Informe anual

VISIÓN CIBERSEGURA | IBEROAMÉRICA

2026

Diagnóstico regional de madurez en ciberseguridad

n = **171 organizaciones** • **26,958** personas
23 países iberoamericanos • Mayo 2026
Comité de Ciberseguridad ALETI • AMITI
Coordinación: **Ana Cecilia Pérez**

aleti
impulsamos la transformación digital

AMITI
Liderando la digitalización por México

Sobre este estudio

ALETI — Asociación Latinoamericana de Empresas de Tecnología de Información

ALETI es la principal organización gremial del sector tecnológico de América Latina. Agrupa a las cámaras y asociaciones nacionales de empresas de tecnología de información de la región, representando a miles de organizaciones en más de 20 países. Su misión es fortalecer el desarrollo de la industria tecnológica latinoamericana, promover políticas que impulsen la competitividad regional y construir puentes de cooperación entre el sector privado, los gobiernos y la academia.

El Comité de Ciberseguridad de ALETI es el espacio técnico y estratégico desde el cual la asociación articula iniciativas, produce diagnósticos y promueve estándares que fortalezcan la postura de seguridad digital de las organizaciones iberoamericanas.

AMITI — Asociación Mexicana de la Industria de Tecnologías de Información

AMITI es la organización que representa a la industria de tecnologías de información en México. Agrupa a las principales empresas del sector — desde grandes corporativos hasta startups — y trabaja para promover el desarrollo de un ecosistema tecnológico competitivo, innovador y responsable. AMITI participa activamente en el diseño de políticas públicas relacionadas con la transformación digital, la ciberseguridad y la economía del conocimiento.

Por qué ALETI y AMITI decidieron hacer este estudio juntos

La ciberseguridad es un problema regional, no nacional. Las amenazas no respetan fronteras, los incidentes en infraestructura crítica tienen efectos transfronterizos y las brechas de talento afectan a toda la región por igual. Sin embargo, el diagnóstico regional disponible dependía casi exclusivamente de fuentes externas — reportes globales que nos incluían como subconjunto estadístico, sin voz propia y sin la granularidad necesaria para entender nuestra realidad específica.

ALETI y AMITI decidieron subsanar ese vacío. Visión Cibersegura Iberoamérica es el resultado de ese compromiso conjunto: el primer diagnóstico regional de madurez en ciberseguridad construido con datos propios, levantados directamente entre las redes especializadas de ambas organizaciones, con instrumentos diseñados para capturar la realidad iberoamericana en toda su complejidad — desde las organizaciones hasta los hogares y las aulas.

Este estudio no es un fin en sí mismo. Es el punto de partida de una agenda de trabajo regional que ALETI y AMITI se comprometen a sostener en el tiempo.

Indicador	Dato
Muestra organizacional (Bloque A)	n = 171 organizaciones, 23 países
Muestra familiar y educativa (Bloque B)	n = 26,958 personas
Período de recolección	Agosto – Diciembre 2025
Idiomas de recolección	Español y portugués
Reportes internacionales de referencia	7 reportes validados
Presentación pública	21 de mayo de 2026

Agradecimientos

Este estudio no existiría sin el compromiso de las personas que lo hicieron posible — no como signatarias de un documento, sino como participantes activos que dedicaron tiempo, criterio y energía a construir algo que la región necesitaba y no tenía.

Al Comité de Ciberseguridad de ALETI en su conjunto: gracias por confiar en que valía la pena hacerlo, y por responder cuando se necesitaba.

Un reconocimiento especial a quienes estuvieron presentes de manera consistente a lo largo de todo el proceso:

Ana Cecilia Pérez Rosales, Fundadora y Socia Directora de Capa8, empresa especializada en ciberseguridad con presencia en México y América Latina que acompaña a más de 100 organizaciones en los sectores financiero, energético, gubernamental y de salud. Con 26 años de trayectoria en el sector, formó parte del equipo que construyó el primer SOC de México, desarrolló metodologías registradas como propiedad intelectual y es co-autora de la guía práctica de Information Security Management de ITIL v4. Es autora de la norma NMX-I-319.
Líder del Comité de Ciberseguridad de ALETI para Iberoamérica, integrante del Consejo Directivo de AMITI, participante del D4D Hub de la Digital Alliance UE-LAC y líder de la Women Task Force de ISC2 México. Socia del IWF y de Conectadas. Dirige las iniciativas Familias Ciberseguras, Escuelas Ciberseguras y el Festival CiberLATAM.
Certificada CISSP, CISM, CISA y CRISC. Reconocida por RSA Conference como Humans as Heroes 2019, como Top Women in Cybersecurity LATAM por WOMCY en 2021 e ISC2 Partner del Año 2021.

Víctor Merchand, Coordinador del Área de Tecnologías de la Información y Ciberdelito de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) en México. Licenciado en Informática y Maestro en Diseño y Gestión de Proyectos Tecnológicos, cuenta además con certificación como Scrum Master y un Diplomado en Gestión Estratégica de Tecnologías de Información de la Universidad de Georgetown. Con más de 24 años de experiencia en gestión de proyectos de tecnología, innovación y ciberdelito, ha desarrollado su carrera en organismos de Naciones Unidas en México, Perú y Ecuador, en el Gobierno Federal mexicano y en

el sector privado. Su trabajo conecta a México con el Programa Global de Ciberdelito de la ONU, que coordina a 193 países en la prevención, investigación y persecución de delitos digitales. Su participación en el estudio aportó la perspectiva de la cooperación internacional y el marco normativo global contra el cibercrimen.

Teresita de Jesús Poblete, Psicóloga, Magíster en Derechos de Infancia y Políticas Públicas por la Universidad de la República (Uruguay), donde actualmente cursa el Doctorado en Antropología. Coordina el Programa Interamericano de Cooperación para el Uso Seguro de Internet del Instituto Interamericano del Niño, la Niña y Adolescentes (IIN-OEA), desde donde impulsa iniciativas regionales sobre ciberseguridad, ciudadanía digital y protección integral de derechos en línea. Es Coordinadora Académica y docente del Diploma en Infancias, Derechos y Políticas Públicas de FLACSO Uruguay, e integrante del proyecto MIGRAMEDIOS. Cuenta con publicaciones en capítulos de libros y revistas indexadas, y ha participado como expositora en congresos internacionales de educación, ciencias sociales e infancias. Su contribución al estudio ancló el Bloque B en el marco de derechos de la infancia y aportó el rigor institucional de la OEA al análisis del entorno educativo y familiar.

Anna De Luca, Directora Ejecutiva de Responsabilidad Social Corporativa en Sybven, empresa venezolana de integración tecnológica. Licenciada en Biología con mención en Zoología por la Universidad Central de Venezuela (1991), Magíster en Gerencia Ambiental por el IUPFAN (1997) y certificada como Coach Organizacional Internacional por la IAC (certificación No. 1047). A lo largo de más de tres décadas ha combinado su trayectoria en gestión empresarial, tecnología y responsabilidad social con un compromiso constante con el sector gremial: desde 2010 es directora de Cavedatos (Cámara Venezolana de las Tecnologías de Información), organización afiliada a ALETI, WITSA e ISOC Internacional, y desde 2024 se desempeña como su Presidenta.

Carlos Enrique Ungo, ejecutivo tecnológico con más de 25 años de experiencia liderando transformación digital, ciberseguridad e innovación en los sectores de telecomunicaciones, logística y gobierno en Panamá y la región. Como CIO y CTO de organizaciones líderes ha dirigido equipos multidisciplinarios de hasta 800 personas y gestionado presupuestos anuales superiores a USD 8 millones. Impulsó las primeras soluciones predictivas de IA móvil de Panamá, marcos nacionales de ciberseguridad y continuidad de negocio, y fue parte del lanzamiento de la primera billetera móvil

del país. Forma parte de consejos asesores en CIONet, EU CyberNet y APEDE, y contribuye activamente a conversaciones sobre gobernanza de IA y política pública digital. Su participación en el comité aportó exactamente lo que un estudio de esta naturaleza necesita: la perspectiva de quien ha ejecutado lo que el diagnóstico mide.

Vladimir Meza, CEO de SESITE y docente con más de 30 años de experiencia en tecnologías de información, capacitación y desarrollo organizacional. Su trayectoria en los sectores gobierno, bancario y comercial, combinada con su formación en educación y su trabajo actual en IA, ciencia de datos y ciberseguridad, aportó al comité exactamente lo que un estudio de esta naturaleza necesita: alguien que entiende tanto la tecnología como a las personas que tienen que aprenderla.

Este estudio también le debe mucho al equipo operativo que hizo posible que todo funcionara. **Aurea Guerrero**, de AMITI, mantuvo el hilo institucional con una precisión que nunca fue visible pero siempre fue indispensable. **Andrea Vesga** y **Estefanía Ramos**, de ALETI, convirtieron cada pendiente en entregable y cada conversación en acción. Sin las tres, este estudio habría seguido siendo una buena intención.

A todos: gracias.

Índice

Capítulo 1. Carta editorial

Hay preguntas que el sector tecnológico iberoamericano lleva años postergando. No por falta de voluntad, sino porque responderlas con rigor requiere algo que no teníamos: datos propios, levantados desde adentro, con las voces de quienes viven el problema todos los días.

Este estudio es nuestra respuesta a esa deuda.

Cuando el Comité de Ciberseguridad de ALETI y AMITI decidió impulsar Visión Cibersegura Iberoamérica, teníamos claro lo que existía. Sabíamos que el WEF, IBM, Verizon, ESET, la OEA y el ITU producen cada año análisis rigurosos sobre el estado global de la ciberseguridad. Los respetamos. Los usamos como referencia a lo largo de todo este estudio. Pero también sabíamos lo que esos reportes no podían darnos: una mirada desde adentro de la región, con preguntas formuladas para nuestra realidad, respondidas por quienes realmente toman decisiones de ciberseguridad en organizaciones iberoamericanas, en sus hogares y en sus aulas.

