UNMSM
Fundación
SAN MARCOS
Por el desarrollo de la Ciencia y la Cultura

DIPLOMADO DE ESPECIALIZACIÓN

GESTIÓN DE LA CIBERSEGURIDAD Y PRIVACIDAD

RESUMEN EJECUTIVO

2025 Cybersecurity Report: Vulnerability and Maturity Challenges to Bridging the Gaps in Latin America America and the Caribbean'

JULIO – OCTUBRE 2026

CENCAEP
CAPACITA

RESUMEN EJECUTIVO

Informe sobre ciberseguridad, vulnerabilidades y madurez de capacidades en América Latina y el Caribe — 2025

Documento elaborado a partir del informe Cybersecurity 2025: Vulnerability and Maturity Challenges to Bridging the Gaps in Latin America and the Caribbean, publicado en 2025 por el Banco Interamericano de Desarrollo (BID), en colaboración con la Organización de los Estados Americanos (OEA) y el Global Cyber Security Capacity Centre (GCSCC) de la Universidad de Oxford.

Propósito: *Presentar las principales conclusiones, tendencias y desafíos identificados en el informe, con el objetivo de facilitar una comprensión integral de la situación actual de la región y de los factores que condicionan el desarrollo de capacidades nacionales de ciberseguridad. El documento busca relacionar los aspectos estratégicos, institucionales, tecnológicos y humanos de la ciberseguridad con la necesidad de fortalecer la resiliencia de los Estados, organizaciones, infraestructuras críticas y servicios digitales.*

Nota de traducción: *Esta es una traducción/síntesis para fines académicos. La edición en inglés es la edición auténtica, según el aviso de la propia publicación.*

Fuente principal: *Inter-American Development Bank (IDB), Organization of American States (OAS) & Global Cyber Security Capacity Centre, University of Oxford (2025).*

PARTE I

INTRODUCCIÓN

La acelerada transformación digital experimentada durante la última década ha cambiado profundamente la manera en que los gobiernos, las empresas y la sociedad interactúan. Los servicios públicos, la banca digital, el comercio electrónico, la salud, la educación, la industria y las infraestructuras críticas dependen cada vez más de plataformas tecnológicas interconectadas. Este nuevo escenario ha generado importantes oportunidades para el desarrollo económico y social; sin embargo, también ha incrementado significativamente la superficie de exposición frente a amenazas cibernéticas.

En este contexto, la ciberseguridad ha dejado de ser una responsabilidad exclusiva de las áreas de tecnología para convertirse en un componente estratégico del desarrollo nacional. Hoy representa un elemento indispensable para garantizar la continuidad de los servicios públicos, proteger los activos digitales del Estado, fortalecer la confianza de los ciudadanos y asegurar la competitividad económica de los países. El informe sostiene que la confianza constituye el verdadero motor de la transformación digital y que dicha confianza solo puede construirse mediante capacidades sólidas de ciberseguridad.

Con esta visión, el Banco Interamericano de Desarrollo (BID), la Organización de los Estados Americanos (OEA) y el Global Cyber Security Capacity Centre (GCSCC) de la Universidad de Oxford desarrollaron el **Cybersecurity Report 2025**, documento que constituye actualmente el diagnóstico más completo sobre el estado de la ciberseguridad en América Latina y el Caribe.

A diferencia de estudios anteriores, esta edición no solo evalúa el nivel de madurez alcanzado por los países, sino que incorpora nuevos factores que están redefiniendo el panorama mundial, como la rápida expansión de la Inteligencia Artificial, la protección de infraestructuras críticas, la cooperación internacional y el fortalecimiento institucional.

El estudio analiza la situación de **31 países de América Latina y el Caribe**, evaluando su capacidad para prevenir, detectar, responder y

recuperarse frente a incidentes cibernéticos mediante la aplicación del **Cybersecurity Capacity Maturity Model (CMM) versión 2021**, considerado uno de los modelos internacionales más reconocidos para medir el desarrollo de capacidades nacionales en materia de ciberseguridad.

LA CIBERSEGURIDAD COMO PILAR DEL DESARROLLO

Uno de los principales aportes del informe consiste en cambiar la percepción tradicional de la ciberseguridad.

