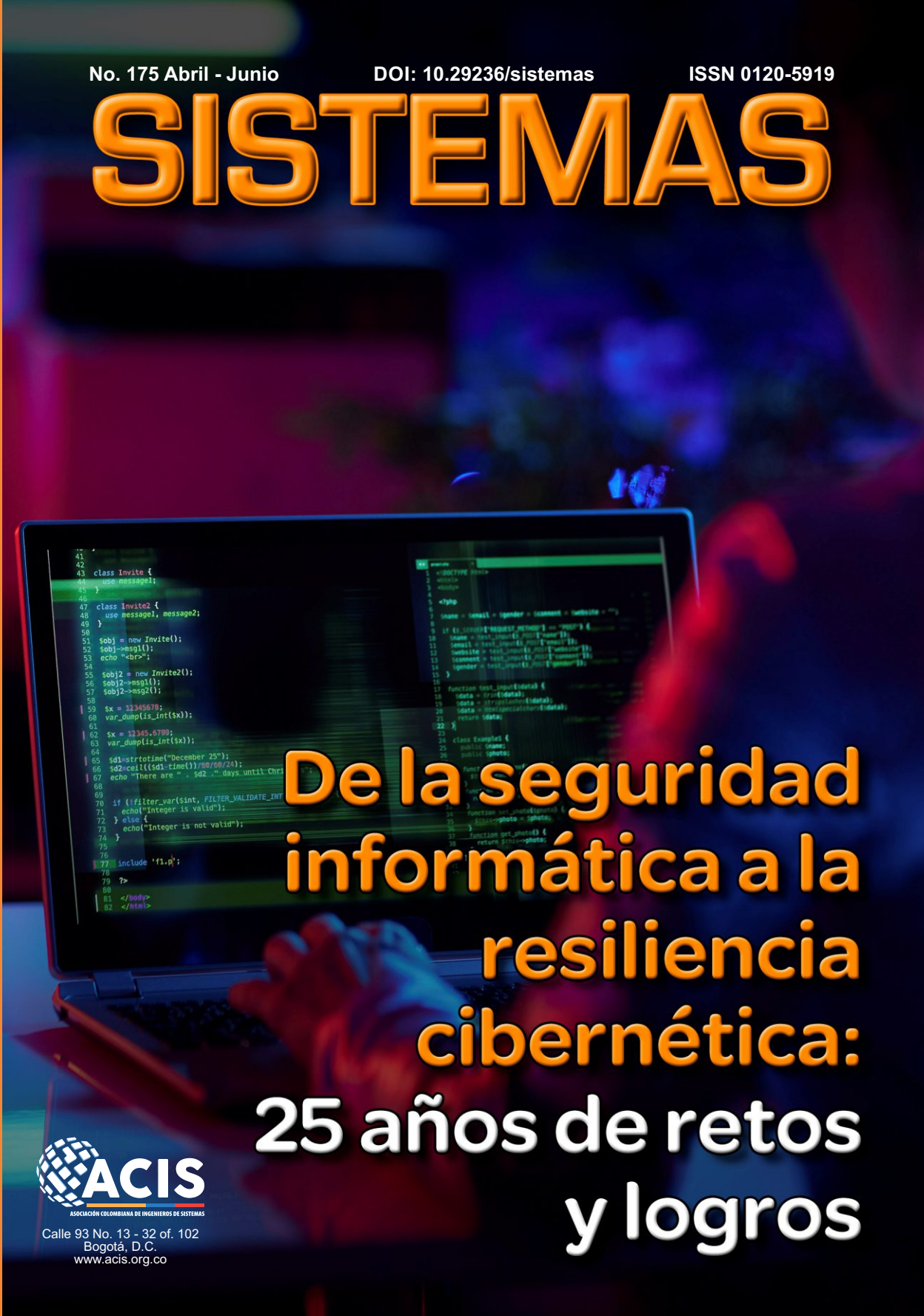
No. 175 Abril - Junio DOI: 10.29236/sistemas ISSN 0120-5919

SISTEMAS



De la seguridad informática a la resiliencia cibernética: 25 años de retos y logros

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS
Calle 93 No. 13 - 32 of. 102
Bogotá, D.C.
www.acis.org.co

REDIS
RED COLOMBIANA DE PROGRAMAS DE INGENIERÍA Y AFINES

ACIS
ASOCIACIÓN COLOMBIANA DE INFORMÁTICA, SISTEMAS Y TECNOLOGÍAS AFINES

Cronograma Maratones de Programción 2025

Programadores de America

Marzo 12 - 22

Salvador do Bahía, Brasil

Training Camp Colombia 2025

Junio 16 - 27

Bogotá, Colombia

ICPC World Finlas 2025

Agosto 31 - Septiembre 5

Bakú, Azerbaiyán

Maratón Nacional 2025

Octubre 18

Bogotá, Medellín, Cali, Bucaramanga, Barranquilla, Manizales

ICPC Latin American Regional 2025

Noviembre 8

20 Países / Bogotá, Colombia

Cronograma CCPL/ICPC 2025

ROUND 1	MARZO 1
ROUND 2	MARZO 22
ROUND 3	ABRIL 12
ROUND 4	MAYO 10
ROUND 5	MAYO 31
ROUND 6	JUNIO 28
ROUND 7	AGOSTO 9
ROUND 8	AGOSTO 30
ROUND 9	SEPTIEMBRE 20
ROUND 10	OCTUBRE 11
ROUND 11	NOVIEMBRE 1

www.acis.org.co/maraton

En esta edición

Publicación de la Asociación Colombiana de Ingenieros de Sistemas (ACIS)
Resolución No. 003983 del Ministerio de Gobierno
Tarifa Postal Reducida Servicios Postales Nacional S.A. No. 2015-186 4-72
ISSN 0120-5919
Apartado Aéreo No. 94334
Bogotá D.C., Colombia

Abril - Junio 2025
Calle 93 No.13 - 32 Of. 102
Teléfonos 616 1407 - 616 1409
A.A. 94334
Bogotá D.C.
www.acis.org.co

ACIS

ASOCIACIÓN COLOMBIANA DE INFORMÁTICA, SISTEMAS Y TECNOLOGÍAS AFINES

XXV JORNADA INTERNACIONAL DE SEGURIDAD INFORMÁTICA

25 Años

Evento presencial

Retando las certezas para anticipar y adaptar el futuro

Universidad Externado de Colombia

¡Vincúlate ahora y sé parte de la JISI 2025!

jisi@acis.org.co

3015530540

Julio 30 y 31 de 2025

Prejornada Julio 29

Postjornada Agosto 1

Apoya

Patrocinadores

Universidad Externado de Colombia – Facultad de Contaduría Pública

SISTANDES – Capítulo de Ingenieros de Sistemas

PATROCINADOR PLATINO MINSAIT

Globaltek · SMARTFENSE · GlobalSuite · GAMMA INGENIEROS · CISO's

https://www.acis.org.co/jisi2025

Editorial

De la seguridad informática a la resiliencia cibernética

DOI: 10.29236/sistemas.n175a1

Andrés Almanza

Hace veinticinco años, cuando se dio inicio a la primera Jornada de Seguridad Informática en Colombia, el panorama digital era muy distinto al que enfrentamos hoy. En aquel entonces, proteger los sistemas informáticos tenían los retos de plantear barreras técnicas tales como antivirus, firewalls, y controles de acceso que en su momento eran los pilares de una estrategia de defensa y control que respondía a un entorno más predecible, con menos volatilidad e incertidumbre.

Como cualquier cosa en la vida el tiempo pasa, la tecnología y las amenazas evolucionaron y más rápido de lo que cualquiera hubiera anticipado.

Hoy, en un contexto marcado por la transformación digital, la hiperconectividad y la sofisticación de los ataques, así como la incertidumbre, volatilidad y fragilidad del ecosistema digital en el que nos encontramos, se entiende que ese solo planteamiento de hablar de la defensa y la seguridad informática, aunque esencial, ya no es suficiente por sí sola. Hoy se ha pasado al concepto de la resiliencia cibernética: una capacidad organizacional y empresarial más integral que no solo busca prevenir incidentes o evitarlos, sino también anticiparlos, adaptarse a ellos, responder con eficacia, recuperarse con agilidad y aprender de ellos, minimizando el impacto sobre la

operación y manteniendo la reputación y protegiendo la confianza de la empresa y las partes interesadas.