La pregunta que nos movió fue sencilla: ¿cómo estamos nosotros, específicamente, cuando dejamos de inferirlo desde datos globales y vamos a preguntarlo directamente?

La respuesta no fue sencilla de obtener.

Conseguir que respondieran quienes debían responder fue uno de los mayores retos del proyecto. No nos interesaba cualquier muestra — nos interesaba la muestra correcta. Directivos, responsables de tecnología y especialistas en seguridad de la información que pudieran hablar desde la realidad de sus organizaciones, no desde la percepción general. Padres, docentes, directivos escolares, adolescentes y niños que pudieran dar cuenta del estado real de la seguridad digital en hogares y escuelas de la región. Llegar a ese perfil, en 23 países, en dos idiomas, con la

disposición de responder con honestidad, tomó tiempo, esfuerzo colectivo y la confianza que solo se construye dentro de redes gremiales comprometidas con el trabajo real.

El resultado son 171 respuestas organizacionales y 26,958 respuestas de familias, docentes y menores. No es el estudio más grande que existe sobre ciberseguridad en la región. Es el más específico. Y esa especificidad es lo que lo hace valioso.

> *Lo que encontramos no es alentador. Pero encontrarlo es el primer paso para poder cambiarlo.*

La región iberoamericana sabe que tiene un problema con la ciberseguridad. Lo saben los directivos que declaran tenerla en su agenda pero no han terminado de formalizarla en políticas operativas. Lo saben los padres que supervisan a sus hijos de manera ocasional porque nadie les enseñó otra forma de hacerlo. Lo saben los docentes que usan tecnología en sus aulas todos los días sin haber recibido formación para gestionar los riesgos que esa tecnología trae consigo. Lo saben los adolescentes que conocen los peligros en línea pero solo de forma parcial.

Saber que existe un problema y tener la capacidad de resolverlo son dos cosas distintas. Esa distancia — entre la conciencia y la acción, entre el discurso y la estructura, entre la intención y la ejecución — es lo que este estudio documenta con datos. Y es lo que ALETI y AMITI se comprometieron a visibilizar, porque sin un diagnóstico honesto no hay política pública que valga, ni inversión que llegue al lugar correcto, ni formación que atienda las brechas reales.

Este estudio no es un punto de llegada. Es el instrumento que necesitábamos para saber desde dónde salimos. Lo que venga después — las políticas que se ajusten, los programas que se diseñen, las conversaciones que se abran entre gobiernos, empresas, escuelas y familias — depende de que este diagnóstico llegue a quienes pueden actuar sobre él.

La región tiene lo que necesita para mejorar: talento, voluntad y, ahora, un espejo propio en el que mirarse.

Lo que sigue depende de todos.

Este estudio existe porque tres personas apostaron por él antes de que existiera. Juan Francisco Martínez, Presidente de ALETI, le dio casa, respaldo y la red que hizo posible llegar a 23 países. Pablo Gómez, Presidente de AMITI, confió en que valía la pena comprometer el nombre de la asociación en un proyecto sin precedente regional. Sofía Pérez Gasque, Directora Nacional de AMITI, tradujo ese respaldo institucional en acción concreta en cada etapa del camino. Sin los tres, esto habría sido una idea bien intencionada. Con ellos, es un estudio.

Ana Cecilia Pérez

Líder del Comité de Ciberseguridad

ALETI — Asociación Latinoamericana de Empresas de Tecnología de Información

Representando a AMITI

Mayo 2026

Capítulo 2. Contexto y justificación

La región iberoamericana lleva años hablando de ciberseguridad. El reto no es perpetuar el discurso — es resolverlo. Y lo que este estudio documenta, antes que cualquier otra cosa, es la distancia entre ambos: la que existe entre el discurso y la capacidad real de respuesta.

Esa distancia no es nueva. Lo que sí es nuevo es que ahora tenemos datos propios para medirla.

El punto de partida: un problema anterior al del resto del mundo

Cuando los grandes reportes globales describen el panorama de ciberseguridad, lo hacen desde la perspectiva de economías con infraestructura institucional consolidada, marcos regulatorios operativos y capacidades técnicas establecidas. Sus recomendaciones asumen un piso de madurez que buena parte de la región iberoamericana todavía no tiene.

En América Latina y el Caribe, solo el 13% de los respondentes tiene confianza en la preparación nacional ante un incidente cibernético mayor — la cifra más baja de todas las regiones del mundo. El 49% declara no tener confianza. *(WEF Global Cybersecurity Outlook 2026)*

Ese dato no describe un rezago técnico. Describe una fractura de confianza entre las organizaciones y los Estados que deberían protegerlas. Las organizaciones que no confían en su entorno regulatorio e institucional toman decisiones de seguridad en solitario, con recursos limitados y sin coordinación regional.

El problema de la región no es el mismo que el del resto del mundo. Es uno anterior. Mientras otros debaten cómo optimizar sus capacidades de respuesta, iberoamérica todavía está cerrando la brecha entre lo que se declara y lo que se ejecuta.

Por qué este estudio era necesario

Antes de este estudio, el diagnóstico de la región en ciberseguridad dependía casi exclusivamente de fuentes externas. Los grandes reportes internacionales — WEF, IBM, Verizon, ESET, OEA/BID, ITU — nos incluyen como subconjunto estadístico dentro de análisis globales. Nos describen desde afuera, con metodologías diseñadas para otros contextos necesariamente y desde marcos de referencia que no siempre corresponden a nuestra realidad institucional.

Eso no los hace menos valiosos. Los utilizamos como ancla de contexto a lo largo de todo este estudio, y si bien no son suficientes para responder la pregunta que realmente importa: ¿cómo estamos nosotros, específicamente, cuando nos miramos desde adentro?

"Visión Cibersegura Iberoamérica" nació para responder esa pregunta. Es el primer estudio de madurez en ciberseguridad construido con datos propios de la región iberoamericana, levantados directamente por organizaciones gremiales de tecnología — ALETI y AMITI — entre sus redes de contacto especializadas en el tema.

Lo que este estudio aporta que otros no tienen

La diferencia no está solo en la geografía. Está en el origen de los datos, en el perfil de quienes respondieron y en las preguntas que se hicieron.

Por un lado, los respondentes del ámbito empresarial y tecnológico no son una muestra aleatoria del mundo corporativo iberoamericano. Son directivos, responsables de tecnología y especialistas en seguridad de la información — las personas que toman decisiones sobre ciberseguridad en sus organizaciones. Cuando el 77% dice que la ciberseguridad está en su mapa de riesgos y solo el 32% está preparado para enfrentar una amenaza avanzada, ese dato no es una percepción externa: es un autodiagnóstico del propio sector especializado.

Por otro lado, el estudio incorpora la voz de los actores del entorno doméstico y educativo, un eslabón tradicionalmente invisible en los diagnósticos regionales de ciberseguridad. Lo reportan directamente niños, adolescentes, padres, cuidadores, docentes y directivos de escuelas. Eso permite observar fenómenos que los macroestudios globales no capturan:

El hallazgo de una supervisión mayoritariamente manual — 50% ocasional y 32% estricta, con solo 10% usando herramientas técnicas — no proviene de una inferencia: lo declaran los propios padres.

La brecha entre conciencia del riesgo y protección efectiva — 91% de adolescentes conoce los riesgos, pero solo 3% de padres usa VPN y 9% doble autenticación — se construye cruzando las dos poblaciones encuestadas.

La debilidad institucional del sistema educativo — 78.67% de docentes sin capacitación en ciberseguridad — es un dato autorreportado por quienes están en el aula, no una opinión externa.

Este enfoque dual produce una fotografía estructural que ningún informe de tendencias globales puede replicar. No porque sea más grande en escala, sino porque es más preciso en lo que mide: el estado de conciencia y capacidad real de quienes más deberían saber cómo está la región, desde la junta directiva hasta la mesa del comedor y el salón de clases.

La brecha de habilidades en ciberseguridad creció un 8% entre 2024 y 2025. Las organizaciones pequeñas tienen siete veces más probabilidad de tener resiliencia insuficiente que las grandes. *(WEF Global Cybersecurity Outlook 2026)*

En ese contexto global, Iberoamérica no es la excepción: es el caso más agudo. Y sin un diagnóstico que integre tanto a quienes definen estrategias como a quienes crían, educan y aprenden, cualquier política de respuesta seguirá siendo una adaptación incompleta de soluciones diseñadas para otros problemas.

El momento en que se realiza este estudio

Este estudio se publica en un momento de aceleración. La inteligencia artificial ya no es una amenaza futura en ciberseguridad: es una herramienta que los atacantes usan hoy, con más velocidad y recursos que la mayoría de las organizaciones de la región.

El ransomware estuvo presente en el 44% de los incidentes globales registrados. En organizaciones pequeñas y medianas, la cifra llega al 88%. *(Verizon DBIR 2025)*

Este contexto de urgencia tecnológica se cruza con un llamado internacional sin precedentes. En noviembre de 2025, ocho organismos de Naciones Unidas — UIT, UNICEF, UNESCO y OIT, entre otros — firmaron la Declaración conjunta sobre inteligencia artificial y derechos del niño. La declaración advierte que "los rápidos avances de la IA están cambiando radicalmente el mundo y afectando a las generaciones presentes y futuras de niños" y señala un problema estructural que este estudio confirma con datos regionales: "la mayoría de las herramientas y aplicaciones basadas en IA no están pensadas teniendo en cuenta a los niños y su bienestar" (UIT et al., 2025). El diagnóstico es directo: existe "falta de formación y capacitación adaptada" para todas las partes interesadas, incluyendo "falta de alfabetización en IA entre niños, maestros, padres y cuidadores, así como la necesidad de formación técnica para los responsables políticos". La propia

declaración insta a los Estados a "adoptar todas las medidas legislativas, administrativas y de otra índole" para garantizar una gobernanza de la IA basada en los derechos del niño, incluyendo "evaluaciones de impacto en los derechos del niño" y la "asignación de presupuesto suficiente" (Declaración conjunta IA y derechos del niño, 2025).

