De la seguridad informática a la resiliencia cibernética

25 años de retos y logros.

DOI: 10.29236/sistemas.n175a6

Resumen

Este artículo ofrece una revisión crítica del desarrollo de la ciberseguridad en Colombia durante los últimos 25 años, resaltando su evolución desde enfoques técnicos iniciales hacia una comprensión más estratégica de la resiliencia cibernética. El análisis parte del contexto global, explora los avances en América Latina y aterriza en el caso colombiano, donde actores como la Asociación Colombiana de Ingenieros de Sistemas (ACIS) han jugado un papel clave en la construcción de comunidad técnica, la formación profesional y la divulgación especializada a través de espacios como la Jornada Internacional de Seguridad Informática (JISI).

La transformación digital en Colombia ha traído consigo importantes logros normativos e institucionales, así como nuevos desafíos derivados del uso de tecnologías emergentes y consolidadas como inteligencia artificial, *blockchain*, contratos inteligentes, *machine learning* y *big data & analytics*. Estas herramientas, si bien generan oportunidades, también amplían la superficie de exposición a amenazas cibernéticas cada vez más sofisticadas y persistentes.

El artículo propone una visión prospectiva de la ciber resiliencia, basada en la necesidad de anticiparse a las amenazas, adaptarse continuamente y sostener una cultura de seguridad digital de largo plazo. Se plantean recomendaciones estratégicas orientadas a actualizar el marco normativo, mejorar la coordinación institucional, invertir en talento humano y fomentar la corresponsabilidad entre Estado, sector privado, academia y ciudadanía. Colombia se encuentra en una posición estratégica para liderar, desde América Latina, una transformación digital que no solo sea eficiente, sino también ética, segura y resiliente.

Palabras claves
Ciberseguridad, resiliencia cibernética, transformación digital, tecnologías emergentes, ecosistema digital

Joshsua J. González Díaz

Introducción

"La seguridad no es un producto, es un proceso", Bruce Schneier, criptógrafo y experto en seguridad informática. Esta afirmación de Bruce Schneier, uno de los referentes más influyentes en el campo de la seguridad digital, encapsula una verdad fundamental: la protección de la información no se logra mediante soluciones únicas o definitivas, sino a través de un enfoque continuo y adaptativo. A lo largo de las últimas dos décadas y media, el panorama de la seguridad informática ha experimentado transformaciones significativas, impulsadas por la evolución tecnológica, la creciente interconexión global y la sofisticación de las amenazas cibernéticas.

En este contexto, la noción de resiliencia cibernética ha emergido como un concepto clave. Más allá de la prevención de incidentes, la resiliencia implica la capacidad de las organizaciones y sistemas para anticiparse, resistir, recuperarse y adaptarse frente a adversidades cibernéticas. Este enfoque reconoce que, en un entorno digital en constante cambio, es imposible garantizar una seguridad absoluta; por lo tanto, la adaptabilidad y la preparación para responder eficazmente a incidentes se convierten en elementos esenciales.

En Colombia, la Asociación Colombiana de Ingenieros de Sistemas (ACIS) ha sido protagonista en este proceso de evolución. Desde la primera edición de la Jornada Internacional de Seguridad Informática (JISI) en 2000, ACIS ha liderado iniciativas para promover la concienciа, el conocimiento y la colaboración en torno a la seguridad de la información y la ciberseguridad.

En 2025, la JISI celebrará su vigésima quinta edición, consolidán-

dose como un espacio de referencia para profesionales, académicos y entidades comprometidas con la protección del entorno digital en el país.

A continuación, se ofrece una revisión de los hitos alcanzados, los desafíos actuales y una visión prospectiva de la ciberseguridad y la ciber resiliencia, tanto a nivel internacional como en el contexto colombiano. Se explorarán las tendencias globales, las estrategias adoptadas en América Latina y el papel crucial de ACIS en la promoción de una cultura de seguridad y resiliencia digital en Colombia.

Desarrollo internacional de la seguridad informática hacia la resiliencia cibernética

En las primeras décadas del siglo XXI, el concepto de seguridad informática se consolidó como un componente esencial de los sistemas tecnológicos y de gestión de la información en el ámbito empresarial, gubernamental y social. Inicialmente, este campo se enfocó en proteger la confidencialidad, integridad y disponibilidad de los datos, conocido como el modelo CIA (por sus siglas en inglés). Este enfoque, basado principalmente en la aplicación de controles técnicos como firewalls, antivirus y sistemas de detección de intrusos, fue suficiente durante los primeros años de masificación del acceso a internet y digitalización organizacional (Whitman & Mattord, 2018).