Este cambio de enfoque no es meramente técnico; es estratégico. Supone comprender que la ciberseguridad no es un destino, sino un camino en constante adaptación. Implica que las organizaciones, públicas y privadas, deben desarrollar capacidades para operar bajo presión, mantener la continuidad de su negocio y preservar la confianza de sus usuarios y ciudadanos, aun en escenarios adversos, inciertos y complejos.

Colombia no ha sido ajena a esta evolución. A lo largo de estas dos décadas y media, hemos avanzado en marcos regulatorios, en cultura organizacional, en formación de talento, y en el fortalecimiento de las capacidades institucionales.

La Jornada de Seguridad Informática ha sido testigo —y protagonista— de ese avance: un espacio de reflexión, aprendizaje y articulación entre la academia, la industria, el Estado y la sociedad civil.

Sin embargo, los retos que se avecinan son aún más complejos. El auge de la inteligencia artificial, la creciente exposición en la nube, un futuro no muy lejano de la computación quántica, la dependencia de infraestructuras críticas digitales y las tensiones geopolíticas que se trasladan al ciberespacio, nos exigen no solo seguir innovando, sino también integrar la resiliencia como parte central de nuestra visión tecnológica y organizacional. Celebrar estos 25 años no es solo mirar al pasado con orgullo, sino mirar al futuro con responsabilidad.

Desde la seguridad informática hasta la resiliencia cibernética, el verdadero progreso está en nuestra capacidad de adaptarnos, aprender y cooperar. Que este número especial de la revista SISTEMAS sea un homenaje al camino recorrido, y una invitación a seguir construyendo un país más preparado y más resiliente en el contexto digital.

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

Seguridad de la información en los años 80 y 90

DOI: 10.29236/sistemas.n175a2

El objetivo de este artículo es presentar como ha cambiado la Seguridad de la información hasta lo que hoy en día se conoce como la Resiliencia Cibernética. En estos últimos años han crecido exponencialmente las herramientas de hackeo y no se necesita un gran conocimiento técnico para hacer ataques y peor aún con el auge reciente de la Inteligencia Artificial y la Computación Cuántica.

Edilberto Sánchez Perdomo

Computación en los años 80s

En los años 80s los **mainframes** eran muy usados en las multinacionales, gobiernos y bancos. IBM era el principal fabricante con sus sistemas **IBM System/370** y luego **System/390**. Otros fabricantes incluían a Univac, **Honeywell** y **Fujitsu**. Usaban lenguajes de programación como **COBOL**, **Assembler**, **PL/1**, **FORTRAN**; Terminales de texto (como el **IBM 3270**) conectadas mediante redes SNA (Systems Network Architecture). **Sistema operativo MVS (Multiple**

Virtual Storage) de IBM. **Sun Microsystems** no fabricó mainframes, pero fue clave en los 80 y 90 con sus **workstations y servidores UNIX**, especialmente bajo su sistema operativo **Solaris**. Fue pionera en la arquitectura **RISC** (SPARC) y en la promoción del **modelo cliente-servidor**, que fue desplazando a los mainframes en muchos entornos.

Burroughs fue uno de los grandes fabricantes de mainframes, especialmente en los años 60, 70 y hasta mediados de los 80. Sus equipos con fuertes sistemas operativos y software de comunicación como BNA jugaron un papel muy importante en Colombia. Sus sistemas eran populares en el sector bancario y gubernamental, conocidos por su fuerte orientación a la seguridad y la transaccionalidad. En 1986, Burroughs se fusionó con **Sperry** para formar **Unisys**, lo que marcó el declive del nombre "Burroughs", aunque sus mainframes Series A con lenguajes poderosos como BPL y de Cuarta Generación como LINC II continuaron evolucionando bajo la marca Unisys. Finalmente, UNISYS le aposto muy tarde al desarrollo de Internet, pero la competencia con la explosión de Windows y de sistemas operativos basados en Unix como Sun Solaris, RISC 6000 y Linux entre otros tomo mucha ventaja. En esta época la mayoría de entidades usaron Internet para mejorar sus sistemas de Front End desde PCs y grandes granjas de servidores de presentación, pero las grandes bases de datos aun residían en los mainframes y servidores centralizados.

Computación en los años 90s

Para los años 90 IBM System/390 evolucionó con mejor capacidad de procesamiento y soporte para tecnologías como TCP/IP, **Introducción del software cliente-servidor**, pero los mainframes siguieron siendo usados para procesamiento de back-end. **Linux y Unix** empezaron a influir en entornos empresariales, aunque los mainframes se adaptaron integrando entornos virtuales. IBM introdujo **VM/ESA**, que permitía múltiples entornos virtuales en un solo mainframe. **Seguridad y fiabilidad**: Se reforzaron, haciéndolos ideales para banca, seguros y gobiernos. **Interfaces gráficas**: Comenzaron a desarrollarse front-ends en PCs conectados a mainframes a través de redes.

Hackers más famosos de estas décadas

Década de los 80s

1. Kevin Mitnick Apodado “El hacker más buscado del mundo” por el FBI. Se infiltró en sistemas de empresas como Nokia, Motorola y Sun Microsystems.

2. Robert Tappan Morris Creador del Morris Worm (1988), uno de los primeros gusanos en Internet. Su ataque colapsó una gran parte de la red ARPANET.

Década de los 90s

1. Adrian Lamo: Conocido como "el hacker nómada", se infiltró en redes como las de Microsoft y The New York Times. Se volvió famoso también por denunciar a Chelsea Manning por filtrar documentos a WikiLeaks.

2. Vladislav Levin Un hacker ruso que robó alrededor de 10 millones de dólares del Citibank usando acceso remoto a sus sistemas.

3. Mafiaboy (Michael Calce) En 2000, con solo 15 años, lanzó un ataque DDoS que tumbó sitios como Yahoo!, CNN,eBay y Amazon.

El robo al Chase Manhattan Bank

En mayo de 1983, Roberto Soto Prieto lideró el desvío de 13,5 millones de dólares de una cuenta del gobierno colombiano en el Chase Manhattan Bank de Nueva York. Suplantando los télex del Banco de la República, el dinero fue transferido primero al Banco Morgan Guaranty y luego a una cuenta cifrada en Suiza. Este robo fue descubierto en octubre de ese mismo año cuando se detectó la ausencia de fondos en una cuenta estatal. Al principio de este caso el Chase no acepto ningún tipo de responsabilidad. El Banco de la Republica contrato a la empresa Británica Control Risk y se comprobó que el Chase acepto unas claves que no eran válidas. Finalmente, el Chase Manhattan tuvo que asumir el valor de este fraude.

El fraude se realizó suplantando un fax que no tenía nada que ver con los sistemas de cómputo centrales del Banco de la República.

Control Risk recomendó al Banco la creación del área de seguridad informática. En este proceso fui seleccionado por tener el mayor conocimiento de la plataforma del Banco como System Programmer y como no se conocía del tema, visite varias entidades importantes a nivel mundial como el Federal Reserve, Bankers Trust, City Bank of New York, Banamex en México y algunos proveedores de tecnología como Burroughs, Cisco, IBM y otros. El área de seguridad informática cubrió rápidamente todos los niveles físicos y lógicos incluyendo mejoras en la seguridad del centro de cómputo en Bogotá y la creación de centros alternos en Medellín, Cali y Barranquilla para contingencia. Para esa época se estudiaron los niveles de seguridad dados por el departamento de defensa de los Estados Unidos TCSEC (Trusted Computer System Evaluation Criteria) que incluían D1, C1, C2, B1, B2, B3 y A y se decidió que el Banco de la República debía por lo menos tener algunas de las características del nivel C2 y B1 y se llevaron a cabo diferentes proyectos a nivel de Pcs, Unix y Sistemas Series A en primera instancia. Así mismo se escogieron

equipos de encripción a nivel hardware para uno de los proyectos más importantes del Banco como lo fue SEBRA (Servicios Electrónicos del Banco de la Republica).