Más recientemente, en el AI Impact Summit 2026 celebrado en Nueva Delhi en febrero de 2026, 91 países y organizaciones internacionales — incluyendo Bolivia, Brasil, Chile, Costa Rica, Cuba, Guatemala, Paraguay, Perú, Portugal y Trinidad y Tobago — firmaron la Declaración de Nueva Delhi sobre el Impacto de la IA. La declaración marca un giro del enfoque de riesgo hacia uno de impacto y desarrollo, y subraya que los beneficios de la IA deben distribuirse de forma equitativa entre todas las naciones.

Solo 13 de los 30 países de América Latina y el Caribe tienen capacidad institucional real para implementar su estrategia nacional de ciberseguridad. Solo 9 están equipados para proteger infraestructura crítica. *(OEA/BID Cybersecurity Report 2025)*

Frente a esta asimetría, la propia declaración de Naciones Unidas insta a los Estados a "adoptar todas las medidas legislativas, administrativas y de otra índole" para garantizar una gobernanza de la IA basada en los derechos del niño, incluyendo "evaluaciones de impacto en los derechos del niño" y la "asignación de presupuesto suficiente" (Declaración conjunta IA y derechos del niño, 2025). Sin embargo, la realidad regional dista de esos estándares: solo 13 de los 30 países de América Latina y el Caribe tienen capacidad institucional real para implementar su estrategia nacional de ciberseguridad. Tener un diagnóstico propio que incluya la voz de niños, adolescentes, familias y docentes no es un lujo académico. Es el primer paso necesario para cualquier respuesta que valga la pena abordar en la región.

Alcance geográfico y temático

El estudio cubre tres dimensiones de análisis: las organizaciones públicas y privadas de la región (Bloque A), la niñez, las escuelas y las familias como primera línea de exposición digital (Bloque B), y el cruce de ambos con el panorama internacional de política pública (Bloque C).

Geográficamente, la muestra abarca 23 países iberoamericanos, con participación adicional de Canadá, Alemania, Israel y Estados Unidos. No todos los países tienen la misma representación — el anexo de resultados por país detalla los datos disponibles y sus limitaciones específicas.

> *Las organizaciones de la región saben que tienen un problema. El problema es que saberlo no es suficiente.*

Ese es el punto de partida de este estudio. Y lo que encontramos, capítulo a capítulo, es la evidencia de cuánto falta para que el saber se convierta en capacidad real.

Capítulo 3. Metodología

Este estudio no es una auditoría. No pretende representar estadísticamente a toda la región iberoamericana ni certificar el nivel de madurez de ningún país o sector. Lo que hace es otra cosa, y es igualmente necesario: documentar el estado real de conciencia y preparación en ciberseguridad entre quienes más deberían saberlo.

Esa distinción importa. Sin tenerla clara desde el principio, cualquier lector podría evaluar este estudio con los criterios equivocados.

Diseño del estudio

El estudio se diseñó en tres bloques de análisis complementarios. El Bloque A examina organizaciones públicas y privadas: cómo gestionan la ciberseguridad, qué tan formalizadas tienen sus estructuras, qué tan preparadas están para enfrentar amenazas reales. El Bloque B analiza niñez, escuelas y familias: el estado de la educación digital, la supervisión parental y la exposición a riesgos en entornos domésticos y escolares. El Bloque C cruza los hallazgos de ambos bloques con el panorama internacional para construir un mapa de madurez regional y derivar recomendaciones de política pública.

Los tres bloques comparten una pregunta de fondo: ¿cómo está la región iberoamericana en ciberseguridad cuando la miramos desde adentro, con datos propios, en lugar de inferirlo desde reportes globales que nos incluyen como subconjunto estadístico?

Instrumento de recolección

Se diseñaron dos instrumentos de recolección complementarios. La Encuesta 1, dirigida a responsables de ciberseguridad, directivos de tecnología y líderes

organizacionales de la región. La Encuesta 2, estuvo dirigida a familias, docentes, directivos escolares, adolescentes y niños, con n=26,958 respuestas completadas en múltiples países de la región. Estos instrumentos son distintos en diseño, población objetivo y alcance geográfico.

Muestra

La muestra del estudio opera en dos niveles. El Bloque A consolidó 171 respuestas de organizaciones en 23 países: Los países con mayor representación son México (34 respuestas), Panamá (28), Colombia (27) y Venezuela (15). Brasil suma 21, Bolivia y Canadá registran 6 respuestas cada uno, y Guatemala 5. El resto de los países participantes tiene entre 1 y 4 respuestas.

El Bloque B operó con una muestra independiente de 26,958 respuestas completadas, distribuidas entre padres y tutores (n=9,516), docentes (n=10,885), directivos escolares (n=1,941), adolescentes de 13 a 17 años (n=3,072) y niños de 6 a 12 años (n=1,544). La muestra tiene concentración mayoritaria en México, que representa el 82% de los docentes participantes, lo que debe considerarse al leer los datos como tendencia regional orientativa, no como representación estadística uniforme de todos los países.

Alcance y limitaciones

Este estudio tiene un alcance claro y lo declaramos con precisión, porque hacerlo fortalece el análisis en lugar de debilitarlo.

La muestra del Bloque A no es estadísticamente representativa del universo empresarial iberoamericano. No fue diseñada para serlo. Su valor no está en la escala sino en el perfil: 171 organizaciones con responsables reales de

ciberseguridad, distribuidas en 23 países, respondiendo sobre su situación concreta. Eso es un diagnóstico de alta señal, no una encuesta de mercado.

Los países con menos de cinco respuestas no permiten derivar conclusiones específicas sobre su realidad nacional. En el anexo de resultados por país, esos casos se presentan con una nota de cautela explícita y sin asignación de nivel de madurez.

> **Nota:** *Este estudio no pretende reemplazar a los grandes reportes internacionales de referencia — WEF Global Cybersecurity Outlook 2025, ESET Security Report 2025 LATAM, IBM Cost of a Data Breach 2025, Verizon DBIR 2025, OEA/BID Cybersecurity Report 2025, ITU Global Cybersecurity Index 2024 y CrowdStrike Global Threat Report 2026. Los utiliza como ancla de contexto internacional. La diferencia está en el origen: esos reportes miran a la región desde afuera. Este la mira desde adentro.*

Análisis de los datos

Los datos de los tres instrumentos fueron procesados y verificados antes de incorporarse al análisis. Cada cifra que aparece en este estudio proviene directamente de los archivos de respuesta originales — no de estimaciones, no de proyecciones, no de extrapolaciones. La diferencia entre lo que sabemos y lo que inferimos está marcada en todo momento.

El Bloque C cruza los hallazgos propios con los siete reportes internacionales seleccionados. Ese cruce no se hace para validar los datos propios con fuentes externas, sino para contextualizar: entender qué lugar ocupa la región en el panorama global y qué tan distintos son los problemas que enfrenta.

Capítulo 4. Bloque A - Organizaciones públicas y privadas

El 77% de las organizaciones participantes declara que la ciberseguridad está en su mapa de riesgos. Solo el 60% tiene una estrategia formal documentada. Solo el 32% está preparado para enfrentar una amenaza avanzada.

Esos tres números, leídos en secuencia, describen el problema central de la región con más precisión que cualquier análisis cualitativo: hay conciencia, hay intención, pero no hay capacidad operativa que los respalde.

Gobernanza y políticas

La gobernanza en ciberseguridad es el conjunto de decisiones formales que una organización toma sobre cómo protegerse: qué políticas implementa, qué estructuras de responsabilidad define, qué presupuesto asigna. Sin gobernanza, la ciberseguridad depende de las personas, no de los procesos. Y las personas cambian.

El 77% incluye la ciberseguridad en su mapa de riesgos. Es un dato positivo, pero incompleto. Solo el 60% tiene una estrategia formal documentada. El 17% no tiene políticas de seguridad de la información implementadas, y otro 15% las tiene en proceso. Eso significa que cerca de un tercio de las organizaciones que dijeron tener conciencia del riesgo aún no tienen las estructuras básicas para gestionarlo.

En cuanto a las cláusulas de seguridad digital en contratos laborales, el 52% de las organizaciones ya las ha incorporado, el 38% no lo ha hecho y el 10% no sabe si existen. Es un indicador concreto de cuánto peso real tiene la ciberseguridad en los acuerdos formales de la organización.

El discurso llegó antes que la estructura. Saber que la ciberseguridad importa no es lo mismo que haberla convertido en política operativa.

Capacidades operativas

Tener políticas no garantiza tener capacidades. El dato más contundente del estudio en esta dimensión es el de los planes de continuidad operativa: el 32% de las organizaciones no tiene uno, y el 22% está en proceso de desarrollarlo. Más de la mitad de las organizaciones participantes no tiene un protocolo formal de respuesta ante un incidente grave.

El ransomware estuvo presente en el 44% de los incidentes registrados globalmente. En organizaciones pequeñas y medianas, la cifra llega al 88%. *(Verizon DBIR 2025)*

El control de seguridad más extendido es la combinación de antivirus, firewall, monitoreo de red y actualizaciones periódicas — presente en el 23% de las organizaciones. Los controles avanzados — SIEM, SOC, pentesting, gestión de vulnerabilidades — no son práctica generalizada.