Sin embargo, la evolución de las tecnologías emergentes, la expansión del internet de las cosas (IoT), la migración a la nube, y, sobre todo, el crecimiento exponencial de la superficie de ataque, demostraron las limitaciones de un enfoque puramente defensivo. Las amenazas digitales dejaron de ser incidentes aislados para transformarse en operaciones organizadas, persistentes y cada vez más automatizadas, muchas veces dirigidas por grupos patrocinados por Estados nación o redes criminales transnacionales (Andress, 2021). Esta transformación no solo aumentó la complejidad del entorno digital, sino que generó nuevas exigencias en términos de gestión del riesgo, continuidad operativa y gobernanza de la información.

En este contexto emergió con fuerza el concepto de resiliencia cibernética, un paradigma que supera la lógica de la prevención absoluta y asume que los incidentes de seguridad son inevitables. La resiliencia no se enfoca exclusivamente en evitar ataques, sino en desarrollar capacidades para resistir, responder eficazmente, recuperarse con rapidez y adaptarse de manera sostenida frente a entornos inciertos y disruptivos. De acuerdo con Linkov et al. (2013), la resiliencia se convierte así en un atributo organizacional multidimensional, que abarca desde la infraestructura técnica hasta la cultura corporativa y los procesos de toma de decisiones.

Diversas instituciones internacionales han adoptado y promovido esta visión más holística. Por ejemplo, el *National Institute of Standards and Technology* (NIST) de los Estados Unidos publicó en 2018 su marco de ciberseguridad basado en cinco funciones clave: identificar, proteger, detectar, responder y recuperar. Este modelo no solo ha sido adoptado ampliamente por entidades gubernamentales y privadas, sino que también ha servido como referencia para la formulación de políticas públicas en distintos países (NIST, 2018). De manera similar, el Foro Económico Mundial ha señalado que, en el mundo digital hiperconectado de hoy, los incidentes cibernéticos deben tratarse como eventos sistémicos, que requieren una gobernanza colaborativa, multiactor y transnacional (World Economic Forum, 2020).

Los últimos 15 años han estado marcados por una sucesión de ataques cibernéticos de escala global que revelaron la vulnerabilidad estructural del ecosistema digital. Casos como Stuxnet en 2010, considerado la primera arma digital capaz de sabotear infraestructura crítica, y campañas masivas como *WannaCry* y *NotPetya* en 2017, que comprometieron sistemas de salud, transporte y energía en decenas de países, pusieron en evidencia la rapidez con la que un incidente puede escalar a una crisis de seguridad nacional o incluso internacional (Zetter, 2014). Más recientemente, el caso *SolarWinds* en 2020 expuso las fragilidades de la cadena de suministro digital, demostrando que incluso proveedores de confianza pueden convertirse en vectores de ataques altamente sofisticados (Sanger, Perlroth & Barnes, 2021).

Estos eventos han impulsado una transformación no solo tecnológica, sino también política y estratégica. Países como Estados Unidos, Reino Unido, Alemania y Australia han fortalecido sus estructuras de ciberdefensa, integrando capacidades civiles y militares, y promoviendo alianzas internacionales para el intercambio de inteligencia. La OTAN, por ejemplo, ha reconocido el ciberespacio como un dominio operativo, al mismo nivel que el terrestre, marítimo y aéreo. A la par, organizaciones como la Unión Europea han desarrollado regulaciones como el *Cybersecurity Act* y propuestas para una identidad digital segura y soberana (European Commission, 2020).

A nivel corporativo, la resiliencia cibernética ha dejado de ser una preocupación exclusiva de los departamentos de TI. Los consejos directivos y comités de auditoría exigen hoy estrategias integradas de gestión de riesgos digitales, considerando tanto las amenazas técnicas como las implicaciones reputacionales, legales y financieras.

En este sentido, se reconoce que la cultura organizacional, la educación de los usuarios y la prepara-

ción para incidentes son tan importantes como las herramientas tecnológicas en la defensa del entorno digital (Mitnick & Simon, 2011).

En resumen, el tránsito de la seguridad informática hacia la resiliencia cibernética representa un cambio de paradigma profundo, que redefine las prioridades, capacidades y responsabilidades de los actores en el ciberespacio. Este cambio ha sido impulsado por la aceleración tecnológica, la sofisticación de las amenazas y la creciente interdependencia digital, y requiere un enfoque colaborativo, adaptativo y sostenido. En las siguientes secciones, se analizará cómo estas dinámicas globales se han reflejado en América Latina y, particularmente, en el contexto colombiano.