En los años 80 y 90 los sistemas operativos de los mainframes eran muy complejos de entender y configurar; funcionaban en un esquema centralizado y no distribuidos con terminales brutas, lo que los hacía mucho más seguros. Adicionalmente estaban muy protegidos y de hecho se necesitaba de un especialista System Programmer para poder administrarlo. La mayoría de entidades en el mundo carecían de conocimiento en seguridad de la información y solo los sectores de defensa de países avanzados y algunas multinacionales tenían los recursos para proteger sus sistemas.

De hecho, para esta época se crea el NSA (National Security Agency) y contaba con más de 70.000 ingenieros dedicados a seguridad, así mismo entidades como Shell Company desarrollaron estándares de seguridad como el BS7799, que más tarde se convirtió en el estándar ISO27001.

Ciberseguridad y resiliencia cibernética

Ciberseguridad

También se conoce como la seguridad digital o electrónica y es el conjunto de medidas y prácticas que protegen los sistemas informáticos, las redes y los datos de amenazas y ataques cibernéticos, su objetivo principal es garantizar la confidencialidad, integridad y disponibilidad de la información.

El estándar ISO 27001 del año 2013 se enfocó en los sistemas de información tradicionales de los mainframes sin tener muy en cuenta el auge de Internet y todo el tema de Cloud Computing, Computación en Tabletas y la masificación de Teléfonos inteligentes y Redes Sociales. Ya el estándar ISO27001 en su versión del año 2022 trata con más detalle estos temas de Ciberseguridad incorporando ISO27032 a ISO27001:2022. Afortunadamente en Colombia la Superintendencia Financiera forzó el uso del estándar ISO27001 hace más de 20 años y el sector financiero lo tuvo que implementar para cumplir las normativas de la SFC. En años recientes Gartner Group generó SASE (Secure Access Service Edge) el cual ha servido mucho a todo tipo de entidades para tener una postura concreta de Ciberseguridad así mismo lo hizo NIST Cibersecurity Framework (CSF).

Resiliencia cibernética

Hoy en día, La Resiliencia Cibernética se define como la capacidad de una empresa para prevenir, detectar, responder y recuperarse lo más rápido posible de interrupciones en la Infraestructura Tecnológica, incluyendo ciberataques y otros incidentes.

Industrias más vulnerables hoy en día

Las industrias más vulnerables desde el punto de vista de ciberseguridad suelen ser aquellas que manejan grandes volúmenes de datos sensibles, dependen de sistemas digitales críticos o tienen infraestructuras complejas y desactualizadas. Estas son algunas de las más vulnerables:

1. Salud: Alta cantidad de datos personales y médicos. Uso de dispositivos conectados (IoMT) muchas veces mal protegidos. Infraestructura tecnológica antigua en muchos hospitales.

2. Finanzas y banca: Objetivo frecuente por el acceso a fondos y datos financieros. Amenazas comunes: ransomware, phishing, robo de identidad.

3. Energía y servicios públicos: Infraestructura crítica (redes eléctricas, petróleo, agua). Posibles consecuencias físicas y económicas graves.

4. Educación: Menor inversión en ciberseguridad. Redes amplias con múltiples usuarios y dispositivos.

5. Retail y comercio electrónico: Alto volumen de transacciones y datos de tarjetas de crédito. Vulnerables a ataques de POS y robo de identidad.

6. Gobierno: Datos sensibles de ciudadanos y seguridad nacional. A menudo objetivo de ciber espionaje y ataques patrocinados por estados.

7. Industria manufacturera: Uso creciente de IoT con poca protección. Ataques a la cadena de suministro.

Sistemas operativos, bases de datos y ERP más atacados

Según informes recientes de ciberseguridad (como los de IBM, Verizon y CISA)

Sistemas Operativos

1. Windows (especialmente versiones antiguas como Windows 7, Server 2008): Por su amplia base instalada. Vulnerabilidades conocidas (como EternalBlue).

2. Linux (especialmente en servidores): Aunque más seguro por diseño, sigue siendo atacado por malware como ransomware (ej. Linux.Reptile).

3. Android: Muy atacado en dispositivos móviles por su fragmentación y apps maliciosas.

Bases de Datos

1. Microsoft SQL Server: Ataques de inyección SQL y explotación de puertos abiertos.

2. Oracle Database: Ataques a versiones no actualizadas, explotación de CVEs.

3. MySQL/MariaDB: Blanco común por ser muy popular en entornos web.

4. MongoDB: Casos frecuentes de bases expuestas sin autenticación (ataques ransomware de "exfiltración y extorsión").

ERP

1. SAP: Muchas organizaciones no aplican parches de seguridad a tiempo. Ataques a interfaces mal protegidas (como SAP Gateway o SAPRouter).

2. Oracle E-Business Suite: Foco por ser usado en entornos corporativos críticos.

3. Microsoft Dynamics 365: Vulnerabilidades en la nube o por malas configuraciones.

Algunos ciberataques recientes en Colombia

1. **EPM (Empresas Públicas de Medellín):** En 2019, EPM sufrió un ciberataque que afectó varios de sus sistemas informáticos, lo que provocó la interrupción de algunos servicios públicos y la filtración de datos.

2. **Gobierno colombiano**: En diversas ocasiones, entidades gubernamentales han sido blanco de ciberataques. En 2020, hubo informes de que los sistemas del Gobierno fueron atacados, y varios departamentos de la administración pública sufrieron interrupciones. En septiembre de 2023 las entidades gubernamentales que tenían servicios de hosting con IFX Networks sufrieron un ataque masivo de Ransomware.

3. **Keralty**: En noviembre de 2022 la organización multinacional fue víctima de un ataque de ramsomware que afecto los sitios web y operaciones de la empresa y sus subsidiarias como la EPS Sanitas y su servicio de medicina prepagada Colsanitas, las cuales tardaron más de 4 meses en estabilizar sus servicios.

4. **SURA**: La aseguradora SURA sufrió un ataque en 2020, que afectó sus sistemas operativos. Aunque no hubo grandes filtraciones de información, el incidente afectó la disponibilidad de algunos servicios.

Riesgos futuros de ciberseguridad

Los riesgos futuros de ciberseguridad están evolucionando rápidamente con los avances tecnológicos. Algunos de los más relevantes:

1. **Ataques impulsados por inteligencia artificial (IA):** Los ciberdelincuentes están empe-

zando a usar IA para automatizar ataques, mejorar el phishing, y evadir sistemas de defensa. Los deepfakes también se usarán para fraudes, suplantación de identidad o desinformación.

2. **Amenazas a infraestructuras críticas:** Energía, agua, salud y transporte están cada vez más digitalizados. Un ataque exitoso podría causar apagones, colapsos hospitalarios o accidentes masivos.

3. **Internet de las cosas (IoT) vulnerable:** Dispositivos conectados como cámaras, relojes inteligentes o electrodomésticos pueden ser puertas de entrada para los atacantes si no se protegen adecuadamente.

4. **Cibercrimen como servicio:** Plataformas clandestinas ya ofrecen herramientas y servicios para lanzar ataques sin que el comprador tenga conocimientos técnicos, lo que democratiza el cibercrimen.

5. **Amenazas cuánticas:** Las computadoras cuánticas podrían romper los sistemas de cifrado actuales, comprometiendo datos altamente sensibles.

6. **Filtraciones y ransomware más agresivos:** Las extorsiones digitales seguirán creciendo, con grupos más sofisticados y estrategias dobles: cifrado más publicación de los datos robados.

Algunos grupos de Hackers en el mundo

Existen numerosos grupos de hackers en el mundo, algunos con fines delictivos, otros con motivaciones políticas o activistas. Lista con algunos de los más conocidos, clasificados según su motivación principal:

1. **Ciberdelincuentes (motivación: dinero):** FIN7 (o Carbanak Group): Roban tarjetas de crédito y datos bancarios; han atacado a empresas en todo el mundo. Conti / Ryuk / LockBit: Grupos de ransomware que cifran información y exigen rescate, vinculados con redes criminales organizadas.

2. **Hacktivistas (motivación: ideología):** Anonymous: Red global de hackers sin liderazgo central, famosos por ataques DDoS, filtraciones y campañas contra gobiernos y corporaciones. Killnet: Grupo pro-ruso que ha atacado infraestructuras digitales de países que apoyan a Ucrania. Guacamaya: Hackers latinoamericanos que han filtrado documentos militares de gobiernos en la región (México, Chile, Colombia).

