuerzan la recomendación de fortalecer la capacidad de los CISOs para comunicar en lenguaje de negocio y cuantificar el riesgo de manera comprensible para los directorios.

El análisis de la conciencia y participación de la alta dirección en ciberseguridad, realizado a través

Gráfica 8. Relación de participación vs consciencia de la alta dirección

del modelo conceptual de la Ventana de Johari, ver gráfica 8, revela patrones significativos en la muestra analizada. Las empresas pequeñas muestran los mayores niveles de involucramiento directo, tanto en términos de conciencia como de participación. Por el contrario, las empresas medianas reflejan mayores brechas, caracterizadas por menores niveles de conciencia ejecutiva y menor integración estratégica del tema. Las grandes empresas muestran resultados mixtos, con un liderazgo más estructurado, pero también con evidencia de cierto distanciamiento en algunos casos.

A nivel sectorial, los sectores de **Consultoría Especializada**, **Salud** y **Telecomunicaciones** destacan por su mayor madurez, reflejada en altos niveles tanto de conciencia como de participación. Por el contrario, sectores como **Gobierno / Sector Público** y **Educación** presentan mayores desafíos, con una mayor proporción de casos en los cuadrantes de baja conciencia o participación.

Por tamaño de empresa

Los datos sugieren que las empresas más pequeñas tienden a involucrarse más directamente en temas de ciberseguridad, probablemente debido a estructuras organizativas más planas y una menor distancia entre la alta dirección y las funciones operativas.

- **Empresas pequeñas (1-50 empleados) 66,7%** reportan alta conciencia y participación.
- **Empresas medianas (501-1000 empleados)** solo **20%** muestran este nivel de involucramiento, predominando los cuadrantes de baja conciencia y participación.
- **Empresas grandes (mayor de 5001 empleados) 48,3%** muestran alta conciencia y participación, aunque también existen casos relevantes de conciencia baja o participación parcial.

Este patrón es consistente con estudios internacionales (*Diligent, 2025; Barsky & Pearlson, 2025; Morgan, 2024; ACC, 2025; IANS, 2023*) en donde también hay rastros de estos comportamientos que hacen a las empresas y sobre todo las de menor tamaño a retos en la gobernanza de ciberseguridad, debido a limitaciones en recursos y estructuras de liderazgo.

Por sector económico

En términos sectoriales:

Se observa en la tabla 6, que sectores tradicionalmente más expuestos a marcos regulatorios exigentes (Financiero, Telecomunicaciones, Salud) tienden a mostrar mayores niveles de madurez. Sin embargo, es llamativo que el sector **Servicios Financieros y Banca**, pese a sus fuertes marcos regulatorios, no lidere en participación

Sector	Alta conciencia y participación (%)
Consultoría Especializada	**60,87 %**
Salud	**50,00 %**
Telecomunicaciones	**50,00 %**
Retail / Consumo masivo	**42,86 %**
Servicios Financieros y Banca	**34,62 %**
Gobierno / Sector público	**31,82 %**
Educación	**23,33 %**

Tabla 6 Consciencia y participación de la alta dirección x sector

consciente, lo cual es coherente con hallazgos recientes que sugieren que en algunos sectores el cumplimiento se centra más en aspectos técnicos que en gobernanza estratégica (PwC, 2024; Cheng & Groysberg, 2017; (Barsky & Pearlson, 2025).

Por el contrario, sectores como **Gobierno / Sector público** y **Educación** muestran la mayor presencia en los cuadrantes de baja conciencia y participación, reflejando desafíos estructurales y culturales que son comunes en estos entornos (IANS, 2023; ENISA 2024).

Estos resultados refuerzan la conclusión de que el involucramiento efectivo de la alta dirección en ciberseguridad no depende únicamente del tamaño o del sector, sino de una combinación de factores culturales, regulatorios y estratégicos que se vienen continuamente convirtiendo en dilemas claves que determinan el nivel de involucramiento necesario a ser atendido (Kierzek, 2025; (van, 2024).

- Las **empresas pequeñas**, a pesar de tener menos recursos, logran una integración más directa del tema en la agenda ejecutiva.
- Las **empresas medianas** requieren atención especial, al ser el segmento donde las brechas son más pronunciadas.
- A nivel sectorial, la madurez es más elevada en sectores regulados, pero incluso en estos persisten oportunidades de mejora en términos de gobernanza y alineación estratégica.