América Latina: desafíos comunes, respuestas diversas

La evolución de la ciberseguridad en América Latina ha estado marcada por una doble condición: por un lado, la región ha sido testigo y partícipe de la transformación digital global; por otro, ha enfrentado retos estructurales que han dificultado la adopción de políticas y prácticas sólidas en materia de protección digital. Factores como la desigualdad en el acceso a la tecnología, la debilidad institucional en algunos países y la falta de marcos regulatorios actualizados han influido en el desarrollo disparejo de capacidades cibernéticas en la región (OEA & BID, 2020).

En términos generales, los países latinoamericanos comenzaron a formular estrategias nacionales de ciberseguridad a partir de la segunda década del siglo XXI, siguiendo recomendaciones de organismos multilaterales como la Organización de los Estados Americanos (OEA), el Banco Interamericano de Desarrollo (BID) y la Unión Internacional de Telecomunicaciones (UIT). Estas estrategias, en su mayoría, han estado orientadas a fortalecer los marcos normativos, establecer centros de respuesta a incidentes (CSIRT), promover la cooperación internacional y fomentar una cultura de ciberseguridad entre ciudadanos y empresas (UIT, 2021).

Sin embargo, el grado de madurez cibernética en la región es desigual. Mientras que países como Chile, Brasil y Colombia han avanzado en la construcción de capacidades técnicas, normativas e institucionales, otros aún carecen de una estrategia nacional formal o presentan rezagos importantes en cuanto a formación de talento y asignación presupuestaria. El Índice de Ciberseguridad Global de la UIT ubica a América Latina en una posición intermedia respecto a otras regiones del mundo, con importantes brechas internas que reflejan la diversidad de contextos políticos y económicos (UIT, 2021).

Uno de los hitos recientes en la región ha sido el caso de Costa Rica, que en 2022 enfrentó una serie de

ataques de *ransomware* atribuidos al grupo criminal *Conti*. El impacto fue profundo: instituciones gubernamentales como el Ministerio de Hacienda, la Caja Costarricense de Seguro Social y el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) vieron comprometidas sus operaciones durante semanas. Este episodio llevó al gobierno costarricense a declarar el estado de emergencia nacional, convirtiéndose en el primer país del mundo en hacerlo exclusivamente por un ataque cibernético (BBC News Mundo, 2022). El caso de Costa Rica evidenció no solo la creciente amenaza que representan los grupos de *ransomware* en la región, sino también la necesidad urgente de contar con capacidades de respuesta robustas, marcos legales actualizados y una estrategia nacional coordinada que abarque tanto al sector público como al privado.

Al mismo tiempo, el crecimiento de ecosistemas digitales en ciudades como São Paulo, Santiago de Chile, Ciudad de México y Bogotá ha impulsado nuevas preocupaciones en torno a la privacidad de los datos, la protección de infraestructuras críticas y la regulación de tecnologías emergentes como la inteligencia artificial y el big data. La pandemia de COVID-19 aceleró la digitalización de muchos servicios, desde la educación hasta la salud y el comercio electrónico, lo que a su vez amplió la superficie de ataque para actores maliciosos. Según un estudio del BID y Microsoft (2021), el 60 % de las organizaciones encuestadas en América Latina había sufrido al menos un incidente de ciberseguridad durante la pandemia, y una proporción significativa carecía de protocolos de respuesta formales o equipos especializados.

La cooperación internacional ha sido otro eje importante en la construcción de resiliencia regional. Iniciativas como el *Cybersecurity Program* de la OEA, que brinda asistencia técnica, capacitación y acompañamiento en la formulación de políticas públicas, han permitido avanzar en la armonización normativa y la creación de redes regionales de CSIRTs. Asimismo, alianzas con países de la OCDE y convenios bilaterales han abierto canales para el intercambio de inteligencia y buenas prácticas. Sin embargo, persiste el desafío de lograr una cooperación sostenida que trascienda los cambios de gobierno y garantice continuidad en las estrategias nacionales.

Uno de los aspectos críticos en la región es la formación de talento humano especializado. La escasez de profesionales en ciberseguridad es un fenómeno global, pero en América Latina se ve agravado por la falta de programas académicos específicos, la fuga de cerebros hacia mercados más competitivos y la escasa inversión en investigación aplicada. Algunas universidades y centros tecnológicos han comenzado a ofrecer programas de maes-

tría o certificaciones técnicas, pero aún es insuficiente para atender la creciente demanda del sector público y privado (OEA & BID, 2020).