Durante muchos años se consideró que la seguridad informática era un asunto exclusivamente técnico, limitado a la protección de redes, servidores y sistemas de información. Actualmente, esa visión resulta insuficiente.

El informe plantea que la ciberseguridad constituye un habilitador del desarrollo económico, de la gobernanza digital y de la estabilidad democrática. Sin instituciones seguras no es posible consolidar gobiernos digitales, atraer inversiones, impulsar la innovación tecnológica ni ofrecer servicios públicos confiables.

La digitalización de las economías latinoamericanas incrementa permanentemente la dependencia de sistemas informáticos. Cuando estos sistemas son comprometidos, las consecuencias trascienden el ámbito tecnológico y afectan directamente la economía, la salud pública, la seguridad ciudadana y la confianza institucional.

Los ataques registrados durante los últimos años contra ministerios de finanzas, hospitales, puertos, sistemas tributarios y empresas proveedoras de servicios esenciales demuestran que los ciberdelincuentes ya no buscan únicamente obtener beneficios económicos, sino también generar interrupciones operativas capaces de afectar el funcionamiento de los Estados.

Por esta razón, el informe sostiene que la inversión en ciberseguridad debe entenderse como una inversión en desarrollo nacional y no únicamente como un gasto tecnológico. Los países que fortalecen sus capacidades institucionales generan mejores condiciones para la inversión privada, promueven economías digitales más competitivas y aumentan la resiliencia frente a crisis nacionales e internacionales.

PRINCIPALES HALLAZGOS DEL INFORME 2025

Uno de los mensajes más contundentes del estudio es que América Latina y el Caribe han logrado avances importantes desde la publicación del informe de 2020, aunque dichos avances continúan siendo insuficientes frente al crecimiento acelerado de las amenazas cibernéticas.

En términos generales, la mayoría de los países ya dispone de estrategias nacionales de ciberseguridad o se encuentra en proceso de elaboración de estas políticas públicas. Sin embargo, disponer de una estrategia no garantiza necesariamente la capacidad para implementarla.

El informe identifica una importante brecha entre la formulación de políticas y su ejecución efectiva.

Entre los datos más relevantes destacan los siguientes:

- La mayoría de los países cuenta con estrategias nacionales de ciberseguridad; sin embargo, únicamente un grupo reducido dispone de instituciones con recursos suficientes para implementarlas eficazmente.
- Solo algunos Estados poseen mecanismos consolidados para proteger infraestructuras críticas nacionales.
- Persisten importantes deficiencias en la formación de profesionales especializados.
- Continúan existiendo limitaciones presupuestarias para fortalecer capacidades nacionales.
- La cooperación entre instituciones públicas y privadas todavía presenta niveles de madurez desiguales.
- La velocidad con que evolucionan las amenazas supera la capacidad de respuesta de numerosos gobiernos.

El informe también evidencia que aquellos países que han mantenido políticas sostenidas de inversión en ciberseguridad presentan mejores indicadores de gobierno digital, mayor confianza ciudadana y mejores condiciones para el desarrollo económico.

Uruguay, Chile, Colombia y Costa Rica aparecen como referentes regionales debido al fortalecimiento continuo de sus estrategias nacionales, sus equipos de respuesta a incidentes (CSIRT), sus programas de formación especializada y sus mecanismos de coordinación público-privada.

LA INTELIGENCIA ARTIFICIAL REDEFINE EL PANORAMA DE LA CIBERSEGURIDAD

Uno de los aspectos más novedosos del informe 2025 es el análisis del impacto que la Inteligencia Artificial (IA) está produciendo sobre la seguridad digital.

La IA representa una tecnología transformadora capaz de incrementar significativamente la productividad, automatizar procesos y fortalecer los mecanismos de defensa informática. No obstante, al mismo tiempo introduce nuevos riesgos que modifican profundamente el panorama de amenazas.

El informe explica que los modelos de lenguaje, los sistemas generativos y las aplicaciones basadas en IA están siendo utilizados tanto por organizaciones legítimas como por actores maliciosos.