3. **APTs (Amenazas persistentes avanzadas, motivación: espionaje):** APT28 (Fancy Bear):

Vinculado al gobierno ruso (GRU), involucrado en hackeos políticos como el del Comité Demócrata en EE.UU. en 2016. APT29 (Cozy Bear): También asociado a Rusia, experto en ciberespionaje. Lazarus Group: Vinculado a Corea del Norte; responsable del ataque a Sony Pictures y el ransomware WannaCry. Charming Kitten: Asociado a Irán, enfocado en espionaje político y académico. APT41: Vinculado a China; mezcla espionaje estatal con robo financiero.

Herramientas de Hacking ético (O no ético)

Existen muchas herramientas de hacking ético (o no ético) utilizadas para evaluar o comprometer la seguridad de sistemas informáticos.

1. **Recolección de información (OSINT):** Maltego: Visualiza redes y relaciones entre personas, organizaciones o IPs. Recon-ng: Framework en Python para recopilar datos de objetivos desde fuentes públicas. TheHarvester: Extrae correos, dominios, hosts desde buscadores y bases de datos públicas.

2. **Escaneo de vulnerabilidades:** Nmap: Escaneo de puertos, detección de sistemas operativos y servicios activos. Nessus: Escáner de vulnerabilidades profesional, usado por empresas y pentesters. OpenVAS: Escáner de código abierto para detectar fallos de seguridad.

3. **Explotación de vulnerabilidades:** Metasploit Framework: Herramienta poderosa para desarrollar y ejecutar exploits. BeEF (Browser Exploitation Framework): Explotación de vulnerabilidades en navegadores web. SQLmap: Automatiza ataques de inyección SQL para extraer bases de datos.

4. **Ataques de red:** Wireshark: Analizador de tráfico en tiempo real, útil para detectar paquetes sospechosos. Aircrack-ng: Cracking de redes Wi-Fi (WEP/-WPA/WPA2) mediante sniffing y fuerza bruta. Ettercap: Ataques MITM (man-in-the-middle) y sniffing de tráfico en redes LAN.

5. **Ingeniería social y phishing:** Social-Engineer Toolkit (SET): Automatiza la creación de ataques de phishing, clonado de páginas y correos maliciosos. Gophish: Plataforma para simular campañas de phishing de manera ética (usada en pruebas corporativas).

6. **Fuerza bruta y cracking:** Hydra: Herramienta para ataques de fuerza bruta sobre múltiples protocolos (SSH, FTP, HTTP, etc.). John the Ripper: Cracking de contraseñas (archivos hash). Hashcat: Crackeo avanzado de hashes, compatible con GPUs.

Principales tipos de ciberataques con IA

1. **Phishing y Spear Phishing Automatizado:** IA genera correos, chats o mensajes altamente personalizados usando información pública (redes sociales, correos filtrados). Aumenta la tasa de éxito del engaño.

2. **Deepfakes:** Videos o audios falsificados con IA para suplantar identidades (ej. directores financieros o políticos). Se han usado para fraudes bancarios, manipulación mediática y extorsión.

3. **Malware que aprende y se adapta:** IA puede analizar entornos de red y adaptarse para evitar detección. Malware polimórfico: cambia su código o comportamiento usando aprendizaje automático para esquivar antivirus.

4. **Ataques a modelos de IA:** Envenenamiento de datos (data poisoning): insertar datos corruptos durante el entrenamiento de un modelo. Evasión (adversarial attacks): inputs maliciosos diseñados para engañar modelos (ej. visión computarizada, reconocimiento facial).

5. **Automatización de ataques:** Bots inteligentes que escanean redes, encuentran vulnerabilidades y lanzan ataques sin intervención humana. Reducción del tiempo de ataque de días a minutos.

6. **Ataques a sistemas de ciberdefensa basados en IA:** Los atacantes pueden estudiar el comportamiento de sistemas de defensa inteligente para evadir detecciones, “engañarlos” o desactivarlos.

Computación cuántica

La computación cuántica representa una revolución tecnológica con un gran potencial tanto para mejorar como para amenazar la ciberseguridad. Aunque su uso en ataques reales aún es limitado, los expertos coinciden en que su impacto será profundo en los próximos 5 a 10 años.

Posibles usos en ciberataques futuros

1. **Rompimiento de criptografía tradicional:** Los algoritmos de cifrado más comunes hoy (como RSA, ECC) podrían ser rotos en segundos con una computadora cuántica suficientemente potente.

2. **Amenazas a blockchain:** Las criptomonedas y contratos inteligentes que usan algoritmos como SHA-256 o ECDSA pueden volverse vulnerables.

3. **Ataques a firmas digitales y autenticaciones:** Cualquier sistema que use firmas digitales

(correo, software, certificados) corre riesgo de ser falsificado.

4. **Espionaje retroactivo:** Los atacantes podrían estar almacenando comunicaciones cifradas actuales para descifrarlas en el futuro cuando tengan acceso a computadoras cuánticas ("store now, decrypt later").

Recomendaciones básicas

Tener alineados los tres ejes de una empresa (Gente, Procesos y Tecnología) desde el punto de vista de Resiliencia Cibernética

1. **Gente**: Capacitación, sensibilización, entrenamiento y certificaciones
2. **Procesos**: Políticas, Normas, Procedimientos y estándares. Plan Continuidad del Negocio incluyendo DRP, Auditorías y Oficial de seguridad de la información.
3. **Tecnología**: Arquitectura de seguridad basada en SASE de Gartner Group y NIST incluyendo firewalls, End Point Security con antivirus antimalware y DLP para fuga de información, VPNs, Autenticación multifactor, Sistemas de evaluación de compromiso continuo y SOC (Security Operation Center).

***Edilberto Sánchez Perdomo**, (gerencia.lutsagroup@gmail.com). Ingeniero de Sistemas y Computación Universidad de los Andes (1981). CEO lutsa group: Miembro juntas directivas en temas de Ciberseguridad. SGSI basado en ISO27001:2022 para Servimercadeo. Banco de occidente Gerente Auditoría Tecnología. UNISYS Gerente Seguridad Informática LATAM preventa SOC (Reston Virginia); Arquitectura Seguridad Informática ISA; Petrobras (Brasil) cumplimiento ISO 27001; secretaria Seguridad Publica (México) Análisis de Impacto al Negocio; Banesco (Venezuela) Plan Continuidad Negocio. PwC Gerente Technology Risk Services Grupo Aval Modelo seguridad informática para Portal Avalnet, ISA, Conavi, Bancolombia, EPM y Banco de la República system programmer, Creador y director Unidad de Seguridad Informática (1986).*

Patricia Prandini

Es argentina y su tarjeta de presentación una valiosa hoja de vida, evidente durante su amplio recorrido profesional.

DOI: 10.29236/sistemas.n175a3

Sara Gallardo M.

Magister en Seguridad Informática de la Universidad de Buenos Aires (UBA), Máster in Accounting Sciences de Universidad de Illinois, EE-UU y Contadora Pública de la UBA. “Poseo certificaciones en auditoría de sistemas, riesgo y COBIT 2019, todas de ISACA y soy auditora Líder ISO 27001. Trabajo actualmente como asesora en la Dirección Nacional de Ciberseguridad de la Subsecretaría de Tecnologías de Información de la Secretaría de Innovación, Ciencia y Tecnología y soy docente en posgrados en seguridad y auditoría informática de la UBA y la Universidad Nacional de San Martín. Soy actualmente Presidenta de la Red de Universidades Latinoamericanas 'Ciberlac', creada con el objetivo de incrementar las capacidades académicas en materia de Ciberseguridad en las Instituciones de Enseñanza Superior de la Región e impulsada por el Banco Interamericano de Desarrollo (BID)”, así se define.

Así mismo ha sido presidente del Capítulo Buenos Aires de ISACA entre 2010 y 2012 y ha participado en eventos nacionales e internacionales vinculados a ciberseguridad y firma digital. Lleva más de 25 años trabajando en el Estado Nacional de Argentina, durante los cuales ha participado en la creación del primer Grupo de Respuesta a Incidentes de Ciberseguridad (ARCERT) de su país, en el desarrollo e implementación de la infraestructura de Firma Digital nacional y en la creación del primer portal del Estado argentino.