Estos hallazgos se alinean con estudios recientes (Deloitte, 2024; IANS 2023; WEF 2025b; Diligent 2025) que enfatizan que el verdadero diferenciador en la madurez de ciberseguridad es el nivel de liderazgo consciente desde la alta dirección, más allá de los controles

técnicos. así mismo, se refuerzan la necesidad de continuar promoviendo un liderazgo consciente en ciberseguridad, capaz de integrar estos temas de manera estratégica en la gestión organizacional. Más allá de los controles técnicos, es el compromiso real de la alta dirección el que marcará la diferencia en la resiliencia cibernética de las organizaciones latinoamericanas en los próximos años. En última instancia se puede decir que el involucramiento de las juntas directivas, cuerpos ejecutivos y niveles superiores de las organizaciones, los convierten en eslabón final de la cadena de defensa, protección y valor de un negocio (Al Issa et al., 2024).

.

Discusión

Los resultados de este análisis confirman varios de los desafíos estratégicos que enfrentan las organizaciones de América Latina en su proceso de madurez en ciberseguridad.

Inversiones y madurez técnica

A pesar de que la mayoría de las organizaciones destina entre un **5% y 15%** de su presupuesto de TI a ciberseguridad, los incidentes costosos y complejos siguen ocurriendo. Esto refuerza lo planteado por IBM (2024; Verizon 2025; WEF 2025a). **la tecnología por sí sola no garantiza resiliencia organizativa**. En la dinámica empresarial, cada organización invierte en la medida que son orientadas y guiadas, aunque definitivamente las brechas entre las grandes empresas y las pequeñas existe, se mantiene y aumenta en términos de la destinación de presupuestos para la seguridad (Heidt et al., 2019; Sage, 2023).

El análisis de **mecanismos usados** muestra que las organizaciones grandes implementan mecanismos avanzados (EDR, SIEM, MFA), mientras que las pymes dependen más de controles básicos (Antivirus tradicional, Firewall). Este patrón es consistente con ISACA (2024) y ENISA (2024). Esa **densidad de mecanismos implementados** según tamaño y sector, pero estas diferencias no siempre se traducen en una menor ocurrencia de incidentes. Esto sugiere la necesidad de avanzar hacia modelos de **resiliencia organizativa** que integren:

- **Gobernanza**
- **Cultura de seguridad**
- **Gestión de riesgos estratégicos**

Por otra parte, incidentes como **Errores humanos** siguen siendo los más frecuentes en toda la muestra, lo que evidencia que los factores **culturales y organizativos** son igual o más relevantes que la sofisticación tecnológica, como destaca algunos reportes de industria (ENISA 2024; Mimecast, 2025; Crowdstrike, 2025; Kaspersky, 2023).

Conciencia de la alta dirección

La percepción de los encuestados muestra que solo un **28%** de los ejecutivos tienen un alto nivel de conciencia sobre ciberseguridad.

En consecuencia, esto limita la capacidad de:

- Priorizar inversiones estratégicas
- Alinear la ciberseguridad con los objetivos del negocio
- Gestionar eficazmente el riesgo cibernético

Según la literatura (WEF, 2025b; Gartner, 2025), los factores que limitan el apoyo directivo incluyen la percepción de ciberseguridad como costo, el desconocimiento del impacto de los incidentes y la desconexión entre discurso técnico y de negocio.

Este hallazgo refuerza la necesidad de que los **CISOs** desarrollen competencias en **comunicación estratégica** y en **cuantificación del riesgo en términos comprensibles para el negocio**, como proponen **FTI Consulting** (2024), **IANS** (2024) y (Hitch Partners, 2025).

Madurez de la función del CISO

Aunque se observa un avance hacia perfiles de CISO **Asesor** (34%) y **Estratega** (26%) en sectores más regulados y organizaciones grandes, persisten brechas en la región:

Según la literatura (FTI Consulting, 2024; IANS, 2025; Hitch Partners, 2025; Splunk, 2025), se destacan desafíos como:

- Limitada participación en comités de dirección
- Falta de alineación estratégica
- Restricciones presupuestales

Sin embargo, estos hallazgos confirman que la función del CISO debe seguir evolucionando hacia un rol **estratégico** y **transversal**, como interlocutor clave en el gobierno corporativo. Así mismo, no se puede considerar al CISO un profesional que resuelva todas las necesidades de las empresas, y mucho menos que pueda llenar todos los vacíos que los cuerpos ejecutivos tengan, agregar un director de seguridad de la información a una junta es un movimiento popular, pero no es suficiente para mejorar la resiliencia cibernética (Hepfer, 2024).