Los delincuentes pueden emplear estas herramientas para elaborar campañas de phishing altamente personalizadas, generar código malicioso, automatizar el descubrimiento de vulnerabilidades, producir contenidos falsificados mediante *deepfakes* y optimizar ataques de ingeniería social con un nivel de sofisticación sin precedentes.

Asimismo, la propia Inteligencia Artificial constituye un objetivo de ataque.

Los modelos de IA pueden ser manipulados mediante técnicas de envenenamiento de datos (*data poisoning*), inversión de modelos, ataques adversariales y explotación de vulnerabilidades durante los procesos de entrenamiento e inferencia. Estas amenazas adquieren especial relevancia cuando la IA se incorpora a sectores críticos como salud, energía, finanzas, transporte o administración pública.

Frente a este escenario, el informe plantea que los países deben avanzar hacia un nuevo concepto denominado **AI-Cybersecurity**

Readiness o preparación nacional para afrontar los riesgos derivados de la Inteligencia Artificial.

Este enfoque propone fortalecer capacidades en áreas como:

- gobernanza de la IA;
- regulación y marcos normativos;
- gestión nacional de incidentes;
- desarrollo de talento especializado;
- incorporación de estándares técnicos;
- fortalecimiento de la investigación científica;
- concienciación ciudadana;
- cooperación internacional para la gestión de riesgos emergentes.

El informe concluye que ningún país podrá enfrentar de manera aislada los desafíos derivados de la Inteligencia Artificial. La naturaleza global de las cadenas de suministro tecnológico, la interdependencia digital y la rápida evolución de estas tecnologías hacen indispensable una cooperación internacional permanente entre gobiernos, academia, sector privado y organismos multilaterales.

PARTE II

GOBERNANZA, MADUREZ Y DESARROLLO DE CAPACIDADES EN CIBERSEGURIDAD

LA MADUREZ EN CIBERSEGURIDAD: MÁS ALLÁ DE LA TECNOLOGÍA

Uno de los principales aportes metodológicos del informe consiste en demostrar que la capacidad de un país para enfrentar las amenazas cibernéticas no depende exclusivamente de la adquisición de tecnología. Aunque disponer de herramientas avanzadas resulta importante, la experiencia internacional demuestra que los incidentes más graves suelen estar relacionados con deficiencias en la gobernanza, la coordinación institucional, el liderazgo político y la gestión del talento humano.

Desde esta perspectiva, el estudio emplea el **Cybersecurity Capacity Maturity Model (CMM)**, desarrollado por el Global Cyber Security Capacity Centre de la Universidad de Oxford, como instrumento para medir el grado de desarrollo de las capacidades nacionales en materia de ciberseguridad. Este modelo permite evaluar el nivel de preparación de un Estado considerando aspectos institucionales, legales, técnicos, organizacionales y sociales, proporcionando una visión integral de la resiliencia digital de cada país.

El modelo establece cinco niveles progresivos de madurez.

El primero corresponde a la etapa **Inicial (Start-up)**, donde prácticamente no existen políticas, instituciones o capacidades formales relacionadas con la ciberseguridad. En este nivel predominan acciones aisladas y una ausencia casi total de planificación estratégica.

El segundo nivel, denominado **Formativo (Formative)**, refleja el inicio de la construcción de capacidades. Comienzan a desarrollarse iniciativas gubernamentales y algunos mecanismos institucionales, aunque todavía carecen de una estructura consolidada y suelen responder a necesidades inmediatas más que a una planificación de largo plazo.

En el nivel **Establecido (Established)**, las políticas públicas, los marcos regulatorios y las capacidades operativas ya funcionan de manera relativamente organizada. Sin embargo, aún existen limitaciones en la asignación estratégica de recursos y en la integración de todos los actores nacionales.

La cuarta etapa corresponde al nivel **Estratégico (Strategic)**. En este punto, la ciberseguridad deja de ser una función operativa para convertirse en un componente transversal de las políticas nacionales de desarrollo. Las inversiones responden a prioridades claramente definidas y existe coordinación entre instituciones públicas, sector privado, academia y organismos internacionales.