"Mi hobby es viajar, visitar lugares exóticos, conocer la cultura de cada lugar. Esa misma lógica la aplico a la hora de elegir un sitio para disfrutar de un buen plato; soy una fanática tomadora de café –aseguró, declarándose optimista frente al futuro a pesar de los momentos oscuros. Creo en la tecnología, sin desconocer que puede haber un uso malicioso. Y, sobre todo, creo en el ser humano". Después de esta definición personal, entramos de lleno a la entrevista.

Sara Gallardo: *¿Cómo ve la evolución de la seguridad de la información a la ciberseguridad empresarial?*

Patricia Prandini: Creo que refleja un cambio notorio en la forma en que las organizaciones protegen sus activos digitales y colaboran entre ellas. Quiero destacar aquí tres aspectos que me parecen relevantes. Mientras que en seguridad de la información el objetivo es proteger la confidencialidad, integridad y disponibilidad de la información de la entidad, con independencia de formato o soporte utilizado, la ciberseguridad empresarial busca alcanzar la resiliencia operativa. En otras palabras, ante la inevitabilidad del incidente, sea que se trate de una falla en la plataforma o en los servicios tecnológicos o de un ciberataque, la ciberseguridad empresarial se concentra en la capacidad de responder buscando contener el impacto negativo y restablecer el servicio lo antes posible.

Un segundo aspecto que me parece relevante es la atención de los activos críticos. La ciberseguridad se concentra fundamentalmente en los activos de información críticos, es decir, aquellos que conteniendo información o interviniendo en su gestión, tienen más valor para la organización. La seguridad de la información, en cambio, debe preservar la confidencialidad, integridad y disponibilidad de los recursos utilizados, con independencia del formato y soporte en el que se encuentren. Efectivamente, las complejidades de las plataformas actuales, la disrupción que acompaña la aparición de nuevas tecnologías y la notable transformación digital que han experimentado las entidades en estos últimos años, llevan a asegurar la visibilidad y la protección de los activos de información que son considerados esenciales

para la supervivencia y el buen funcionamiento de la entidad.

Finalmente, si bien siguen siendo relevantes el tipo de medida de seguridad a adoptar y la vulnerabilidad que debe ser enfrentada, hoy damos un paso más atrás y el foco está en la predicción del tipo de situación o afectación que podría producirse. Así cobra cada vez más relevancia el campo de la inteligencia de amenazas cibernética; es decir, tratar de visibilizar las situaciones anómalas que pueden producirse antes de que ocurran. Esta visión de nuestra disciplina ha llevado al surgimiento de nuevos marcos, estándares y normas internacionales de gobierno y de gestión, así como técnicos, que muestran que las empresas deben considerar a la ciberseguridad como un tema estratégico y no solo como un "problema técnico". Solo así podrán contribuir a asegurar la continuidad del negocio, la transparencia y la confianza del usuario.

SG: *¿Cuáles elementos de la ciberseguridad hoy son completamente diferentes de lo que se conocía previamente en seguridad de la información?*

PP: Nos encontramos frente a un panorama cambiante y creciente de amenazas. Cambiante porque se recrean riesgos que persisten en cuanto a sus objetivos, pero adquieren nuevas modalidades. Creciente, porque la aparición de nuevas tecnologías y la mayor dependencia que tienen las organizaciones de los datos y de sus plataformas tecnológicas, genera una mayor exposición para la organización. Además, la seguridad de la información buscó siempre proteger el perímetro y su énfasis estaba puesto en el uso de redes internas protegidas. No es que hoy estas problemáticas no existan, pero el panorama es diferente. Hoy las fronteras de la organización se han extendido y ya no es posible limitar las medidas de seguridad a la protección de un lugar físico ni durante un "marco horario" determinado. Se requiere en cambio, una verificación permanente, evitando confiar en los controles existentes. A manera de ejemplo, cada entidad debe autenticarse y autorizarse constantemente, sin importar si está dentro o fuera de la red corporativa.

En cuanto a las infraestructuras tecnológicas, antes eran únicamente "on-premise," con límites y controles físicos y lógicos integrales. Hoy la tecnología de nube, en todas sus modalidades, llegó para quedarse, lo que obliga a extremar el uso del cifrado, de la autenticación federada, etc. Por otra parte, los ciberataques mostraban anteriormente un nivel bajo de sofisticación y la actividad maliciosa estaba en manos de delincuentes aislados. Hoy existe un verdadero mercado de la actividad maliciosa en el que reina el ransomware como servicio, el uso de herramientas de inteligencia artificial para reali-

zar ciberataques, amenazas persistentes avanzadas (APT), bots automatizados o el uso de información falsa para la ingeniería social. También la cantidad de dispositivos se ha diversificado. Mientras antes la seguridad estaba centrada en las computadoras de escritorio y los servidores, hoy deben protegerse miles de dispositivos móviles, sensores de Internet de las cosas y los llamados “endpoints”, lo que trae aparejado nuevos desafíos de visibilidad, autenticación y control.

Para ir cerrando, ha aumentado considerablemente la normativa vinculada a esta temática, generando mayor presión sobre las organizaciones. Hoy existe un verdadero enjambre de regulaciones locales e internacionales que deben ser cumplidas y que las exponen a sanciones de todo tipo y que requieren atención. Las empresas deben pensar la ciberseguridad de manera integral, es decir, considerando no solo la tecnología sino también los procesos y las personas. Son estas últimas quienes configuran, utilizan, desarrollan, implementan y monitorean la información. Efectivamente, son el primer escudo. Por lo tanto, resulta fundamental la generación de una cultura organizacional en torno al riesgo cibernético, centrada en una responsabilidad compartida.

SG: *¿Habría que actualizar las prácticas de seguridad de la información frente a los retos que tienen la empresa en el contexto digital? ¿Cómo se debería hacer ese cambio?*

PP: Sí, es fundamental actualizar las prácticas en torno a la protección de los activos de información frente a los retos del contexto digital actual. Como ya se dijo, las ciberamenazas han cambiado, los entornos tecnológicos también, y los modelos de negocio se han digitalizado. Continuar con prácticas tradicionales deja a las empresas expuestas a riesgos significativos. La transformación digital acelerada de las organizaciones, la disrupción de las nuevas tecnologías, la aparición de ciber amenazas más sofisticadas, el surgimiento de regulaciones más estrictas y mayores expectativas de usuarios y clientes en cuanto a su privacidad, seguridad y transparencia, requiere de nuevas maneras de hacer las cosas. Como todo cambio, debe empezar por un buen diagnóstico y una evaluación del estado actual. En ese proceso, se reconocerán

los riesgos actuales y el nivel de madurez en ciberseguridad de la organización.

Para avanzar, las prácticas deberán tener un enfoque basado en los riesgos a los que se expone la organización y priorizar aquellos que pueden afectar activos críticos. La protección debe centrarse en aquello que más afecta al negocio. En ese camino, será necesario revisar y actualizar periódicamente las políticas de seguridad digital y de uso responsable de la información y de las herramientas tecnológicas, de gestión de contraseñas, de cifrado, de acceso remoto, etc. Como todo proceso de transformación deberá estar acompañado de un cambio cultural que incluya programas de concientización, simulacros de ciber incidentes, talleres de ciberejercicios y la generación de una cultura de ciberseguridad adaptada al negocio. En suma, las prácticas deberán facilitar el establecimiento de un plan de respuesta y resiliencia ante incidentes, que refleje el estado actual del proceso de adopción tecnológica de la organización y proteja en forma efectiva su plataforma tecnológica.

SG: *¿Cómo debería variar la formación de los profesionales de seguridad/ciberseguridad frente a los escenarios que tenemos hoy?*

PP: La formación de los profesionales de seguridad/ciberseguridad debe adaptarse a la realidad y estar a la altura de los desafíos actuales. Ya no basta con saber configurar firewalls o conocer normas nacionales. Hoy se necesita una combinación de habilidades técnicas, estratégicas, legales y personales.