Los resultados evidencian que las organizaciones con una alta conciencia directiva y una función madura del CISO tienden a reportar una mejor alineación entre inversiones en ciberseguridad y capacidades organizativas, mostrando menores brechas entre expectativas y resultados.

Obstáculos

Los obstáculos se pueden agrupar de manera general como lo muestra la tabla 7:

Tamaño	Obstáculos
Pequeñas empresas	Obstáculos culturales y de formación
Grandes empresas	Obstáculos de gobernanza y colaboración inter-áreas

Tabla 7 Agrupación general de obstáculos por tamaños de empresas globales

La complejidad de las organizaciones, en la medida que aumentan sus desafíos de posicionamiento de mercado, de crecimiento y expansión, hacen que la ciberseguridad en si misma tenga más obstáculos, no queriendo decir con esto que no se pueden enfrentar dicho desafío (Joshi, 2025; EY, 2025), estos desafíos evolucionan a medida que crece la complejidad organizativa.

Temas claves

El análisis de los **temas estratégicos identificados por sector** revela diferencias relevantes (tabla 8).

Interpretación estratégica

Estos cruces refuerzan la necesidad de:

- Diseñar **estrategias sectoriales diferenciadas**.
- Promover una **madurez cibernética contextualizada**, adaptada a las amenazas y prioridades de cada industria.
- Fortalecer la capacidad de los **CISOs** para alinear su agenda con los riesgos específicos del negocio.

Los sectores avanzados (Consultoría, Fuerzas Armadas) abordan temas complejos (APT, ciber conflictos, cuantificación de riesgos). Otros sectores, como Educación, priorizan la protección de infraestructuras críticas, mientras que sectores emergentes se centran en desafíos tecnológicos como IoT y Blockchain.

Este patrón respalda lo propuesto por (WEF 2025a; 2025b) y ENISA

Sector	Temas clave
Consultoría especializada	APT, Ciberespionaje, Ataques a infraestructuras críticas, Cyber Risk Quantification
Educación	Protección de infraestructuras críticas, Talento humano en seguridad, Noticias falsas (Fake news), Seguridad en la nube
Fuerzas Armadas	Ciberconflictos, Ciberarmas, Ciberespionaje
Otros sectores	IoT, Blockchain, seguridad en la nube

Tabla 8 Temas claves x sectores

(2024): la necesidad de construir estrategias diferenciadas **por sector y contexto**.

Síntesis

En conjunto, estos resultados aportan evidencia a favor de un enfoque de ciberseguridad:

- **Holístico**
- **Adaptativo**
- **Orientado a negocio**
- **Contextualizado por sector y madurez organizativa**

Conclusiones

El presente análisis exploratorio de la encuesta nacional de Seguridad Informática (ELSI) 2025 permite identificar patrones clave en el proceso de madurez de la ciberseguridad organizacional en América Latina.

Principales hallazgos

La ciberseguridad sigue siendo un desafío transversal, con una evolución heterogénea según el tamaño y el sector de las organizaciones.

Aunque las inversiones en ciberseguridad han crecido, persiste una brecha entre la **implementación tecnológica** y la **resiliencia organizativa**. Incidentes como **Errores humanos** siguen siendo altamente frecuentes en todos los tamaños de empresa.

La figura del **CISO** muestra avances en su madurez: los perfiles de **Asesor** (34 %) y **Estratega** (26 %) son cada vez más comunes en sectores regulados y grandes empresas, aunque persisten brechas en términos de participación estratégica.

La **conciencia de la alta dirección** continúa siendo un factor crítico de éxito. Solo un **28%** de los encuestados percibe un alto nivel de conciencia en los altos mandos.

Los **obstáculos para la ciberseguridad** evolucionan con el tamaño de la organización: las pymes enfrentan desafíos principalmente culturales, mientras que las grandes empresas enfrentan problemas de gobernanza y colaboración inter-áreas.

Las **prioridades estratégicas en ciberseguridad** son claramente diferenciadas por sector, lo que subraya la necesidad de enfoques adaptativos y contextualizados.

Implicaciones prácticas

Los resultados sugieren que las organizaciones deben avanzar hacia un modelo de ciberseguridad **integrado y estratégico**, que contemple:

- El fortalecimiento de la **gobernanza** y la **cultura de seguridad**.

- La mejora de la **comunicación entre el CISO y la alta dirección**.
- La **alineación de la ciberseguridad con la estrategia de negocio**.
- La **adaptación de las estrategias según sector y madurez organizativa**.