Sobre el uso de inteligencia artificial en ciberseguridad: el 44% ya la utiliza, el 44% no, y el 13% está en proceso de adopción. La región está dividida en dos mundos que coexisten dentro de la misma muestra.

Preparación ante amenazas reales

El 32% dice estar preparado ante amenazas avanzadas, el 36% parcialmente preparado, y el 32% no preparado. Un tercio en cada extremo, con un tercio en tierra de nadie. Sobre incidentes en el último año: el 62% dice no haber tenido ninguno, el 26% reconoce haber tenido al menos uno, y el 12% no pudo confirmar si fue atacado.

Ese 12% es el dato más grave del estudio. Los incidentes que no se detectan no se contienen, no se reportan y no se aprende de ellos.

El 32% de las organizaciones en América Latina no cuenta con las herramientas necesarias para confirmar si recibió un ataque cibernético. *(ESET Security Report 2025 LATAM)*

Entre quienes sí registraron incidentes, el tipo más frecuente fue la interrupción operativa (19%), seguida de ransomware (9%) y robo de información (7%). El 38% audita anualmente y el 30% semestralmente o más. Pero el 32% nunca audita.

Cultura de ciberseguridad

El 45% capacita a más del 50% de su personal. El 36% capacita a menos del 10%. El 21% no ofrece ninguna formación. La distribución es bimodal: un grupo que hizo de la capacitación una práctica sistemática y otro que no ha comenzado.

En nivel de formación: el 38% ofrece formación básica, el 27% continua, el 14% avanzada y el 21% ninguna. El déficit no es solo de alcance — también es de profundidad.

La brecha de habilidades en ciberseguridad creció un 8% entre 2024 y 2025. Las organizaciones pequeñas tienen siete veces más probabilidad de tener resiliencia insuficiente que las grandes. *(WEF Global Cybersecurity Outlook 2026)*

Coordinación y confianza institucional

El 29% se ubica en nivel Avanzado o Líder a nivel de su propia organización. Pero el 76% califica a su país en Inicial o En desarrollo. Solo el 13% considera que su país está en nivel Avanzado, y apenas el 4% en Líder.

Una organización que no confía en su Estado toma decisiones de seguridad en solitario, sin coordinación regional. La combinación más demandada al gobierno — elegida por el 30% de los respondentes — es formación y capacitación, regulación e infraestructura tecnológica.

El 75% de los respondentes está dispuesto a seguir participando en iniciativas relacionadas con el estudio — el 46% quiere recibir resultados y el 29% participar activamente. La comunidad especializada de la región está lista para moverse.

Niveles de madurez

Dimensión	Nivel de madurez
Gobernanza y políticas	**En desarrollo**
Capacidades operativas	**En desarrollo**
Cultura de ciberseguridad	**En desarrollo**
Inversión y recursos	**Inicial**
Coordinación y cooperación regional	**Inicial**

Tres dimensiones en nivel En desarrollo y dos en Inicial. Ninguna en Avanzado. El patrón es coherente con el diagnóstico: hay conciencia y hay intención, pero la ejecución no ha llegado todavía.

Capítulo 5. Bloque B - Niñez, escuelas y familias

La ciberseguridad no empieza en las organizaciones. Empieza en las personas — y las personas se forman mucho antes de llegar al mundo laboral. Lo que un niño aprende sobre el manejo de su identidad digital, sobre los riesgos en línea y sobre la privacidad de su información, determina en buena medida qué tipo de profesional y qué tipo de ciudadano digital será en el futuro.

El Bloque B analiza ese primer eslabón: el estado de la educación digital y la protección ante riesgos cibernéticos en niñez, escuelas y familias de la región iberoamericana.

> *El dato de partida del Bloque B: el 72.33% de los niños de 6 a 12 años usa internet todos los días. En ese entorno de alta exposición, el 82% de los padres aplica supervisión manual — 50% ocasional y 32% estricta — con solo el 10% usando herramientas técnicas de control parental. Alta exposición, supervisión débil: ese es el punto de partida de todo lo que sigue.*

Cultura digital en el hogar

La cultura digital en el hogar depende de lo que los padres saben, de lo que conversan con sus hijos y de cómo traducen ese conocimiento en límites y acompañamiento.

El 91% de los adolescentes declara conocer los riesgos digitales, pero ese conocimiento es mayoritariamente parcial: el 46% conoce algunos riesgos, el 35% la mayoría y solo el 10% tiene conocimiento avanzado. Saber que existen los peligros no es lo mismo que saber cómo identificarlos, evitarlos o responder ante ellos.

En los padres, el patrón es más preocupante. El 82% aplica supervisión manual, el 16% no usa ninguna medida de seguridad en el hogar. Las medidas más usadas son básicas: contraseñas seguras (55%) y antivirus (17%). Solo el 9% usa doble autenticación, el 3% VPN, y el 10% controles parentales.

Supervisión y acompañamiento parental

El 82% de los padres reporta supervisión manual — 50% ocasional y 32% estricta. Ese dato, leído junto con el 16% que no usa ninguna medida y el 10% que apenas usa controles parentales, muestra que la supervisión predominante es reactiva y opera sin herramientas auxiliares.

El acompañamiento humano es necesario, pero ya no es suficiente. Los niños pasan más de dos horas diarias conectados en muchos casos. La supervisión efectiva en el entorno digital requiere reglas claras, límites técnicos y capacidad de monitoreo asíncrono. Ninguna de esas tres condiciones está generalizada en los hogares de la región.

Tecnología en el entorno educativo

La escuela es, potencialmente, el mecanismo que reduce la brecha para fortalecer entornos digitales seguros. Es el único espacio que alcanza a toda la población infantil y adolescente independientemente del nivel educativo o los ingresos de sus familias.

Los datos muestran dos realidades simultáneas. Una positiva: el 80.69% de los niños de 6 a 12 años reporta que su escuela les ha explicado cómo usar internet con cuidado. Una menos positiva: entre los adolescentes, el 41% dice haber recibido formación suficiente, el 31% insuficiente y el 28% ninguna. El 72% recibió algún tipo de formación, pero más de la mitad considera que no fue suficiente.

La razón estructural de esa insuficiencia: el 78.67% de los docentes declara no haber recibido capacitación en ciberseguridad. El 85.5% de los directivos escolares reporta no tener presupuesto asignado para tecnología segura. Solo el 18% de los docentes se considera preparado para actuar ante un incidente digital con un estudiante.

La escuela expone a los niños y adolescentes a entornos digitales sin haber preparado a sus docentes para gestionar los riesgos. Esa contradicción es una decisión de política educativa que la región aún no ha resuelto.

Exposición a riesgos digitales

El 72.33% de los niños accede a internet todos los días. El 91% de los adolescentes declara conocer los riesgos, pero el 46% los conoce solo parcialmente. Esto refleja que la exposición es alta, el conocimiento es parcial y la protección — supervisión ocasional, herramientas técnicas mínimas — es baja. Esa fórmula define el perfil de vulnerabilidad de la región.

Capacidades de protección digital

Las capacidades de protección se miden por tres indicadores: herramientas disponibles, formación recibida y protocolos existentes. Los tres son débiles en la región.

En herramientas: contraseñas seguras (55%), antivirus (17%), doble autenticación (9%), VPN (3%). El 16% no usa ninguna medida. En formación: el 72.8% de los padres y cuidadores no ha recibido ningún tipo de capacitación sobre uso seguro de internet. Entre quienes sí la recibieron, las fuentes son dispersas — trabajo (16%), sitios web educativos (15%), medios de comunicación (11%) — no institucionales, no sistemáticas y no evaluables. En protocolos: en las escuelas, las respuestas sobre protocolos ante incidentes digitales se concentran en "No" y "No lo sé".

La protección digital en la región tiene el mismo problema que la gobernanza en las organizaciones: hay conciencia, hay intención, pero no hay estructura. Sin estructura, la protección queda librada a la voluntad individual de padres y docentes.

Niveles de madurez

Dimensión	Nivel de madurez
Cultura digital en el hogar	**En desarrollo**
Supervisión y acompañamiento parental	**En desarrollo**
Tecnología en el entorno educativo	**Inicial**
Exposición a riesgos digitales	**En desarrollo**
Capacidades de protección digital	**Inicial**

El patrón del Bloque B replica, en el ámbito familiar y escolar, lo mismo que el Bloque A documentó en las organizaciones: conciencia alta, capacidades bajas. Ese hallazgo no es una coincidencia. Es la expresión, en dos niveles distintos, de un mismo déficit estructural. La brecha que documenta el Bloque A tiene, en parte, su origen aquí.

Capítulo 6. Bloque C - Análisis transversal y política pública

Los bloques A y B documentan lo que ocurre dentro de las organizaciones y en los hogares. El Bloque C hace otra cosa: cruza esos hallazgos con el panorama internacional y pregunta qué significan. No para relativizar lo que encontramos, sino para entender exactamente qué tan grande es la distancia entre donde está la región y donde debería estar.

La respuesta no es alentadora. Pero tampoco es irreversible.

El Bloque A en el análisis transversal

Hallazgo transversal 1 — La región tiene un problema anterior

En América Latina y el Caribe, solo el 13% de los respondentes tiene confianza en la preparación nacional ante un incidente cibernético mayor — la cifra más baja de todas las regiones del mundo. *(WEF Global Cybersecurity Outlook 2026)*

Mientras la agenda global debate cómo optimizar la respuesta ante amenazas avanzadas, la agenda iberoamericana todavía tiene que resolver cuestiones previas: cómo formalizar estrategias que solo existen en el discurso, cómo capacitar a personas que nunca recibieron formación básica, cómo construir confianza institucional en países donde el 76% de las organizaciones no confía en que su Estado esté preparado para protegerlas.