En este complejo escenario, América Latina se encuentra en una encrucijada: el potencial de crecimiento digital es enorme, pero las capacidades para protegerlo son todavía limitadas. La consolidación de una cultura de ciberseguridad y resiliencia en la región requiere voluntad política, inversión sostenida, colaboración internacional y una ciudadanía informada y comprometida. Aunque los avances son notables en algunos países, el desafío sigue siendo convertir la seguridad digital en una prioridad transversal que acompañe el desarrollo económico y social de la región.

Colombia: de la seguridad informática a una estrategia nacional de ciber resiliencia

El desarrollo de la seguridad digital en Colombia ha sido un proceso progresivo que refleja el tránsito desde una visión técnica centrada en la protección de datos e infraestructuras, hacia un enfoque más amplio e integrado de resiliencia cibernética. Este cambio ha implicado no solo una transformación en las políticas públicas y en la gobernanza digital del país, sino también una evolución en los sectores estratégicos como el financiero, donde la gestión del riesgo cibernético se ha convertido en una prioridad nacional.

Durante la década de los 2000, los temas relacionados con la seguridad informática comenzaron a ocupar un lugar creciente en la agenda académica y profesional.

Fue precisamente en este contexto que la Asociación Colombiana de Ingenieros de Sistemas (ACIS) tuvo un papel determinante al impulsar desde el año 2000 la Jornada Internacional de Seguridad Informática (JISI). Este evento se consolidó como un espacio pionero en el país para la discusión de amenazas emergentes, soluciones tecnológicas y tendencias internacionales en ciberseguridad, contribuyendo de manera decisiva a la formación de una comunidad técnica y profesional especializada. En 2025, la JISI alcanzará su vigésima quinta edición, lo que refleja la continuidad y el impacto que esta iniciativa ha tenido en el desarrollo de capacidades en Colombia (ACIS, 2023).

En paralelo, el Estado colombiano comenzó a estructurar una política pública orientada a enfrentar los desafíos del entorno digital. En 2011 se estableció la primera Política Nacional de Seguridad Digital y, posteriormente, en 2016, el documento CONPES 3854 definió lineamientos estratégicos para la protección del ciberespacio nacional. Este documento propuso acciones para la articulación interinstitucional, la creación de capacidades técnicas, la formación de talento humano y la cooperación interna-

cional, elementos fundamentales para fortalecer la seguridad digital en los sectores público y privado (Departamento Nacional de Planeación, 2016).

Uno de los sectores más proactivos en la implementación de estrategias de ciberseguridad ha sido el sector financiero, dada su exposición a riesgos de fraude, fuga de datos y ataques de denegación de servicio. En este ámbito, la Superintendencia Financiera de Colombia (SFC) ha liderado un proceso normativo sostenido y cada vez más robusto. Un primer punto de inflexión fue la emisión de la Circular Externa 052 de 2007, que estableció los requerimientos mínimos en materia de seguridad y calidad para el manejo de la información a través de medios electrónicos, incluyendo aspectos como la autenticación, el cifrado y la trazabilidad de las operaciones digitales.

En años posteriores, la SFC complementó este marco con regulaciones adicionales. La Circular Externa 014 de 2009 reforzó la gestión del Sistema de Control Interno (SCI), incorporando la seguridad de la información como un eje transversal para la mitigación de riesgos operativos. Pero sería en 2018 cuando la Superintendencia dio un paso decisivo con la Circular Externa 007, que estableció lineamientos específicos para la gestión del riesgo de ciberseguridad en las entidades vigiladas. Esta norma definió principios fundamentales como la adopción de una política institucional de ciberseguridad, el diseño de un modelo de prevención y detección de incidentes, la existencia de equipos especializados en gestión de crisis cibernéticas y la obligatoriedad de realizar pruebas de penetración y ejercicios de simulación (Superintendencia Financiera de Colombia, 2018).

Este marco regulatorio ha posicionado a Colombia como uno de los países latinoamericanos con mayores avances normativos en materia de seguridad digital aplicada al sector financiero. La capacidad de anticiparse a los riesgos, implementar estándares internacionales y monitorear de forma continua la superficie de ataque ha sido clave para mantener la confianza en los servicios financieros digitales, cuya adopción se aceleró significativamente a partir de la pandemia de COVID-19. No obstante, persisten desafíos, como la necesidad de fortalecer la ciberseguridad en cooperativas, Fintech y otros actores emergentes del sistema financiero que aún presentan brechas tecnológicas o regulatorias.