Finalmente, el nivel **Dinámico (Dynamic)** representa el grado más alto de madurez. Los países que alcanzan esta etapa poseen la capacidad de adaptar rápidamente sus estrategias frente a nuevas amenazas, redistribuir recursos de manera eficiente, actualizar permanentemente sus políticas y ejercer liderazgo internacional en materia de ciberseguridad.

El informe evidencia que la mayoría de los países de América Latina y el Caribe aún se encuentran entre los niveles **Formativo** y **Establecido**, mientras que solamente un número reducido ha logrado avanzar hacia niveles estratégicos en determinadas dimensiones.

Esta situación demuestra que el desafío regional ya no consiste únicamente en elaborar estrategias nacionales, sino en consolidar instituciones capaces de ejecutarlas de manera sostenida y adaptarlas a un entorno tecnológico que cambia constantemente.

EL LIDERAZGO POLÍTICO COMO FACTOR DECISIVO

Uno de los mensajes más relevantes del informe es que la ciberseguridad constituye, ante todo, un problema de gobernanza.

Durante muchos años se asumió que las amenazas cibernéticas debían ser gestionadas exclusivamente por especialistas en tecnologías de la información. Sin embargo, la experiencia acumulada durante la última década demuestra que las decisiones

más importantes relacionadas con la protección del ciberespacio dependen de los niveles superiores de gobierno.

Los autores sostienen que ningún país puede desarrollar una estrategia sólida de ciberseguridad sin voluntad política. Son los gobiernos quienes establecen prioridades nacionales, asignan recursos presupuestarios, crean instituciones especializadas, promueven reformas legales y articulan la cooperación entre organismos públicos y privados.

El caso de **Costa Rica**, analizado en el informe, constituye un ejemplo ilustrativo. En 2022, una serie de ataques de ransomware afectó gravemente al Ministerio de Hacienda y a diversas instituciones públicas, comprometiendo la prestación de servicios esenciales y generando importantes pérdidas económicas. La magnitud del incidente llevó al gobierno costarricense a declarar, por primera vez en la historia, un estado de emergencia nacional provocado por un ciberataque.

Más allá de la gravedad del episodio, el informe destaca la respuesta institucional posterior. El país fortaleció su modelo de gobernanza, creó un centro centralizado de operaciones de seguridad y revisó sus mecanismos nacionales de respuesta a incidentes. Este proceso evidencia que las crisis pueden convertirse en oportunidades para acelerar la madurez institucional cuando existe liderazgo político y capacidad para aprender de la experiencia.

En contraste, numerosos países continúan enfrentando limitaciones relacionadas con presupuestos insuficientes, cambios frecuentes de autoridades, escasa continuidad en las políticas públicas y baja prioridad otorgada a la ciberseguridad dentro de las agendas nacionales.

El informe concluye que la resiliencia digital comienza en el más alto nivel de decisión política y que ninguna infraestructura tecnológica puede compensar la ausencia de liderazgo estratégico.

LA CAPACIDAD DE APRENDER: EL CONCEPTO DE "ABSORPTIVE CAPACITY"

Uno de los conceptos más innovadores desarrollados en el informe es el de **Capacidad de Absorción** (*Absorptive Capacity*).

Este término hace referencia a la habilidad que poseen las organizaciones y los Estados para incorporar nuevos conocimientos, adoptar tecnologías emergentes, aprender de experiencias nacionales e internacionales y transformar ese aprendizaje en mejoras concretas de sus capacidades institucionales.

En el ámbito de la ciberseguridad, esta capacidad resulta especialmente importante debido a que las amenazas evolucionan con enorme rapidez. Las herramientas utilizadas por los ciberdelincuentes cambian constantemente; aparecen nuevas vulnerabilidades, se desarrollan tecnologías disruptivas y surgen modalidades de ataque que obligan a actualizar permanentemente las estrategias de defensa.

Los autores sostienen que un país con alta capacidad de absorción no solo responde adecuadamente a un incidente, sino que utiliza esa experiencia para fortalecer sus políticas públicas, actualizar protocolos, mejorar la capacitación del personal e incrementar la resiliencia institucional frente a futuros ataques.

Esta visión rompe con los enfoques tradicionales, centrados exclusivamente en la prevención, e incorpora el aprendizaje organizacional como un componente esencial de la seguridad nacional.