El entorno cambia constantemente. Por lo tanto, se requiere que los programas de estudio reflejen esta gimnasia de adaptación continua y de permanente actitud de alerta y desconfianza. Además, las organizaciones deben comprender que es necesario generar programas formación continua que incluyan laboratorios prácticos, nuevas regulaciones y estándares y un entrenamiento en amenazas emergentes (usos maliciosos de la inteligencia artificial, ransomware como servicio, etc.). El enfoque ha dejado de ser exclusivamente técnico y hoy es multidisciplinario. Como consecuencia, los profesionales deberán formarse en tecnología, administración del negocio, regulación y psicología, entre otras áreas.

Además, ya no existe un único perfil. Se requiere formar especialistas en inteligencia de amenazas, gestión de riesgos cibernéticos, técnicas de ciberataque y defensa, forensia digital, ciberseguridad en la nube, desarrollo seguro, usos ofensivos y defensivos de la inteligencia artificial, ciberseguridad industrial, cumplimiento, auditoría técnica, comunicación efectiva con dirección y con áreas no técnicas, toma de decisiones bajo presión, gestión de crisis y liderazgo en incidentes, por nombrar algunas.

Resumiendo, la formación debe ser ágil, práctica, multidisciplinaria y con una actualización constante. Hoy más que nunca, la ciberseguridad es un campo en donde quien no se actualiza, corre el riesgo de quedar obsoleto rápidamente.

SG: *¿Qué competencias deben cambiar o actualizarse frente al reto de la ciberseguridad empresarial en la actualidad?*

PP: Frente a los retos actuales de la ciberseguridad empresarial, las competencias que se exigen a los profesionales del área deben actualizarse significativamente. Como ya se dijo, no basta con tener habilidades técnicas básicas. Se necesita un perfil integral, adaptable y orientado al negocio. Sea cual fuere el rol que le toque cumplir, debe comprender el negocio, es decir qué hace la organización. Las decisiones que se tomen repercutirán tarde o temprano en la función que debe desempeñar. Y a su vez, el resultado de su trabajo tendrá un efecto sobre el negocio. Además, estará en condiciones de evaluar las posibles repercusiones que un ciberincidente pueden tener a nivel operativo, financiero, reputacional y de toda otra índole. Hecho esto, podrá delinear en forma precisa las acciones que deben ejecutarse para cumplir con los objetivos estratégicos de la empresa.

Asimismo, el profesional debe pasar de un enfoque meramente normativo ("hay que cumplir") a una gestión continua del riesgo de ciberseguridad, en el que la seguridad sea proactiva y no solo reactiva. Debe contar con la capacidad para evaluar y priorizar amenazas, establecer cómo proteger los activos críticos a través de controles eficaces y sostenibles. Además de conocer los riesgos que acompañan toda nueva tecnología, deberá desarrollar también las llamadas "habilidades blandas", vinculadas a la comunicación a no especialistas sobre los riesgos, la redacción de informes y los procesos de toma de decisiones del negocio. Todo esto devendrá en una labor alineada con los objetivos de la organización, que además sea colaborativa, transversal y que favorezca la creación de una cultura de ciber seguridad.

Sara Gallardo M. *Periodista comunicadora, universidad Jorge Tadeo Lozano. Ha sido directora de las revistas Uno y Cero, Gestión empresarial y Acuc Noticias. Editora de Aló Computadores del diario El Tiempo. Redactora en las revistas Cambio 16, Cambio y Clase Empresarial. Coautora del libro "Lo que cuesta el abuso del poder". Ha sido corresponsal de la revista Infochannel de México; de los diarios La Prensa de Panamá y La Prensa Gráfica de El Salvador y corresponsal de la revista IN de Lanchile e investigadora en publicaciones culturales. Se ha desempeñado también como gerente de Comunicaciones y Servicio al Comensal en Inmaculada Guadalupe y amigos en Cía. S.A. (Andrés Carne de Res) y editora de Alfaomega Colombiana S.A. En la actualidad es asesora en escritura y producción de libros y editora de esta revista.*

Encuesta Latinoamericana de Seguridad (ELSI 2025)

Madurez de la ciberseguridad organizacional en América Latina

DOI: 10.29236/sistemas.n175a4

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

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

Introducción

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

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

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

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

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

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

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

Metodología

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

Diseño de la encuesta

La encuesta fue estructurada en torno a siete bloques temáticos:

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

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

Población y muestra

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

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

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

Procesamiento de los datos

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

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

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

Limitaciones

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

Demografía

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

Tamaño de la organización

La distribución según tamaño muestra que:

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

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

Sectores representados

Los principales sectores de actividad representados en la muestra son:

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

Presupuestos

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

Porcentaje del presupuesto global destinado a ciberseguridad

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

Presupuesto en términos absolutos (USD)

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

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

Cruce: Presupuesto ↔ Sector

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

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

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

Tabla 1 Sectores por nivel de inversión

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

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

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

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

Incidentes

Frecuencia de incidentes

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

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

Costos de los incidentes

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

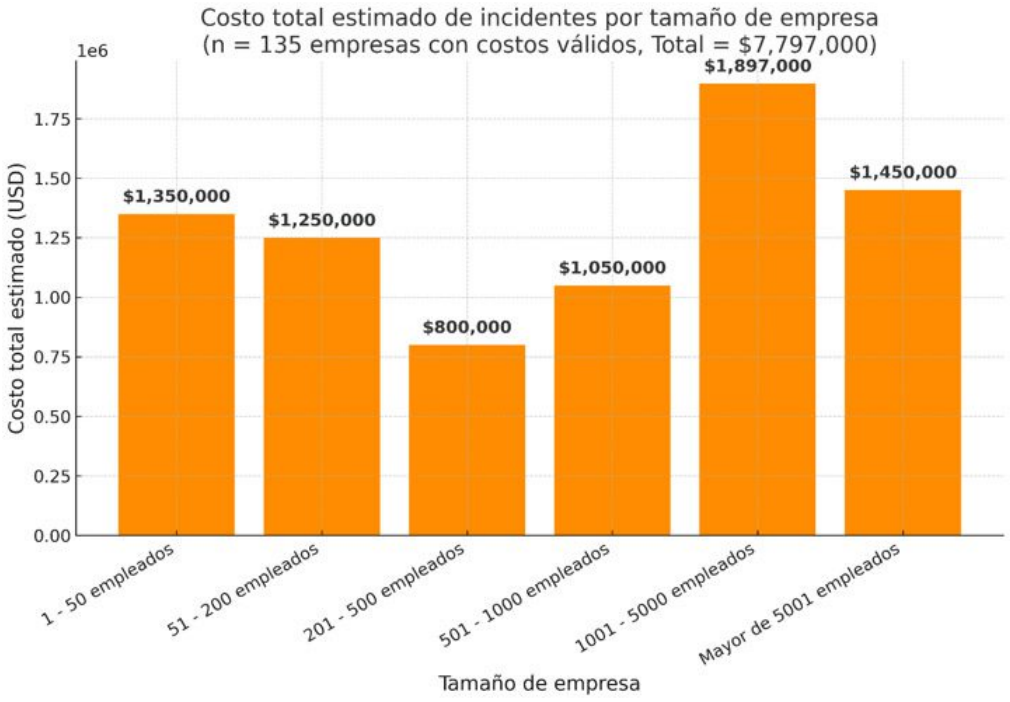
La dificultad para cuantificar con precisión estos costos refuerza la necesidad de desarrollar mejores prácticas de **cuantificación de riesgos cibernéticos** (*IBM, 2024; ENISA, 2025; FBI 2025*), sin embargo, se ha avanzado en usar métodos que al menos ayuden a las empresas a poder hacer la labor de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

un 15% según PwC (2024) realiza cuantificación.