Desde el punto de vista institucional, Colombia cuenta con entidades como el Grupo de Respuesta a Emergencias Cibernéticas (colCERT), adscrito al Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), encargado de coordinar la respuesta nacional ante incidentes cibernéticos.

Asimismo, fuerzas como la Policía Nacional y el Comando Conjunto Cibernético (CCOCI) de las Fuerzas Militares han desarrollado capacidades especializadas para enfrentar delitos informáticos, ciberterrorismo y campañas de desinformación. La coordinación entre estos actores, junto con el sector privado, ha sido vital para crear un ecosistema de confianza digital.

En el ámbito normativo más amplio, Colombia ha avanzado en la regulación de temas fundamentales como la protección de datos personales, mediante la Ley 1581 de 2012, y la tipificación de los delitos informáticos, a través de la Ley 1273 de 2009. Sin embargo, estos marcos requieren actualización constante frente al dinamismo de las amenazas y al surgimiento de nuevos desafíos como el uso malicioso de inteligencia artificial, la minería de datos en redes sociales o los riesgos asociados a tecnologías emergentes como *blockchain* y dispositivos IoT.

Finalmente, uno de los elementos más prometedores del proceso colombiano es el fortalecimiento del capital humano. Universidades, centros de investigación y programas públicos han incrementado significativamente la oferta educativa en ciberseguridad, con nuevas maestrías, diplomados y certificaciones técnicas. La colaboración con organizaciones como ACIS ha sido fundamental en este campo, permitiendo que el conocimiento técnico se traduzca en prácticas aplicadas que impactan tanto al sector privado como a la gestión pública.

En conjunto, el caso colombiano ilustra cómo un país puede avanzar en la construcción de una estrategia nacional de ciber resiliencia combinando marcos regulatorios, fortalecimiento institucional, participación del sector privado y formación de talento humano. Si bien los desafíos son persistentes, el país cuenta hoy con una base sólida para afrontar los riesgos del entorno digital y construir una cultura resiliente frente a las amenazas cibernéticas.

Ciber resiliencia en tiempos de incertidumbre: desafíos presentes y escenarios futuros

La ciberseguridad contemporánea ha dejado de ser un componente técnico aislado para convertirse en un eje estratégico que condiciona la estabilidad económica, la seguridad nacional y la confianza en los servicios digitales. En Colombia y América Latina, la digitalización acelerada de servicios públicos, financieros y sociales, junto con la adopción de nuevas tecnologías, ha generado beneficios sustanciales, pero también ha expuesto a gobiernos, empresas y ciudadanos a una serie de amenazas emergentes que evolucionan con rapidez.

Uno de los retos más apremiantes es la integración segura de tecno-

logías emergentes y consolidadas, como inteligencia artificial (IA), *blockchain*, *big data* y analítica avanzada, *machine learning* y *smart contracts*. Estas herramientas han reconfigurado los procesos operativos, la toma de decisiones y los modelos de negocio en múltiples sectores. Sin embargo, su implementación sin una evaluación rigurosa del riesgo puede introducir nuevas vulnerabilidades. Por ejemplo, el uso de contratos inteligentes en ecosistemas financieros descentralizados ofrece automatización y transparencia, pero también puede ser aprovechado por actores maliciosos si existen errores en su programación, ya que son inmutables una vez desplegados (Gordon et al., 2022).

La IA y el aprendizaje automático permiten detectar patrones anómalos, automatizar respuestas ante amenazas y mejorar la eficiencia de los sistemas de defensa cibernética. No obstante, estas mismas tecnologías pueden ser explotadas para crear herramientas ofensivas sofisticadas: malware polimórfico, *phishing* personalizado, e incluso *deepfakes* utilizados para engañar usuarios y manipular decisiones políticas o financieras (Brundage et al., 2018). La falta de regulación específica para estas tecnologías en muchos países latinoamericanos agrava el problema, generando un vacío legal frente a su uso malintencionado.

Simultáneamente, el crecimiento exponencial de los datos, impulsado por el desarrollo de plataformas digitales en salud, educación, finanzas y comercio electrónico, ha consolidado al *big data* y la analítica como herramientas esenciales para el diseño de políticas públicas, segmentación de mercados y vigilancia epidemiológica, entre otros. Pero esta masificación de datos personales también ha incrementado los riesgos de violaciones de privacidad, exfiltración masiva de información y toma de decisiones sesgadas por algoritmos opacos. Sin una arquitectura de gobernanza de datos robusta, la exposición a ciberamenazas se incrementa exponencialmente.