Desde una perspectiva académica, este concepto resulta particularmente relevante porque demuestra que la madurez en ciberseguridad no depende únicamente del conocimiento técnico, sino también de la capacidad institucional para adaptarse continuamente a un entorno caracterizado por la incertidumbre.

LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

Uno de los aspectos que mayor preocupación genera en el informe es la limitada capacidad de varios países para proteger sus infraestructuras críticas.

En la actualidad, prácticamente todos los servicios esenciales dependen de sistemas digitales. El suministro de energía eléctrica, los sistemas financieros, las telecomunicaciones, los hospitales, los aeropuertos, los puertos marítimos, el abastecimiento de agua potable y los sistemas tributarios operan mediante plataformas tecnológicas altamente interconectadas.

Esta realidad convierte a dichas infraestructuras en objetivos prioritarios para organizaciones criminales, grupos de ransomware e incluso actores patrocinados por Estados.

El informe señala que, aunque varios países han avanzado en la formulación de estrategias nacionales, el desarrollo de políticas específicas para la protección de infraestructuras críticas continúa siendo limitado. En consecuencia, numerosas organizaciones responsables de servicios esenciales permanecen expuestas frente a amenazas cada vez más sofisticadas.

La protección de estos sectores exige una visión integral que combine tecnologías de detección temprana, protocolos de continuidad operativa, equipos nacionales de respuesta a incidentes (CSIRT), marcos regulatorios actualizados y mecanismos permanentes de intercambio de información entre instituciones públicas y operadores privados.

El informe enfatiza que la continuidad de los servicios esenciales constituye hoy uno de los principales indicadores de resiliencia nacional.

EL DÉFICIT DE TALENTO: LA BRECHA MÁS DIFÍCIL DE CERRAR

Si bien las inversiones en infraestructura tecnológica continúan creciendo en toda la región, el informe identifica una limitación aún más compleja: la insuficiencia de profesionales especializados en ciberseguridad.

La escasez de talento afecta tanto al sector público como al privado y constituye uno de los principales obstáculos para incrementar la resiliencia digital de América Latina y el Caribe.

La formación de especialistas requiere procesos de largo plazo que involucran universidades, centros de investigación, programas de

certificación profesional y mecanismos permanentes de actualización de competencias.

A ello se suma una intensa competencia internacional por captar profesionales altamente calificados, fenómeno que favorece la migración de talento hacia economías con mayores niveles de remuneración e inversión tecnológica.

El informe sostiene que cerrar esta brecha exige una estrategia integral que incluya educación especializada, capacitación continua, fortalecimiento de la investigación aplicada, certificaciones internacionales y políticas públicas orientadas al desarrollo del capital humano. La creación de una cultura nacional de ciberseguridad comienza en las aulas y se consolida mediante el aprendizaje permanente de todos los actores del ecosistema digital.

PARTE III

COOPERACIÓN REGIONAL, TRANSFORMACIÓN DIGITAL Y DESAFÍOS ESTRATÉGICOS DE LA CIBERSEGURIDAD EN AMÉRICA LATINA Y EL CARIBE

LA CIBERSEGURIDAD ES UN DESAFÍO GLOBAL

Uno de los mensajes centrales del informe es que ningún país puede proteger eficazmente su ciberespacio actuando de manera aislada. La naturaleza de Internet, la interconexión de las cadenas de suministro digitales y la actuación transnacional de los grupos criminales hacen que la cooperación internacional deje de ser una opción para convertirse en una necesidad estratégica.

Los ataques cibernéticos actuales no reconocen fronteras políticas. Un grupo de ransomware puede operar desde un continente, utilizar infraestructura ubicada en otro y afectar simultáneamente a organizaciones de varios países. De igual manera, una vulnerabilidad presente en un software ampliamente utilizado puede comprometer miles de organizaciones alrededor del mundo en cuestión de horas.

Esta realidad obliga a los Estados a desarrollar mecanismos permanentes de intercambio de información, coordinación operativa y asistencia mutua. El informe sostiene que la resiliencia digital regional depende, en gran medida, de la capacidad de los países para compartir inteligencia sobre amenazas, coordinar respuestas ante incidentes y armonizar sus marcos regulatorios.