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

Impacto económico general de los incidentes

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



Gráfica 1 Costos de incidentes x tamaños de empresa

Tipos de incidentes más frecuentes

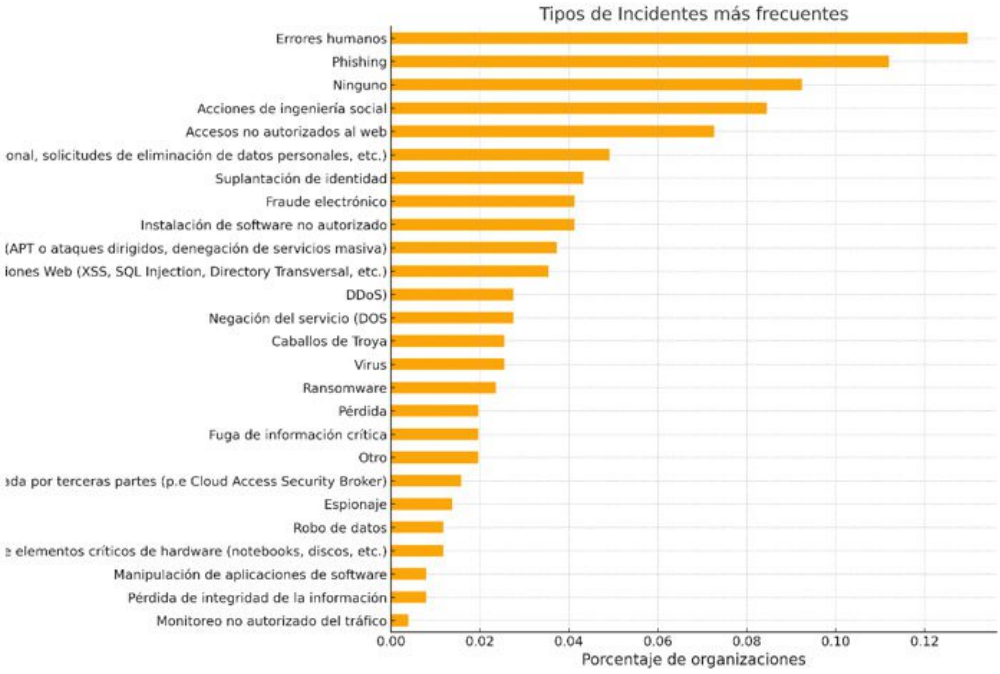
Se listan los más representativos, Tabla 2.

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

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

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

Tabla 2 Tipo de incidentes y frecuencias



Gráfica 2 Total de tipos de incidentes

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

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

Tipos de incidentes y sus impactos económicos

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

Gráfica 3 Tipos de incidentes y costos

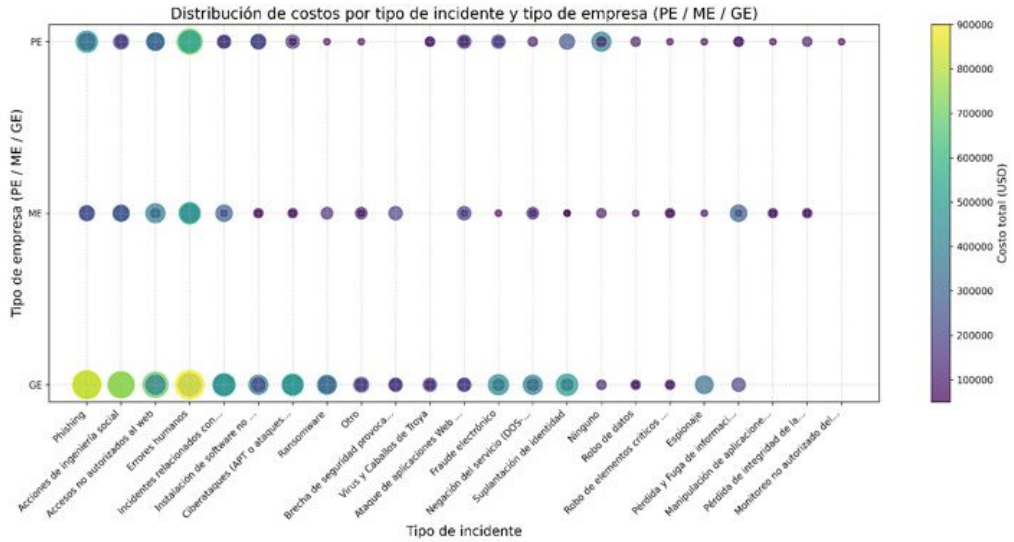
Impacto económico por tipo de incidente

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

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

Distribución de costos por tipo de incidente y tipo de empresa

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



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

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

El análisis revela varios hallazgos relevantes:

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

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

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

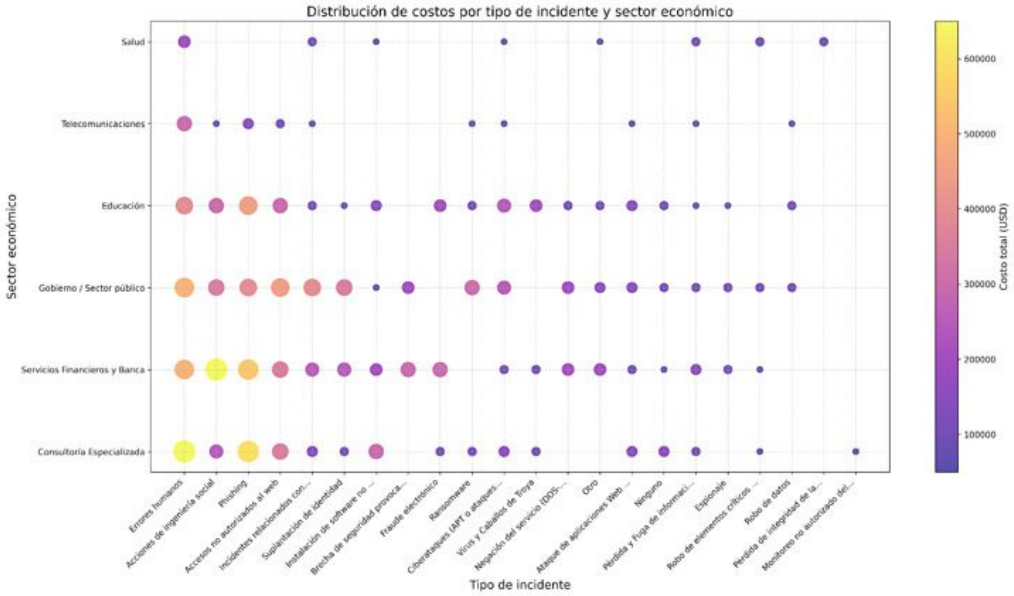
Menor presencia de incidentes complejos en medianas empresas: Se advierte que las medianas empresas (ME) registran, en esta muestra, menores costos relativos en categorías como ciberataques avanzados o ataques a aplicaciones web, lo que podría reflejar tanto diferencias en la madurez tecnológica como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

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

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

Distribución de costos por tipo de incidente y sector económico

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



Gráfica 5 Distribución de los tipos de incidentes x sector económico

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

El análisis evidencia patrones diferenciados entre los sectores:

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

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

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

pacitación y cultura organizacional en ciberseguridad.

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

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

Herramientas

Cantidad de mecanismos implementados

El conteo revela:

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

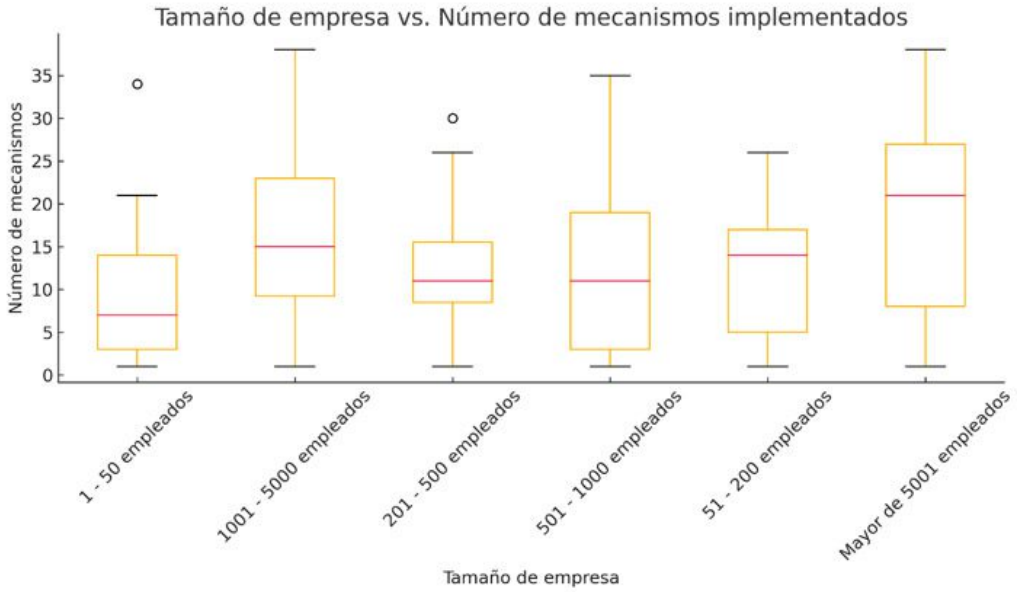
Mecanismos más usados por tipo de empresa