En este entorno de creciente complejidad técnica, el talento humano capacitado se convierte en un activo estratégico. Sin embargo, América Latina enfrenta una brecha estructural en formación de especialistas en ciberseguridad. Según ISACA (2022), la demanda supera ampliamente la oferta, y Colombia no es la excepción. La falta de perfiles en áreas como ciber inteligencia, auditoría de sistemas, seguridad en la nube y análisis forense digital limita la capacidad de respuesta del país frente a incidentes de alto impacto.

Además del reto del talento, persiste una fragmentación institucional. En Colombia, múltiples entidades participan en la gestión de la seguridad digital: el MinTIC, colCERT, el Comando Conjunto Cibernético, la Policía Nacional, la

Superintendencia Financiera y otras agencias sectoriales. Aunque se han dado pasos hacia una mejor coordinación, aún existen vacíos normativos y operativos, solapamientos de funciones y una limitada articulación con el sector privado y académico.

Entre las amenazas más relevantes, destaca la creciente profesionalización del *ransomware* como modelo de negocio criminal. Este tipo de ataques ha pasado de afectar archivos individuales a paralizar operaciones completas de gobiernos y empresas. La experiencia de Costa Rica en 2022, que se vio obligada a declarar el estado de emergencia nacional, es un ejemplo de la magnitud que puede alcanzar este fenómeno (BBC News Mundo, 2022). En Colombia, sectores como salud, banca, educación y gobierno han reportado múltiples intentos de extorsión digital y cifrado de información crítica.

También preocupa la adopción acelerada de tecnologías financieras como billeteras digitales, plataformas de pago instantáneo y servicios Fintech, que, si bien promueven la inclusión financiera, no siempre cuentan con controles de seguridad adecuados. La regulación suele ir por detrás del ritmo de la innovación, lo que expone a los usuarios a fraudes, robo de identidad y pérdida de fondos. En este sentido, entidades como la Superintendencia Financiera han comenzado a establecer lineamientos más claros, como lo demuestra la Circular Externa 007 de 2019, que establece requerimientos mínimos para la gestión del riesgo de ciberseguridad en el sector financiero colombiano (Superintendencia Financiera de Colombia, 2019).

Frente a este panorama, la construcción de resiliencia cibernética debe entenderse como una capacidad dinámica, orientada no solo a proteger activos digitales, sino también a anticipar, resistir, adaptarse y recuperarse ante eventos disruptivos. Esto implica adoptar arquitecturas seguras desde el diseño (*security by design*), realizar ejercicios de simulación de crisis cibernéticas (*cyber range*), e integrar la ciberseguridad en los planes de continuidad del negocio y en las políticas de transformación digital.

En este contexto de desafíos, es necesario proyectar una visión de futuro que trascienda la lógica reactiva y apueste por la transformación digital segura. Esta visión debe estar anclada en tres pilares fundamentales: la anticipación, la adaptabilidad y la sostenibilidad.

La anticipación implica el fortalecimiento de las capacidades de ciber inteligencia, tanto en el sector público como en el privado. Esto significa no solo monitorear amenazas en tiempo real, sino desarrollar una comprensión prospectiva de los riesgos emergentes, como los ataques potenciados por inteligencia artificial, la manipulación de infor-

mación mediante *deepfakes*, o los escenarios de guerra híbrida digital.

La adaptabilidad requiere que las organizaciones cuenten con planes de continuidad del negocio, protocolos de respuesta y recuperación efectivos, y procesos de aprendizaje posteriores a los incidentes. En este sentido, el concepto de ciber resiliencia no se limita a proteger, sino también a transformar: cada incidente debe ser una oportunidad para rediseñar procesos, fortalecer alianzas y mejorar la gobernanza digital.

Finalmente, la sostenibilidad digital implica integrar la ciberseguridad en las estrategias de desarrollo del país. Esto no solo como un componente técnico, sino como un derecho y una responsabilidad compartida. La inclusión de la ciudadanía en la protección del entorno digital, a través de la educación en ciberseguridad desde la escuela hasta el entorno laboral, será clave para crear una cultura resiliente de largo plazo. Organizaciones como ACIS, con su labor de sensibilización, formación técnica y generación de comunidad, tienen aquí un rol cada vez más relevante.