Hallazgo transversal 2 — La invisibilidad del daño

El 12% de las organizaciones participantes no pudo confirmar si fue atacada en el último año. Ese dato, leído junto con el hecho de que el 32% nunca audita y que los

controles predominantes son antivirus y firewall, describe un problema de visibilidad crítico.

El 32% de las organizaciones en América Latina no cuenta con herramientas para confirmar si recibió un ataque cibernético. *(ESET Security Report 2025 LATAM)*

El agravante: el 82% de las detecciones globales en 2025 fueron libres de malware, ejecutadas mediante credenciales válidas por vías autorizadas. Los controles básicos que predominan en la región son ciegos ante esa clase de ataques.

El 82% de las detecciones en 2025 estuvo libre de malware. Los adversarios operaron mediante credenciales válidas y vías autorizadas, mezclándose con la actividad normal. *(CrowdStrike Global Threat Report 2026)*

Hallazgo transversal 3 — El costo subestimado

El costo promedio global de una brecha de datos alcanzó USD 4.44 millones en 2025. Las organizaciones que usan IA en ciberseguridad ahorran en promedio USD 1.9 millones por brecha. *(IBM Cost of a Data Breach 2025)*

Para la región, ese dato tiene dos lecturas. El costo real de los incidentes es mayor de lo que las organizaciones registran, porque los incidentes no detectados no entran en ningún cálculo. Y la inteligencia artificial ofrece un retorno concreto y medible en reducción de costos, lo que convierte su adopción en un argumento económico, no solo técnico.

Hallazgo transversal 4 — La brecha de ejecución institucional

Solo 13 de los 30 países de América Latina y el Caribe cuentan con capacidad institucional real para implementar su estrategia nacional de ciberseguridad. Solo 9

están equipados para proteger infraestructura crítica. *(OEA/BID Cybersecurity Report 2025)*

Esa brecha replica, a escala de Estado, exactamente lo mismo que ocurre a escala organizacional: el 77% de las organizaciones tiene la ciberseguridad en su mapa de riesgos, pero solo el 32% está preparado para responder. La distancia entre declarar y ejecutar es el patrón estructural que define a la región.

La mayoría de los países iberoamericanos se ubica en los niveles 3 y 4 del índice global de ciberseguridad, donde las medidas legales están más avanzadas que las capacidades técnicas y organizacionales. *(ITU Global Cybersecurity Index 2024)*

Hallazgo transversal 5 — La IA como acelerador asimétrico

El ransomware afectó al 44% de los incidentes globales. El elemento humano estuvo presente en el 60% de las brechas. La participación de terceros se duplicó, alcanzando el 30% de los casos. *(Verizon DBIR 2025)*

En ese contexto, el 44% de las organizaciones que ya usa IA está mejor posicionado — pero no inmunizado. El 44% que no la usa opera con una desventaja creciente.

Aumento del 89% en ataques habilitados por IA durante 2025. Tiempo promedio de comprometimiento del cibercrimen: 29 minutos. Caso más rápido registrado: 27 segundos. *(CrowdStrike Global Threat Report 2026)*

Una organización sin detección automática ni IA en sus defensas no tiene margen real de respuesta en esas condiciones.

El Bloque B en el análisis transversal

El Bloque B confirma tres cosas que el estudio, sin este componente, no podría afirmar con la misma solidez.

Primero: la brecha de implementación que documenta el Bloque A no empieza en las organizaciones. Empieza mucho antes. Si la mayoría de los adultos que hoy toman decisiones de ciberseguridad no recibió formación sistemática en la escuela ni tuvo en su hogar herramientas de protección digital, es razonable esperar que esa cultura de conciencia sin capacidad se reproduzca en el ámbito profesional.

Segundo: la formación docente es el cuello de botella olvidado de la política pública de ciberseguridad. El 78.67% de los docentes de la región nunca recibió formación en ciudadanía digital. Sin docentes formados, cualquier política de educación digital es estructuralmente inviable.

Tercero: la supervisión parental no puede seguir siendo un acto de fe. El paso que falta no es alertar más — es proveer herramientas y formación para que la supervisión parental pase de ser ocasional y manual a ser continua y asistida técnicamente.

Implicaciones de política pública

Tres áreas no pueden cerrarse desde dentro de las organizaciones — requieren acción del Estado. La primera es la formación: mientras el 21% de los empleados no recibe ninguna capacitación y el 78.67% de los docentes nunca fue formado en ciberseguridad, la brecha de talento no se resuelve con iniciativas voluntarias. Requiere currículos, presupuestos y estándares vinculantes. La segunda es la regulación: no como obstáculo burocrático, sino como el único mecanismo que establece mínimos exigibles para las organizaciones que todavía no han comenzado. La tercera es la coordinación: los sistemas de energía,

telecomunicaciones y finanzas no saben de fronteras. Las respuestas a incidentes críticos, en cambio, sí están fragmentadas por país — y esa asimetría tiene consecuencias reales.

Capítulo 7. Mapa de madurez regional

El mapa de madurez es la síntesis operativa del estudio. Convierte los hallazgos de los tres bloques en un diagnóstico estructurado por dimensiones, que permite identificar con precisión dónde están las brechas más críticas y qué tipo de intervención requiere cada una.

El marco utiliza cuatro niveles: Inicial, En desarrollo, Avanzado y Líder. Cada nivel refleja el grado en que las organizaciones o los sistemas han formalizado, implementado y evaluado sus capacidades en cada dimensión.

Dimensiones consolidadas — Bloques A y C

Dimensión	Nivel	Fuente
Gobernanza y políticas	**En desarrollo**	A + C
Capacidades operativas	**En desarrollo**	A + C
Cultura de ciberseguridad	**En desarrollo**	A + C
Inversión y recursos	**Inicial**	A + C
Coordinación y cooperación regional	**Inicial**	A + C

Dimensiones — Bloque B

Dimensión (Bloque B)	Nivel	Fuente
Cultura digital en el hogar	**En desarrollo**	B
Supervisión y acompañamiento parental	**En desarrollo**	B
Tecnología en el entorno educativo	**Inicial**	B
Exposición a riesgos digitales	**En desarrollo**	B
Capacidades de protección digital	**Inicial**	B

Leído en conjunto, el mapa de madurez regional describe una región que está mayoritariamente en los dos primeros niveles del marco. Ninguna dimensión alcanza el nivel Avanzado de forma generalizada. La región sabe que tiene un problema. El problema es que saberlo no es suficiente.

Capítulo 8. Brechas y hallazgos clave

Tres brechas estructurales atraviesan los bloques del estudio. No son problemas técnicos — son problemas de sistema. Y esa distinción cambia el tipo de respuesta que requieren.

Brecha 1 — La brecha de implementación

El 77% dice que la ciberseguridad está en su agenda. Solo el 60% tiene estrategia formal. Solo el 32% está preparado para responder ante una amenaza avanzada. La distancia entre el primer número y el tercero es la brecha de implementación.

Esta brecha se replica a escala de Estado — solo 13 de 30 países tienen capacidad institucional real — y en el sistema educativo: el 85.5% de los directivos escolares no tiene presupuesto para tecnología segura. La brecha de implementación no se cierra con más documentos. Se cierra con estructuras, presupuesto real y responsabilidades asignadas que se evalúan.

Brecha 2 — La brecha de talento y cultura

El elemento humano estuvo presente en el 60% de las brechas de seguridad registradas globalmente en 2025. *(Verizon DBIR 2025)*

El 21% de las organizaciones no ofrece ninguna formación en ciberseguridad a sus empleados. El 36% capacita a menos del 10% de su personal. Y el 78.67% de los docentes de la región no ha recibido capacitación en ciberseguridad. La brecha de talento no empieza en las organizaciones — empieza en las escuelas.

Brecha 3 — La brecha de visibilidad y medición

El 32% nunca audita sus sistemas. El 12% no pudo confirmar si fue atacada en el último año. El control más extendido — antivirus, firewall, actualizaciones — es insuficiente ante un panorama donde el 82% de los ataques globales son libres de malware.

La falta de visibilidad genera un ciclo que se refuerza: incidentes no detectados, estadísticas subestimadas, políticas basadas en datos incompletos, presupuestos asignados sin diagnóstico real.

Los cinco hallazgos que no deben perderse de vista

H1 — Conciencia sin formalización

El 77% dice que la ciberseguridad está en su agenda, pero el 40% no tiene estrategia formal. El paso que falta no es sensibilizar — es formalizar.

H2 — Dos mundos en una sola muestra

El 45% capacita a más del 50% de su personal. El 36% a menos del 10%. El 21% a nadie. No hay gradiente: hay dos organizaciones completamente distintas que coexisten en la misma región.

H3 — El discurso no alcanza para defenderse

El 32% está preparado para una amenaza avanzada. El 36% parcialmente. El 32% no está preparado. Un tercio en cada categoría, y ninguno de los tres tercios en posición cómoda.

H4 — No saber si te atacaron es tan grave como haber sido atacada

El 12% no pudo confirmar si tuvo incidentes en el último año. La invisibilidad del daño es un problema de gobernanza, no solo de tecnología.

H5 — Las organizaciones no confían en sus países

El 29% de las organizaciones se considera Avanzada o Líder. El 76% califica a su país en Inicial o En desarrollo. Las organizaciones están construyendo capacidades en solitario porque no esperan que el Estado las acompañe.

Capítulo 9. Hipótesis de riesgo y recomendaciones

Las hipótesis que siguen tienen una condición: cada una está anclada en un dato propio del estudio y en al menos una referencia internacional verificada. No son proyecciones de escenario — son trayectorias probables si las brechas identificadas no se cierran. Y cada una cierra con una acción concreta, no con una declaración de intención.