Este estudio busca servir como referencia para la construcción de estrategias de ciberseguridad más maduras, adaptativas y contextualizadas para las organizaciones latinoamericanas en los próximos años.

Referencias

ACC. (2025). *2025 State of Cybersecurity Report: An In-house Perspective | Association of Corporate Counsel (ACC)*. Acc.com. https://www.acc.com/resource-library/2025-state-cybersecurity-report-house-perspective

Al Issa, A., Boehm, J., & Nayfeh, M. (2024). *Boards of directors: The final cybersecurity defense for industrials | McKinsey*. www.mckinsey.com. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/boards-of-directors-the-final-cybersecurity-defense-for-industrials

Barsky, N. P., & Pearlson, K. (2025). *Boards Need a More Active Approach to Cybersecurity*. Harvard Business Review. https://hbr.org/2025/05/boards-need-a-more-active-approach-to-cybersecurity

Check Point Research. (2025). *Q1 2025 Global Cyber Attack Report from Check Point Software*. https://blog.checkpoint.com/research/q1-2025-global-cyber-attack-report-from-check-point-software-an-almost-50-surge-in-cyber-threats-worldwide-with-a-rise-of-126-in-ransomware-attacks/

Cheng, J. Y.-J., & Groysberg, B. (2017). *Why Boards Aren't Dealing with Cyberthreats*. Harvard Business Review. https://hbr.org/2017/02/why-boards-arent-dealing-with-cyberthreats

CISA. (2020). *Cost of a cyber incident: Systematic review and cross-validation*. https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf

Crowdstrike. (2025). *CrowdStrike 2025 Global Threat Report*. Crowdstrike.com. https://go.crowdstrike.com/2025-global-threat-report.html

CyberEdge. (2025). *Cyberthreat Defense Report 2025*. CyberEdge Group. https://cyberedgegroup.com/cdr/

Deloitte. (2024). *Global Future of Cyber Survey, 4th Edition*. Deloitte. https://www.deloitte.com/content/dam/assets-shared/docs/services/risk-advisory/2024/deloitte-global-future-of-cyber-survey-4th-edition-the-promise-of-cyber.pdf

Diligent. (2025). *What Directors Think 2025*. Diligent.com. https://www.diligent.com/resources/research/WDT-2025

Duncan, A. (2025). *Global Directors' and Officers' Survey Report 2024/2025*. WTW. https://www.wtwco.com/en-hk/insights/2025/03/global-directors-and-officers-survey-report-2024-2025

ENISA. (2024). *ENISA Threat Landscape 2024*. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

EY. (2025). *Cybersecurity: From value protection to value creation | EY - Global*. Ey.com. https://www.ey.com/en_gl/insights/consulting/how-can-cybersecurity-go-beyond-value-protection-to-value-creation

FBI. (2025). *FBI Releases Annual Internet Crime Report | Federal Bureau of Investigation*. Federal Bureau of Investigation. https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report

FTI Consulting. (2024). *ciso-redefined-navigating-c-suite-perceptions*. FTI Strategic Communications. https://fticommunications.com/ciso-redefined-navigating-c-suite-perceptions-and-expectations/

Gartner. (2025). *Top Cybersecurity Trends and Strategies for Securing the Future | Gartner*. Gartner. https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends

Gauthier, B. (2009). *Recherche Sociale*. PUQ.

Heidt, M., Gerlach, J. P., & Buxmann, P. (2019). Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments. *Information Systems Frontiers*, *21*(6), 1285–1305. https://doi.org/10.1007/s10796-019-09959-1

Hepfer, M. (2024). *One CISO Can't Fill Your Board's Cybersecurity Gaps | Manuel Hepfer*. MIT Sloan Management Review. https://sloanreview.mit.edu/article/one-ciso-cant-fill-your-boards-cybersecurity-gaps/

Hitch Partners. (2025). *Hitch Partners*. Hitch Partners. https://www.hitchpartners.com/ciso-security-leadership-survey-results-25

IANS. (2023). *CISOs as Board Directors, CISO Board Readiness Analysis*. IANS. https://www.iansresearch.com/resources/infosec-content-downloads/research-report-insights/cisos-as-board-directors-ciso-board-readiness-analysis

IANS. (2024). *Security Budget Benchmark Report| IANS Research*. IANS. https://www.iansresearch.com/resources/ians-security-budget-benchmark-report

IANS. (2025). *State of the CISO*. IANS. https://www.iansresearch.com/resources/ians-state-of-the-ciso-report