Mirando hacia 2030 y más allá, Colombia necesita consolidar una agenda nacional de resiliencia digital que sea multisectorial, interoperable, centrada en las personas y alineada con estándares internacionales. La participación activa en foros multilaterales, el desarrollo de infraestructuras seguras, la inversión en ciencia y tecnología, y la promoción de la innovación responsable serán elementos clave para garantizar que la transformación digital sea no solo eficiente, sino también confiable y segura. Asimismo, es urgente promover marcos regulatorios que acompañen la innovación sin frenar su desarrollo, garantizando al mismo tiempo principios de seguridad, privacidad, transparencia y rendición de cuentas.

Organizaciones como ACIS, que durante más de dos décadas han liderado la formación y concienciación sobre seguridad digital, juegan un papel clave en esta transición. Su capacidad para articular redes de conocimiento, conectar a profesionales con los desafíos reales del país y promover una cultura de ciberseguridad inclusiva será fundamental en los años por venir.

Conclusiones y recomendaciones estratégicas: hacia una resiliencia digital sostenible

Colombia ha recorrido un camino significativo en las últimas dos décadas, consolidando una visión progresiva de la seguridad digital. Este proceso ha estado marcado por la transición de un enfoque centrado en la seguridad informática tradicional hacia uno más integral: la ciber resiliencia. La evolución normativa, el fortalecimiento insti-

tucional, la consolidación de comunidades profesionales como las promovidas por la Asociación Colombiana de Ingenieros de Sistemas (ACIS), y el avance de estrategias nacionales como el CONPES 3854 de 2016, han sido hitos claves en esta transformación (Departamento Nacional de Planeación, 2016).

Sin embargo, el ritmo acelerado de la digitalización, junto con la adopción de tecnologías como inteligencia artificial, *blockchain*, *big data*, *machine learning* y contratos inteligentes, ha generado una complejidad sin precedentes en el entorno de riesgos. Estas tecnologías, si bien habilitan procesos de innovación, automatización y eficiencia, también amplían la superficie de exposición a amenazas, muchas de las cuales aún están en proceso de comprensión regulatoria, ética y técnica (Brundage et al., 2018; Conti et al., 2018).

Uno de los grandes desafíos consiste en armonizar el marco legal existente con la aparición de estos nuevos modelos tecnológicos. A pesar de los avances logrados con leyes como la 1273 de 2009 sobre delitos informáticos y la 1581 de 2012 sobre protección de datos personales, Colombia necesita incorporar disposiciones más amplias y actualizadas que consideren los riesgos de la inteligencia artificial autónoma, la trazabilidad de datos en *blockchain*, y los vacíos de responsabilidad que emergen de los contratos inteligentes (Superintendencia Financiera de Colombia, 2018; Congreso de Colombia, 2009, 2012).

A nivel institucional, si bien existen múltiples entidades comprometidas con la ciberseguridad —como el MinTIC, colCERT, la Policía Nacional, la SFC y el Comando Conjunto Cibernético— todavía se observan redundancias, descoordinación y vacíos de interoperabilidad que reducen la efectividad de la respuesta nacional ante incidentes. Es fundamental consolidar una arquitectura institucional más integrada, con liderazgo estratégico, visión a largo plazo y articulación intersectorial.

En cuanto al talento humano, la brecha en ciberseguridad sigue siendo preocupante. El déficit de profesionales especializados en Colombia limita la capacidad del país para auditar, prevenir y responder eficazmente a amenazas avanzadas. Esta situación se ve agravada por la migración de talento hacia economías más desarrolladas, la escasa oferta de programas de formación en regiones fuera de los grandes centros urbanos y la falta de incentivos para la investigación aplicada en temas de ciberdefensa (ISACA, 2022).

La incorporación de nuevas tecnologías debe ir acompañada de una visión ética y segura. La seguridad debe pensarse desde la concepción del diseño (*security by design*),

integrando criterios de protección y privacidad desde las etapas tempranas de desarrollo tecnológico. Esto es particularmente relevante en el caso de la inteligencia artificial y los sistemas automatizados, donde decisiones críticas pueden ser tomadas por algoritmos entrenados sobre datos sesgados o manipulados (Gordon et al., 2022; World Economic Forum, 2020).

Por otra parte, se requiere promover una cultura digital basada en la corresponsabilidad. La resiliencia no puede ser entendida únicamente como una competencia institucional; debe involucrar a los ciudadanos, a las empresas, a la academia y a los entes territoriales. La educación en ciberseguridad desde edades tempranas, la alfabetización digital continua y el acceso a información clara y transparente sobre los riesgos del entorno digital son condiciones indispensables para que la resiliencia sea una construcción colectiva y sostenible (Brundage et al., 2018).