H1 — El costo acumulado superará el costo de prevenir

Si la brecha entre lo que se declara y lo que se ejecuta no se cierra en los próximos 24 meses, el costo acumulado de los incidentes no detectados superará con creces el costo de haber implementado los controles básicos que los habrían prevenido.

El 12% de las organizaciones no puede confirmar si fue atacada — hay incidentes ocurriendo que no se contabilizan en ningún presupuesto de daños. El costo promedio global de una brecha es USD 4.44 millones, y las organizaciones de la región operan sin los controles que reducirían ese costo.

Las organizaciones que utilizan IA en sus operaciones de seguridad ahorran en promedio USD 1.9 millones por brecha. *(IBM Cost of a Data Breach 2025)*

Recomendación: Priorizar la implementación de auditorías anuales en las organizaciones que aún no las realizan — el 32% de la muestra — como primer paso hacia la visibilidad del riesgo real.

H2 — El déficit de talento profundizará la vulnerabilidad

Si el déficit de talento no se atiende de forma sistemática, la región seguirá siendo el flanco más vulnerable del mapa global en un momento en que la demanda de especialistas crece y la oferta formativa no la alcanza.

El 21% no ofrece ninguna formación. El 36% capacita a menos del 10% de su personal. Leídos junto con el hecho de que el elemento humano estuvo presente en el 60% de las brechas globales, esos números definen el riesgo con precisión: enorme superficie de ataque humano, poca inversión en reducirla.

La brecha de habilidades en ciberseguridad creció un 8% entre 2024 y 2025. *(WEF Global Cybersecurity Outlook 2026)*

Recomendación: Desarrollar programas de formación gremial articulados entre ALETI, AMITI y sus organizaciones miembro, con énfasis en los dos grupos extremos — los que no forman a nadie y los que forman con nivel básico.

H3 — Los silos nacionales generarán incidentes regionales sin respuesta conjunta

Si los países siguen construyendo sus estrategias de ciberseguridad en silos nacionales, los próximos incidentes de infraestructura crítica tendrán impacto transfronterizo sin capacidad de respuesta coordinada.

Solo 9 de los 30 países de la región están equipados para proteger infraestructura crítica. En un entorno donde los sistemas de energía, telecomunicaciones y finanzas están interconectados, un incidente en un país puede afectar a los vecinos.

La participación de terceros en los incidentes se duplicó, alcanzando el 30% de los casos registrados. *(Verizon DBIR 2025)*

Recomendación: Impulsar desde ALETI y AMITI, en coordinación con la OEA, el diseño de un protocolo de cooperación ante incidentes de infraestructura crítica.

H4 — La desprotección estructural en el hogar generará adultos digitalmente vulnerables

Los datos del Bloque B revelan que la región gestiona la seguridad de los menores bajo un esquema de voluntarismo que ya no es suficiente ante la sofisticación de las amenazas actuales. La dependencia casi exclusiva de una supervisión parental manual y básica genera un vacío de protección crítico: sin herramientas técnicas automatizadas, las familias pierden la capacidad de detectar o responder a amenazas que ocurren fuera de su vigilancia directa.

Mientras el acceso digital es masivo y temprano, la arquitectura de protección sigue siendo mayoritariamente reactiva. El 82% de los padres aplica supervisión manual; solo el 10% usa controles parentales; el 16% no usa ninguna medida de seguridad.

Recomendación: Migrar de campañas de sensibilización genérica hacia programas que doten a las familias de habilidades técnicas operativas, estandarizando el uso de infraestructuras de protección dinámica — controles parentales, filtros de contenido a nivel de red y autenticación robusta — para transformar la supervisión ocasional en una capa de protección continua.

H5 — El aula como entorno de riesgo institucional desatendido

Existe un profundo desfase operativo-formativo en el sistema educativo regional. Aunque la tecnología se utiliza de forma masiva en el aprendizaje, se hace sin un marco de gobernanza de ciberseguridad claro. La ausencia generalizada de protocolos ante incidentes y la falta de capacitación docente — que supera el 78% en la muestra — convierten a la escuela en un actor pasivo ante el riesgo digital.

Al no existir mecanismos de respuesta institucional, el sistema educativo no solo falla en su deber de cuidado, sino que traslada una carga de gestión de crisis a los hogares que estos no están preparados para manejar.

Recomendación: Establecer protocolos obligatorios de respuesta ante incidentes digitales — ciberacoso, sextorsión, acceso a contenido nocivo — y vincular formalmente la capacitación en ciudadanía digital con el escalafón y la formación continua del magisterio.

Capítulo 10. Conclusiones y próximos pasos

Empezamos este estudio con una afirmación: las organizaciones de la región saben que tienen un problema. El problema es que saberlo no es suficiente.

Lo que encontramos, a lo largo de 171 respuestas organizacionales en 23 países y 26,958 respuestas de familias, docentes y menores, confirma esa afirmación con datos. Y la profundiza. No es solo que las organizaciones sepan y no actúen — es que el entorno institucional tampoco ha actuado con la velocidad que el problema requiere. Es que la formación no llega a todos. Es que los incidentes no se ven porque no hay herramientas para verlos. Es que la coordinación regional que haría más eficiente cualquier esfuerzo individual todavía no existe.

Ese es el diagnóstico. No es alentador. Pero tampoco es el punto final.

Lo que este estudio aporta

Por primera vez, la región iberoamericana tiene un diagnóstico propio de su madurez en ciberseguridad — construido con datos propios, entre respondentes con responsabilidad real, y complementado con la voz directa de familias, docentes, directivos escolares, adolescentes y niños.

Lo que encontramos no es un conjunto de problemas aislados. Son cinco brechas que se alimentan entre sí: implementación, talento, visibilidad, protección familiar y formación educativa. Ninguna se cierra si las otras permanecen abiertas. Y ninguna se cierra sola. Requieren acción coordinada, voluntad real de medir y la honestidad de reconocer que declarar no es lo mismo que ejecutar.

Lo que viene después

La presentación regional del estudio, programada para la semana del 21 de mayo de 2026, es un punto de partida — no de llegada. Hay cuatro rutas de activación que los datos permiten sostener con evidencia: la agenda de política pública, la formación gremial, la cooperación regional y la continuidad del estudio como serie longitudinal.

La segunda edición: una decisión que hay que tomar hoy

De los 171 respondentes del Bloque A, 111 manifestaron interés en participar en ediciones futuras. Ese es el núcleo de un panel longitudinal que permitiría medir, con las mismas organizaciones, si las brechas se están cerrando o ampliando.

Las preguntas sobre la segunda edición — recurrencia, alcance, financiamiento, alianzas — deben empezar a responderse ahora, mientras el estudio está presente en la agenda.

Una nota final

> *Las organizaciones de la región saben que tienen un problema. El problema es que saberlo no es suficiente. Este estudio existe para que dejar de saber sea cada vez más difícil de justificar.*

Ese es el compromiso del Comité de Ciberseguridad de ALETI y de AMITI: no solo documentar el problema, sino construir las condiciones para que la región tenga las herramientas, el talento y la coordinación para empezar a resolverlo.

El diagnóstico está hecho. Lo que sigue depende de todos.

Capítulo 11. Agenda de acción regional

El diagnóstico que produce este estudio no tiene valor si no se traduce en acción. Este capítulo presenta las políticas públicas que los hallazgos del estudio permiten sustentar con evidencia, los acuerdos de colaboración que se proponen como resultado directo del análisis y las acciones concretas que ALETI, AMITI y sus organizaciones miembro pueden impulsar.

Una aclaración necesaria: las recomendaciones que siguen no repiten lo que ya existe. Parten del diagnóstico específico de este estudio — las brechas concretas identificadas, los vacíos que los marcos actuales no cubren, los instrumentos que existen en papel pero carecen de capacidad operativa — y proponen intervenciones dirigidas a cerrar esas brechas específicas.

Políticas públicas que el estudio sustenta

1. Educación digital obligatoria con formación docente vinculante

El problema: el 78.67% de los docentes no ha recibido capacitación en ciberseguridad, y el 85.5% de los directivos escolares no tiene presupuesto para tecnología segura. Las políticas de educación digital existentes en la mayoría de los países iberoamericanos no incluyen la formación docente como requisito vinculante ni establecen presupuestos mínimos institucionales.

La propuesta: reformar los marcos curriculares nacionales para incluir competencias digitales y de ciberseguridad como contenido obligatorio en todos los niveles educativos, acompañado de un programa de certificación docente con estándares verificables y financiamiento asignado. Los países que ya tienen marcos de

competencias digitales docentes deben actualizarlos para incluir específicamente ciberseguridad — no solo uso de tecnología.

2. Marco regulatorio mínimo de ciberseguridad para organizaciones

El problema: el 40% de las organizaciones participantes no tiene estrategia formal de ciberseguridad. La regulación existente en la mayoría de los países iberoamericanos establece obligaciones para sectores críticos — banca, energía, telecomunicaciones — pero no define mínimos exigibles para el universo más amplio de organizaciones.

La propuesta: desarrollar marcos regulatorios de ciberseguridad que establezcan mínimos verificables para organizaciones de todos los sectores — no solo los críticos — incluyendo: estrategia documentada, plan de continuidad operativa, auditoría periódica y reporte de incidentes. Estos marcos deben ser graduales en sus exigencias según el tamaño de la organización, para no excluir a las pequeñas y medianas.

3. Protocolo regional de cooperación ante incidentes de infraestructura crítica

El problema: solo 9 de los 30 países de la región están equipados para proteger infraestructura crítica, y no existen mecanismos formales de cooperación transfronteriza ante incidentes de alto impacto. El instrumento que más se aproxima — el Acuerdo de Cooperación en Ciberseguridad de la OEA — carece de protocolos operativos específicos y capacidades de respuesta conjunta.