IBM. (2024). *Cost of a data breach report 2024*. IBM. https://www.ibm.com/reports/data-breach

IIA. (2017). *Seven hidden costs of a cyber-attack | Instituut van Internal Auditors*. www.iia.nl. https://www.iia.nl/actualiteit/nieuws/seven-hidden-costs-of-a-cyberattack

IMF. (2025). *Strengthening Cybersecurity: Lessons from the Cybersecurity Survey*. IMF; International Monetary Fund. https://www.imf.org/en/Publications/TNM/Issues/2025/03/21/Strengthening-Cybersecurity-Lessons-from-the-Cybersecurity-Survey-559636

ISACA. (2024). *State of Cybersecurity 2024 | ISACA*. ISACA. https://www.isaca.org/resources/reports/state-of-cybersecurity-2024

Joshi, A. (2025). *The growing complexity of global cybersecurity: Moving from challenges to action*. World Economic Forum. https://www.weforum.org/stories/2025/01/growing-complexity-global-cybersecurity-from-challenges-action/

Kaspersky. (2023). *Redefining the Human Factor in Cybersecurity*. www.kaspersky.com. https://www.kaspersky.com/blog/human-factor-360-report-2023/

Kierzek, H. (2025). *NACD Survey Uncovers 2025 Board Trends and Areas for Improvement*. https://www.nacdonline.org/all-governance/governance-resources/directorship-magazine/online-exclusives/2025/q1-2025/nacd-survey-uncovers-2025-board-trends-and-areas-for-improvement/

LastPass. (2024). *SMB Cybersecurity Disconnect Report - LastPass*. Lastpass.com. https://www.lastpass.com/it/resources/reports/smb-commercial-cybersecurity-report

Marsh. (2025). *Using data to prioritize cybersecurity investments | Marsh*. Marsh.com. https://www.marsh.com/en/services/cyber-risk/insights/using-cybersecurity-analytics-to-prioritize-cybersecurity-investments.html

Microsoft. (2024). *Microsoft Digital Defense Report 2024*. Microsoft.com. https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

Mimecast. (2025). *Human risk has surpassed technology gaps as the biggest cybersecurity challenge for organizations around the globe as demonstrated in the findings of our SOHR 2025 Report.* Mimecast. https://www.mimecast.com/resources/ebooks/state-of-human-risk-2025/

Morgan, S. (2024). *Boardroom Cybersecurity Report 2024*. Secureworks. https://www.secureworks.com/centers/boardroom-cybersecurity-report-2024

Petrosyan, A. (2025). *Global distribution of cyber attacks in top industries 2022*. Statista. https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/

PwC. (2025). *2025 Global Digital Trust Insights here: PwC*. PwC. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights/report-download-2025.html

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, *2*(2), 121–135. https://doi.org/10.1093/cybsec/tyw001

Sage. (2023). *Cyber Security for SMBs: Navigating Complexity and Building Resilience*. Sage.com. https://www.sage.com/en-gb/company/digital-newsroom/2023/10/12/cyber-security-for-navigating-complexity-and-building-resilience/

Splunk. (2025). *The CISO Report*. https://www.splunk.com/en_us/pdfs/gated/ebooks/ciso-report-2025.pdf

ThreatConnect. (2024). *ThreatConnect Risk Quantification Report: Healthcare, Manufacturing & Utilities*. ThreatConnect. https://threatconnect.com/resource/threatconnect-risk-quantification-report-healthcare-manufacturing-utilities/

TrendMicro. (2025). *Trend 2025 Cyber Risk Report | Trend Micro (US)*. Trendmicro.com. https://www.trendmicro.com/vinfo/us/security/news/threat-landscape/trend-2025-cyber-risk-report

van. (2024). *Directors Should Prepare to Address Five Board Dilemmas in 2025*. https://www.nacdonline.org/all-governance/governance-resources/governance-research/outlook-and-challenges/2025-governance-outlook/preparing-for-five-crucial-board-balancing-acts-in-2025/

Verizon. (2025). *Verizon*. Verizon Business. https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf

WEF. (2025a). *Global Cybersecurity Outlook 2025*. World Economic Forum; WEF. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

WEF. (2025b). *The Global Risks Report 2025 20th Edition*. https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf

Wolf, A. (2024). *Hidden Costs of Cyber Attacks | Arctic Wolf*. Arctic Wolf. https://arcticwolf.com/resources/blog/hidden-costs-of-cyber-attacks/