En este contexto, organismos como la Organización de los Estados Americanos (OEA), el Banco Interamericano de Desarrollo (BID), la Universidad de Oxford y otras instituciones multilaterales desempeñan un papel fundamental en el fortalecimiento de capacidades nacionales, la formación de especialistas y la elaboración de políticas públicas basadas en evidencia.

El informe resalta que la cooperación internacional debe evolucionar desde el intercambio ocasional de información hacia verdaderos ecosistemas regionales de confianza, capaces de responder de manera coordinada frente a incidentes de gran magnitud.

LAS REDES REGIONALES COMO MECANISMO DE DEFENSA COLECTIVA

Durante los últimos años América Latina y el Caribe han fortalecido diversas iniciativas de cooperación orientadas al intercambio de conocimientos y al desarrollo conjunto de capacidades.

Una de las más relevantes es la red **CSIRTAméricas**, coordinada por la OEA, que integra equipos nacionales de respuesta a incidentes de múltiples países de la región. Su objetivo consiste en facilitar el intercambio de alertas tempranas, buenas prácticas, indicadores de compromiso y mecanismos de cooperación técnica durante la atención de incidentes cibernéticos.

El informe también destaca el trabajo desarrollado por **CARICOM IMPACS** en el Caribe, orientado al fortalecimiento de las capacidades de investigación de delitos informáticos y a la armonización de la legislación sobre ciberdelincuencia.

Asimismo, resalta iniciativas recientes como el **LAC4 Cyber Competence Centre**, impulsado con apoyo de la Unión Europea; la red académica **Ciberlac**, promovida por el Banco Interamericano de Desarrollo; y la **RedGEALC**, que incorpora la ciberseguridad como un eje transversal dentro del proceso de transformación digital de los gobiernos de la región.

Estas experiencias demuestran que la construcción de capacidades nacionales puede acelerarse significativamente cuando existe cooperación entre gobiernos, universidades, organismos internacionales y sector privado.

TRANSFORMACIÓN DIGITAL Y CIBERSEGURIDAD: DOS PROCESOS INSEPARABLES

El informe sostiene que la transformación digital y la ciberseguridad constituyen procesos inseparables.

Durante muchos años se asumió que primero debía desarrollarse la digitalización de los servicios públicos y posteriormente incorporar medidas de seguridad. Sin embargo, la experiencia internacional ha demostrado que este enfoque genera elevados niveles de vulnerabilidad.

Actualmente, la ciberseguridad debe integrarse desde la fase de diseño de cualquier iniciativa de transformación digital.

Los autores explican que la digitalización está modificando profundamente el funcionamiento de sectores estratégicos como energía, transporte, salud, educación, justicia, finanzas y administración pública. La incorporación de inteligencia artificial, Internet de las Cosas, computación en la nube, análisis masivo de datos y automatización de procesos incrementa considerablemente la eficiencia institucional, pero también amplía la superficie de ataque disponible para actores maliciosos.

En consecuencia, la confianza digital se convierte en un activo estratégico.

Cuando ciudadanos y empresas perciben que los servicios digitales son seguros, aumenta su utilización, se fortalece la economía digital y mejora la relación entre el Estado y la sociedad.

Por el contrario, incidentes graves de seguridad pueden generar pérdida de confianza, reducción en el uso de plataformas digitales, afectación económica y deterioro de la legitimidad institucional.

El informe concluye que la ciberseguridad debe ser entendida como un habilitador del desarrollo digital y no como un requisito técnico adicional.

LOS PRINCIPALES DESAFÍOS QUE ENFRENTA LA REGIÓN

El análisis realizado por el BID, la OEA y la Universidad de Oxford permite identificar varios desafíos estructurales que limitan el avance de América Latina y el Caribe hacia mayores niveles de madurez en ciberseguridad.

El primero corresponde a la persistencia de importantes diferencias entre los países de la región. Mientras algunas naciones han consolidado instituciones especializadas, equipos nacionales de respuesta y marcos regulatorios modernos, otras aún enfrentan limitaciones significativas relacionadas con recursos financieros, infraestructura tecnológica y disponibilidad de talento especializado.