La propuesta: diseñar, en coordinación con la OEA y los países con mayor capacidad institucional de la región, un protocolo operativo de cooperación ante incidentes que afecten infraestructura crítica transfronteriza. Los países con capacidad avanzada actúan como ancla; los países con menor capacidad se integran de forma gradual.

4. Incentivos para la adopción de tecnologías de protección familiar

El problema: solo el 10% de los padres usa controles parentales y el 3% VPN. Las barreras no son solo de conocimiento — son también económicas y de accesibilidad. Las políticas de protección de menores en línea existentes se enfocan principalmente en penalización de contenido, no en provisión de herramientas.

La propuesta: desarrollar programas de provisión subsidiada o gratuita de herramientas de control parental para familias en situación de vulnerabilidad, acompañados de programas de alfabetización digital para padres y cuidadores. Las políticas de protección de menores deben complementar la regulación de contenido con instrumentación técnica accesible.

Acuerdos de colaboración propuestos

Entre ALETI, AMITI y los ministerios de educación de la región

Para el diseño e implementación de programas de formación docente en ciberseguridad, con estándares comunes y reconocimiento mutuo entre países. El punto de partida puede ser los países con mayor representación en el estudio — México, Panamá, Colombia, Venezuela — y expandirse gradualmente.

Entre ALETI, AMITI y el sector privado tecnológico

Para el desarrollo de una oferta formativa gremial articulada que responda directamente a las brechas identificadas en el estudio. El foco inicial: las organizaciones que forman a menos del 10% de su personal y las que no forman a nadie — más de la mitad de la muestra.

Entre ALETI, AMITI y organismos multilaterales (OEA, BID, CEPAL)

Para la gestión de financiamiento regional destinado a programas de fortalecimiento de capacidades en ciberseguridad, con énfasis en los países con menor representación institucional. El estudio aporta el diagnóstico de base; los organismos multilaterales aportan los instrumentos de financiamiento.

Entre ALETI, AMITI y la academia iberoamericana

Para el desarrollo de programas de formación técnica en ciberseguridad que reduzcan la brecha de talento especializado, con reconocimiento regional de certificaciones y movilidad entre países.

Acciones que ALETI y AMITI pueden impulsar directamente

Panel longitudinal — Segunda edición del estudio

111 de los 171 respondentes organizacionales expresaron interés en participar en ediciones futuras. Activar ese panel para la segunda edición es la acción con mayor retorno inmediato: permite medir el cambio en el tiempo con las mismas organizaciones y construir el único indicador regional verificable de evolución en madurez de ciberseguridad.

Programa de certificación gremial en ciberseguridad

Diseñar y ofrecer a través de las redes de ALETI y AMITI un programa de certificación en ciberseguridad con tres niveles — básico, intermedio y avanzado — que responda directamente al déficit de formación identificado en el Bloque A. La certificación

debe ser accesible, regionalmente reconocida y orientada a la práctica, no a la teoría.

Plataforma regional de inteligencia sobre amenazas

Crear un mecanismo de intercambio de inteligencia sobre amenazas entre las organizaciones miembro de ALETI y AMITI. No requiere infraestructura propia — puede operar como red de intercambio sobre plataformas existentes. El valor es el intercambio sistemático de información sobre incidentes, vectores de ataque y respuestas efectivas.

Landing page pública del estudio con actualización anual

Publicar el estudio de forma abierta y descargable desde una landing page con registro. Los datos de contacto de quienes descarguen el estudio se integran a la base de convocatoria para futuras ediciones, eventos de ALETI y AMITI, y programas de formación. El estudio se actualiza anualmente con los datos del panel longitudinal.

Glosario

Este glosario define los términos técnicos, los acrónimos y los conceptos especializados que aparecen a lo largo del estudio. Su propósito es garantizar que el documento sea accesible para lectores de distintos perfiles — desde directivos empresariales hasta tomadores de decisión en gobierno — sin requerir formación técnica previa en ciberseguridad.

Amenaza avanzada persistente (APT)

Tipo de ataque en el que un actor malicioso obtiene acceso no autorizado a una red y permanece sin ser detectado durante un período prolongado. Generalmente asociado a actores estatales o grupos altamente organizados.

Antivirus

Software diseñado para detectar, prevenir y eliminar programas maliciosos. Es el control de seguridad más básico y extendido, pero insuficiente para detectar amenazas avanzadas que no usan malware tradicional.

Auditoría de seguridad

Proceso sistemático de evaluación de los controles, políticas y prácticas de ciberseguridad de una organización. Puede ser interna o realizada por terceros. Su ausencia es una señal crítica de falta de gestión activa del riesgo.

Bloque A / Bloque B / Bloque C

Denominación de los tres bloques de análisis de este estudio. Bloque A: organizaciones públicas y privadas. Bloque B: niñez, escuelas y familias. Bloque C: análisis transversal y política pública.

Brecha de datos (data breach)

Incidente de seguridad en el que información confidencial o protegida es accedida, divulgada o robada sin autorización. El costo promedio global de una brecha en 2025 fue de USD 4.44 millones (IBM).

Ciberacoso (cyberbullying)

Uso de medios digitales para acosar, amenazar, humillar o intimidar a otra persona. Es uno de los riesgos digitales más frecuentes entre adolescentes.

Control parental

Herramientas o configuraciones tecnológicas que permiten a los padres o cuidadores supervisar, filtrar o limitar el acceso de los niños y adolescentes a contenidos o funciones en dispositivos digitales.

Continuidad operativa (BCP)

Plan que define los procedimientos y recursos necesarios para que una organización pueda continuar funcionando ante un incidente mayor. Su ausencia implica que la organización no tiene respuesta formal ante un ataque grave.

Credenciales válidas

Nombres de usuario y contraseñas legítimos que los atacantes obtienen mediante phishing, robo o compra en mercados ilegales, y usan para acceder a sistemas sin necesidad de malware. El 82% de los ataques globales en 2025 usó este método (CrowdStrike GTR 2026).

CrowdStrike Global Threat Report 2026

Informe anual de la empresa de ciberseguridad CrowdStrike que analiza las amenazas cibernéticas del año anterior. El informe 2026 analiza el panorama de amenazas de 2025 y es uno de los siete reportes de referencia de este estudio.

Ciudadanía digital

Conjunto de habilidades, derechos y responsabilidades que las personas deben desarrollar para participar de forma segura, ética y efectiva en entornos digitales.

Doble autenticación (2FA)

Método de seguridad que requiere dos formas de verificación antes de permitir el acceso a una cuenta o sistema. Reduce significativamente el riesgo de acceso no autorizado.

Firewall

Sistema de seguridad que monitorea y controla el tráfico de red entrante y saliente, basándose en reglas de seguridad predefinidas. Es un control básico de perímetro, insuficiente como única capa de defensa.

Ingeniería social

Técnica de manipulación psicológica que engaña a las personas para que revelen información confidencial o realicen acciones que comprometan la seguridad. El phishing es su forma más común.

Infraestructura crítica

Sistemas y activos físicos y digitales cuya interrupción tendría un impacto grave en la seguridad nacional, la salud pública o la economía. Incluye energía, telecomunicaciones, finanzas, agua y transporte.

Inteligencia artificial (IA) en ciberseguridad

Uso de algoritmos de aprendizaje automático para detectar amenazas, automatizar respuestas y reducir el tiempo de detección y contención de incidentes. Las organizaciones que usan IA ahorran en promedio USD 1.9 millones por brecha (IBM 2025).

ITU Global Cybersecurity Index 2024 (GCI)

Índice publicado por la Unión Internacional de Telecomunicaciones que mide el compromiso de los países con la ciberseguridad en cinco dimensiones: legal, técnica, organizativa, desarrollo de capacidades y cooperación.

Nivel de madurez

En este estudio, categoría que describe el grado de desarrollo de las capacidades de ciberseguridad de una organización o sistema. Los cuatro niveles utilizados son: Inicial, En desarrollo, Avanzado y Líder.

OEA/BID Cybersecurity Report 2025

Informe conjunto de la Organización de los Estados Americanos y el Banco Interamericano de Desarrollo sobre el estado de la ciberseguridad en América Latina y el Caribe. Es uno de los siete reportes de referencia de este estudio.

Phishing

Ataque de ingeniería social que usa comunicaciones falsas — generalmente correos electrónicos — para engañar a las víctimas y obtener información confidencial o acceso a sistemas.

Plan de continuidad (BCP/DRP)

Ver Continuidad operativa.

Ransomware

Tipo de malware que cifra los datos de la víctima y exige un pago (rescate) para restaurar el acceso. Estuvo presente en el 44% de los incidentes globales registrados en 2025 (Verizon DBIR).

SIEM (Security Information and Event Management)

Sistema que recopila y analiza datos de seguridad en tiempo real desde múltiples fuentes, permitiendo la detección temprana de amenazas. Es un control avanzado que solo está presente en organizaciones con capacidades maduras.

SOC (Security Operations Center)

Centro de operaciones de seguridad. Equipo o unidad responsable de monitorear, detectar, analizar y responder a incidentes de ciberseguridad de forma continua.

Sextorsión

Forma de extorsión en la que el atacante amenaza con revelar imágenes o información íntima de la víctima, generalmente obtenidas mediante engaño o robo. Afecta principalmente a adolescentes.

VPN (Virtual Private Network)

Red privada virtual. Tecnología que cifra la conexión a internet del usuario, protegiéndola de interceptaciones. Solo el 3% de los padres encuestados en el Bloque B la utiliza.

WEF Global Cybersecurity Outlook 2025

Informe anual del Foro Económico Mundial sobre el panorama global de ciberseguridad. Es uno de los siete reportes de referencia de este estudio.