Por último, Colombia tiene la capacidad y las condiciones para consolidar un modelo de transformación digital centrado en la seguridad, la confianza y la inclusión. El reto es proyectar esa base hacia una agenda de futuro que combine anticipación, adaptabilidad y sostenibilidad. Actores como ACIS, con su labor continua de formación, articulación y liderazgo, tienen un rol esencial en la construcción de esta visión. Fortalecer la resiliencia digital del país no solo es una necesidad operativa: es una apuesta estratégica por la soberanía tecnológica, la innovación responsable y la confianza en el futuro digital de la nación.

Referencias

ACIS. (2023). Jornada Internacional de Seguridad Informática (JISI). Asociación Colombiana de Ingenieros de Sistemas. https://www.acis.org.co

Andress, J. (2021). The basics of information security: Understanding the fundamentals of InfoSec in theory and practice (3rd ed.). Syngress.

Banco Interamericano de Desarrollo, & Organización de los Estados Americanos (OEA). (2020). Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe. https://publications.iadb.org/

BBC News Mundo. (2022). Costa Rica: cómo fue el ciberataque que llevó al país a declarar el estado de emergencia nacional. https://www.bbc.com/mundo/noticias-america-latina-61332535

BID, & Microsoft. (2021). Ciberseguridad en América Latina y el Caribe: Panorama y desafíos. https://www.microsoft.com/

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. arXiv:1802.07228. https://arxiv.org/abs/1802.07228

Congreso de Colombia. (2009). Ley 1273 de 2009 – Delitos informáticos. Diario Oficial.

Congreso de Colombia. (2012). Ley 1581 de 2012 – Protección de datos personales. Diario Oficial.

Conti, M., Kumar, S., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of blockchain technology. IEEE Communications Surveys & Tutorials, 21(2), 116–145. https://doi.org/10.1109/COMST.2018.2842460

Departamento Nacional de Planeación. (2016). Política Nacional de Seguridad Digital – Documento CONPES 3854. https://colaboracion.dnp.gov.co

European Commission. (2020). Cybersecurity strategy for the digital decade. https://ec.europa.eu

Gordon, W., Werner, J., & Sirer, E. G. (2022). Towards a framework for evaluating the security of smart contracts. ACM Transactions on Internet Technology, 22(1), 1–28. https://doi.org/10.1145/3491224

ISACA. (2022). State of cybersecurity 2022: Global update on workforce efforts, resources and cyberoperations. https://www.isaca.org

Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. Environment Systems and Decisions, 33(4), 471–476. https://doi.org/10.1007/s10669-013-9485-y

MinTIC. (2020). Informe de avances en la política de seguridad digital. Ministerio de Tecnologías de la Información y las Comunicaciones. https://www.mintic.gov.co

Mitnick, K., & Simon, W. L. (2011). The art of deception: Controlling the human element of security. Wiley.

National Institute of Standards and Technology (NIST). (2018). Framework for improving critical infrastructure cybersecurity. https://www.nist.gov/cyberframework

Sanger, D. E., Perlroth, N., & Barnes, J. E. (2021). How the U.S. government hacks the world. The New York Times. https://www.nytimes.com

Superintendencia Financiera de Colombia. (2007). Circular Externa 052 de 2007. https://www.superfinanciera.gov.co

Superintendencia Financiera de Colombia. (2009). Circular Externa 014 de 2009. https://www.superfinanciera.gov.co

Superintendencia Financiera de Colombia. (2018). Circular Externa 007 de 2018. https://www.superfinanciera.gov.co

Unión Internacional de Telecomunicaciones (UIT). (2021). Global cybersecurity index 2020. https://www.itu.int/

Whitman, M. E., & Mattord, H. J. (2018). Principles of information security (6th ed.). Cengage Learning.

World Economic Forum. (2020). Global cybersecurity outlook 2020. https://www.weforum.org

Msc. Joshsua J. González Díaz. *Ingeniero de Sistemas CCNA, CEH, CHFI, ECSA, LPT, CFRI, ISO27001 Lead Auditor, ISO27032 Lead Cybersecurity Manager, Máster en Seguridad de la información. Especialista en Seguridad de la Información. Especialista en Derecho Informático, Pontificia Universidad Javeriana, Universidad de los Andes Universidad Externado de Colombia.*