Un segundo desafío es la velocidad con la que evolucionan las amenazas. El desarrollo de la inteligencia artificial, la automatización de ataques, las campañas avanzadas de ransomware y las nuevas modalidades de ingeniería social exigen procesos permanentes de actualización tecnológica y normativa. Las políticas públicas no pueden mantenerse estáticas frente a un entorno que cambia diariamente.

En tercer lugar, el informe identifica la necesidad de fortalecer la cultura nacional de ciberseguridad. La protección del ciberespacio no depende únicamente de especialistas técnicos; requiere que funcionarios públicos, directivos, empresarios, docentes, estudiantes y ciudadanos comprendan los riesgos asociados al entorno digital y adopten prácticas seguras en sus actividades cotidianas.

Finalmente, el estudio enfatiza que la sostenibilidad de cualquier estrategia nacional dependerá de la inversión continua en educación, investigación científica, innovación tecnológica y desarrollo del capital humano.

RECOMENDACIONES ESTRATÉGICAS DEL INFORME

A partir del análisis de los treinta y un países evaluados, el informe propone diversas líneas de acción orientadas a fortalecer la resiliencia digital de América Latina y el Caribe.

Entre las recomendaciones más relevantes destacan:

- Consolidar la ciberseguridad como una política de Estado respaldada por liderazgo político de alto nivel.
- Fortalecer los marcos legales y regulatorios para responder eficazmente a las nuevas modalidades de ciberdelincuencia.
- Incrementar la inversión pública en infraestructura, investigación y tecnologías de protección digital.
- Desarrollar programas permanentes de formación y certificación de profesionales especializados.
- Promover una cultura nacional de ciberseguridad mediante campañas de sensibilización dirigidas a toda la población.

- Reforzar la cooperación entre gobierno, sector privado, academia y organismos internacionales.
- Incorporar la gestión de riesgos derivados de la Inteligencia Artificial dentro de las estrategias nacionales de ciberseguridad.
- Fortalecer los mecanismos de protección de infraestructuras críticas y de continuidad operativa.
- Impulsar sistemas nacionales de respuesta a incidentes capaces de actuar de manera coordinada frente a amenazas complejas.
- Establecer procesos permanentes de evaluación de la madurez institucional utilizando modelos internacionales como el Cybersecurity Capacity Maturity Model (CMM).

Estas recomendaciones reflejan una visión integral de la ciberseguridad, en la que los aspectos tecnológicos se complementan con dimensiones organizacionales, legales, educativas y de gobernanza.

CONCLUSIONES

El **Cybersecurity Report 2025** constituye uno de los diagnósticos más completos sobre el estado de la ciberseguridad en América Latina y el Caribe. Su principal contribución consiste en demostrar que la resiliencia digital no depende exclusivamente de la incorporación de nuevas tecnologías, sino de la capacidad de los Estados para construir instituciones sólidas, desarrollar talento humano, promover la cooperación internacional y mantener una visión estratégica de largo plazo.

Para quienes se preparan profesionalmente en el campo de la ciberseguridad, este informe ofrece una enseñanza fundamental: proteger el ciberespacio implica comprender la interacción entre tecnología, derecho, políticas públicas, economía, gestión del riesgo y liderazgo institucional. El profesional moderno debe ser capaz de interpretar las amenazas desde una perspectiva multidisciplinaria y participar activamente en la formulación de soluciones que fortalezcan la resiliencia de organizaciones y países.

Asimismo, el estudio pone de manifiesto que la Inteligencia Artificial, la computación en la nube, las infraestructuras críticas y la transformación digital redefinirán el ejercicio profesional durante los próximos años. En este escenario, la actualización permanente del conocimiento dejará de ser una ventaja competitiva para convertirse en una condición indispensable para el desempeño laboral.

Finalmente, el informe transmite un mensaje claro: la ciberseguridad no representa un obstáculo para la innovación, sino el fundamento que hace posible el desarrollo sostenible de la economía digital. Los países que logren integrar la seguridad como parte de su estrategia de transformación tecnológica estarán mejor preparados para proteger a sus ciudadanos, fortalecer sus instituciones y aprovechar plenamente las oportunidades de la revolución digital.