Anexo — Resumen de resultados por país

Este anexo presenta los resultados del Bloque A desagregados por país. El nivel de detalle de cada ficha depende del número de respuestas disponibles: ficha completa con nivel de madurez para países con 5 o más respuestas, ficha parcial sin nivel de madurez para países con 3-4 respuestas, y mención en tabla resumen para países con 1-2 respuestas. En todos los casos, los datos son orientativos y no estadísticamente representativos del universo empresarial de cada país.

Fichas completas (n ≥ 5 respuestas)

México · n = 34 respuestas

Indicador	Resultado
Nivel de madurez asignado	En desarrollo
Mapa de riesgos — Sí	85% (29/34)
Estrategia formal — Sí	59% (20/34)
Preparación ante amenazas avanzadas — Sí	26% (9/34)
Preparación — Parcialmente	44% (15/34)
Incidentes confirmados — No	65% (22/34)
Auditorías — Anualmente	44% (15/34)
Nivel formación — Básica predominante	47% (16/34)

México es el país con mayor representación en la muestra y muestra el patrón regional con mayor claridad: alta conciencia del riesgo (85% con mapa de riesgos),

estrategia formal en la mayoría (59%), pero preparación real limitada (solo el 26% está preparado para una amenaza avanzada). La formación está concentrada en nivel básico. La percepción del país es crítica: el 82% califica a México en Inicial o En desarrollo, lo que refleja una brecha significativa entre la autopercepción organizacional y la confianza institucional.

Nota: datos orientativos. n=34, concentrados en organizaciones con presencia en la Encuesta 1 (Bloque A).

Panamá ·n = 28 respuestas

Indicador	Resultado
Nivel de madurez asignado	En desarrollo
Mapa de riesgos — Sí	71% (20/28)
Estrategia formal — Sí	64% (18/28)
Preparación — Sí	43% (12/28)
Incidentes confirmados — No	68% (19/28)
Auditorías — Nunca	39% (11/28)
Madurez org — Avanzado	36% (10/28)

Panamá presenta uno de los perfiles más heterogéneos de la muestra. El 43% dice estar preparado ante amenazas avanzadas — uno de los porcentajes más altos por país — pero el 39% nunca audita, lo que limita la confianza en esa autopercepción. El 36% se ubica en nivel Avanzado organizacionalmente, pero el 89% califica a su país en Inicial o En desarrollo.

Nota: datos orientativos. n=28.

Colombia · n = 27 respuestas

Indicador	Resultado
Nivel de madurez asignado	En desarrollo
Mapa de riesgos — Sí	78% (21/27)
Estrategia formal — Sí	59% (16/27)
Preparación — No	44% (12/27)
Incidentes — No lo sabemos	19% (5/27)
Auditorías — Nunca	37% (10/27)
Formación — Básica predominante	48% (13/27)

Colombia presenta el mayor porcentaje de organizaciones no preparadas (44%) y uno de los porcentajes más altos de incertidumbre sobre incidentes (19% no sabe si fue atacada). El 37% nunca audita. La formación disponible es mayoritariamente básica. El patrón sugiere que la conciencia del riesgo no se ha traducido en inversión real en capacidades.

Nota: datos orientativos. n=27.

Venezuela · n = 15 respuestas

Indicador	Resultado
Nivel de madurez asignado	En desarrollo
Mapa de riesgos — Sí	73% (11/15)
Estrategia formal — Sí	67% (10/15)
Preparación — Sí	40% (6/15)
Incidentes — No	80% (12/15)
Formación — Continua predominante	53% (8/15)
Auditorías — Equilibrado entre niveles	33% cada categoría

Venezuela muestra el perfil de formación más sólido de los países con representación significativa: el 53% ofrece formación continua, frente al predominio de formación básica en el resto. La estrategia formal es alta (67%) y la preparación declarada razonable (40%). El 100% califica a su país en Inicial o En desarrollo, reflejando la brecha entre capacidades organizacionales y contexto institucional.

Nota: datos orientativos. n=15.

Bolivia ·n = 6 respuestas

Indicador	Resultado
Nivel de madurez asignado	Inicial
Mapa de riesgos — Dividido	50% Sí / 50% No
Estrategia formal — Dividida	50% Sí / 50% No

Indicador	Resultado
Preparación — Ninguno Sí	0% preparados
Auditorías — Nunca	67% (4/6)
Formación — Básica predominante	50% (3/6)

Bolivia presenta el perfil de menor madurez entre los países con ficha completa. Ninguna organización respondente se declara preparada para una amenaza avanzada, y el 67% nunca audita. La mitad no tiene estrategia formal ni mapa de riesgos. Los datos son orientativos dado el tamaño de la muestra, pero son consistentes con el contexto institucional del país según el ITU GCI 2024.

Nota: datos orientativos. n=6. Interpretar con cautela.

Guatemala · n = 5 respuestas

Indicador	Resultado
Nivel de madurez asignado	Inicial
Mapa de riesgos — Sí	80% (4/5)
Estrategia formal — No	60% (3/5)
Preparación — Parcialmente	80% (4/5)
Auditorías — Anualmente	60% (3/5)

Guatemala muestra alta conciencia del riesgo (80% con mapa de riesgos) pero baja formalización (60% sin estrategia formal). La preparación declarada es parcial en la

mayoría de los casos. Dado el n=5, estos datos deben interpretarse como señales cualitativas, no como representación del sector.

Nota: datos orientativos. n=5. Interpretar con cautela.

Brasil · n = 21 respuestas (Encuesta 2)

Las 21 respuestas brasileras representan el perfil más corporativo de toda la muestra: el 59% proviene de dirección o alta gerencia, el 27% de responsables de TI o ciberseguridad, y el 64% son organizaciones pequeñas (1–50 colaboradores).

Indicador	Resultado
Nivel de madurez asignado	**En desarrollo**
Mapa de riesgos — Sí	73% (16/22)
Estrategia formal — Sí	55% (6 de 11 con respuesta)
Preparación amenazas — Sí	27% (6/22)
Preparación — Parcialmente	45% (10/22)
IA en ciberseguridad — Sí	55% (12/22) — el más alto de la muestra

Brasil presenta el porcentaje más alto de adopción de IA en ciberseguridad de toda la muestra (55%), por encima del promedio regional del 44%. La formación disponible es relativamente sólida: predomina la formación básica (50%) con una presencia significativa de capacitación continua (32%). Sin embargo, el 41% nunca audita y solo el 27% se declara preparado para amenazas avanzadas. El patrón replica la paradoja regional: mayor adopción tecnológica no garantiza mayor preparación operativa. El 73% califica a Brasil en nivel Inicial o En desarrollo como país.

Nota: datos orientativos. n=21 (Brasil) + 1 (EE.UU.), Encuesta 2. Coordinación: Anna De Lucca.

Fichas parciales (3-4 respuestas)

Los siguientes países tienen entre 3 y 4 respuestas. Se presentan datos cuantitativos básicos sin asignación de nivel de madurez. Los resultados son orientativos y no permiten derivar conclusiones sobre la realidad nacional del sector.

País	n	Estrategia (Sí)	Preparados	Nota de cautela
Ecuador	4	50%	0% preparados	*n insuficiente para conclusiones*
España	4	75%	25% preparados	*n insuficiente para conclusiones*
Perú	3	67%	33% preparados	*n insuficiente para conclusiones*
Chile	3	67%	33% preparados	*n insuficiente para conclusiones*

Tabla resumen (1-2 respuestas)

Los siguientes países tienen entre 1 y 2 respuestas. No se presentan fichas individuales. Su participación enriquece la cobertura geográfica del estudio pero no permite derivar ninguna conclusión sobre su realidad nacional.

País	n	Categoría
El Salvador	2	Iberoamérica
Honduras	2	Iberoamérica
Paraguay	2	Iberoamérica
Argentina	2	Iberoamérica

País	n	Categoría
Puerto Rico	1	Iberoamérica
Uruguay	1	Iberoamérica
Brasil (Enc. 1)	1	Iberoamérica
República Dominicana	1	Iberoamérica
Alemania	1	Participación internacional adicional
Israel	1	Participación internacional adicional
Canadá / EE.UU. (combinado)	1	Participación internacional adicional

> **Nota:** *Brasil suma 21 respuestas adicionales a través de la Encuesta 2 (portugués, Bloque A). Canadá suma 5 respuestas en la Encuesta 1, de las cuales 1 fue registrada como 'Canadá y USA' combinado.*

Referencias

A continuación se listan los reportes internacionales utilizados como fuentes de referencia en este estudio, así como otras fuentes citadas en el texto.

Reportes internacionales de referencia

CrowdStrike (2026). Global Threat Report 2026: El año del adversario evasivo. CrowdStrike. Disponible en: https://www.crowdstrike.com/global-threat-report/

ESET (2025). Security Report 2025 LATAM. ESET Research. Disponible en: https://www.eset.com/latam/

IBM Security (2025). Cost of a Data Breach Report 2025. IBM Corporation. Disponible en: https://www.ibm.com/security/data-breach

ITU (2024). Global Cybersecurity Index 2024. Unión Internacional de Telecomunicaciones. Disponible en: https://www.itu.int/gci

OEA/BID (2025). Ciberseguridad 2025: América Latina y el Caribe. Organización de los Estados Americanos / Banco Interamericano de Desarrollo.

Verizon (2025). Data Breach Investigations Report (DBIR) 2025. Verizon Communications. Disponible en: https://www.verizon.com/business/resources/reports/dbir/

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

Declaraciones y documentos internacionales

Gobierno de India / Ministerio de Electrónica y TI (2026). New Delhi Declaration on AI Impact. AI Impact Summit 2026, Nueva Delhi, 18-21 de febrero de 2026. Disponible en: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2232005

UIT, UNICEF, UNESCO, OIT et al. (2025). Declaración conjunta sobre inteligencia artificial y derechos del niño. Unión Internacional de Telecomunicaciones, noviembre de 2025.