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

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

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

Tabla 3 Uso de mecanismos y herramientas de protección



Gráfica 6 distribución de mecanismos por tamaños de empresa

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

Obstáculos percibidos para la ciberseguridad

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

Interpretación:

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

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

Tabla 4 Obstáculos de la seguridad por tamaña de las empresas

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

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

Función ejecutiva del CISO

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

Presencia formal de la figura de CISO

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

Tipología del CISO (tabla 5)

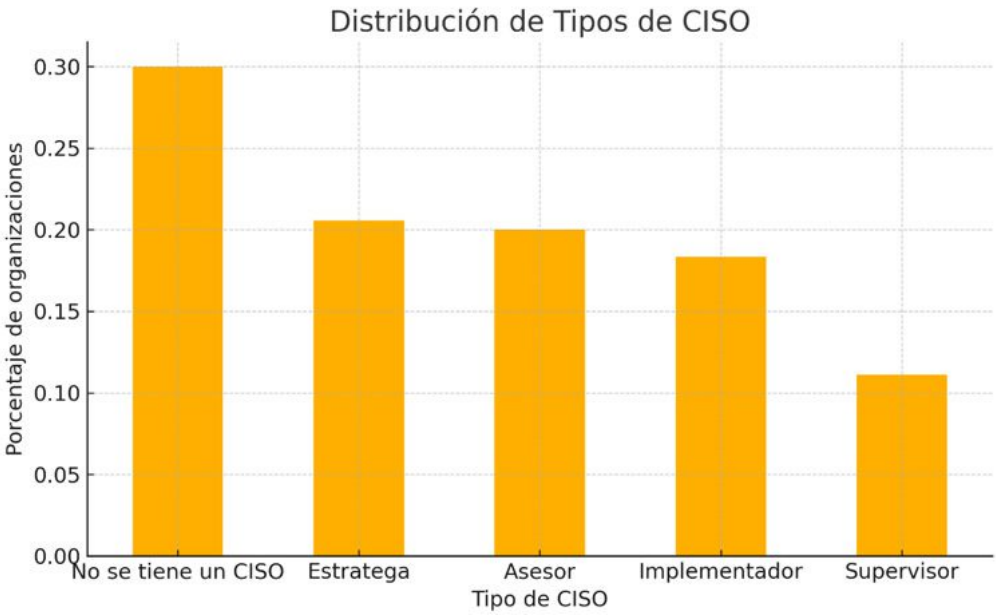
Predominan los perfiles tipo 3 (Asesor) y 4 (Estratega) en organizaciones de mayor tamaño y sectores regulados. En contraste, en pymes y sectores emergentes prevalecen los perfiles tipo 1 (Implementador) y 2 (Supervisor). Este patrón se evidencia en la gráfica 7.

Brechas identificadas

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

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

Tabla 5 Tipos de CISO



Gráfica 7 distribución de tipos de CISO

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

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

Conciencia de la alta dirección

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

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

Percepción sobre el nivel de conciencia

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

Factores que limitan el apoyo directivo

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

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

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

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

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

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

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

Por tamaño de empresa

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

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

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

Por sector económico

En términos sectoriales:

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

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

Tabla 6 Consciencia y participación de la alta dirección x sector

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

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

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

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

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

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

.

Discusión

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

Inversiones y madurez técnica

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

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

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

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

Conciencia de la alta dirección

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

En consecuencia, esto limita la capacidad de:

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

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

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

Madurez de la función del CISO

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

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

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

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

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

Obstáculos

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

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

Tabla 7 Agrupación general de obstáculos por tamaños de empresas globales

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

Temas claves

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

Interpretación estratégica

Estos cruces refuerzan la necesidad de:

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

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

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

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

Tabla 8 Temas claves x sectores

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

Síntesis

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

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

Conclusiones

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

Principales hallazgos

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

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

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

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

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

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

Implicaciones prácticas

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

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

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

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

Referencias

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ACIS
ASOCIACIÓN COLOMBIANA DE INFORMÁTICA, SISTEMAS Y TECNOLOGÍAS AFINES

REDUC@TE

2025

REDUC@TE es el encuentro diseñado para que educadores, ingenieros, diseñadores, y amantes de las TIC, puedan conocer las buenas prácticas, experiencias, tendencias y nuevas metodologías donde la tecnología converge con la educación y la formación.

PRIVILEGIOS	PATROCINADOR
Oportunidad de conferencia	Conferencia
Aviso publicitario en la Revista Sistemas	Aviso
Participación asistencia al Taller	2 Cupos (Taller)
Asistentes al evento	5 Cupos (Conferencia)
Participación en el panel	Página del evento Panel de proveedores
Logo en difusión del evento	Logo
Logo en memorias	
Logo en correo de difusión	

301 553054 suscripciones@acis.org.co

https://www.acis.org.co/reducate

La ciberseguridad multigeneracional

DOI: 10.29236/sistemas.n175a5

Jeimy J. Cano y Andrés Almanza moderadores de la reunión dieron la bienvenida a los participantes y procedieron a iniciar el debate.

"Este número 175 está dedicado a los asuntos de seguridad de la información, de la ciberseguridad, además, tiene que ver con los veinticinco (25) años de la Jornada Internacional de Seguridad Informática y todo lo que eso representa alrededor de la dinámica de ACIS, para el sector y el gremio", manifestaron los moderadores.

Luego, cedieron la palabra a los invitados para su respectiva presentación y entrar de lleno al debate.

Gonzalo Romero
Soy ingeniero de sistemas y computación, especialista en telemática de la Universidad de Los Andes y agradezco mucho la invitación para participar en este panel; en la actualidad, me desempeño como director de seguridad de la información en una organización multinacional americana que opera el dominio de Internet de Colombia.

Tengo alrededor de 20 años de experiencia en temas de seguridad de

la información y más de 35 en temas de infraestructura tecnológica (IT).

John César Arango
Soy ingeniero de sistemas, especialista en ciberseguridad, con dos especializaciones en redes y telecomunicaciones y otra en finanzas.

Tengo una empresa de ciberseguridad que se dedica a la seguridad ofensiva y soy docente, director de la especialización en ciberseguridad de la Universidad Católica de Mendizábal, además de docencia del módulo de ética, el *hacking* que normalmente dictan varias universidades, no solamente de Colombia, sino también de otros países.

Luego de las presentaciones de los invitados, se dio paso a la formulación de las preguntas por parte de los moderadores del encuentro, Jeimy J. Cano y Andrés Almanza.

¿Cómo han visto la evolución de la seguridad de la información a la ciberseguridad empresarial?

Gonzalo Romero
Antiguamente, nos enfocábamos en proteger los datos de la organización, había un interés, una concentración total en proteger los datos. Y eso se ha convertido ahora en una partecita dentro de una visión holística integral que prioriza en dos grandes puntos que son primero, la resiliencia operacional y segundo, la continuidad del negocio.

Me parece que eso es lo que ha sucedido. Nos estábamos enfocando en algo muy acotado y pasamos a algo mucho más global, mucho más organizacional, más integral en términos de protección. Antiguamente protegíamos el dato, hoy protegemos la organización, el negocio. ¿A partir de qué? A partir de temas de resiliencia y continuidad. Antes hablábamos de controles perimetrales, de dispositivos de seguridad, de firewalls o cortafuegos, accesos restringidos. Ahora estamos hablando de modelos mucho más dinámicos, más adaptativos.

La protección requiere de una gestión de riesgos eficiente, una respuesta proactiva y claramente la automatización que brinda la inteligencia artificial para poder anticipar y neutralizar las amenazas antes de que impacten las operaciones del negocio.

John César Arango
De verdad ha habido un cambio. Antes se pensaba en algo muy básico, es decir, tenemos que instalar Fire Wall, antivirus y manejar parches, eso era lo que uno hablaba anteriormente, hoy nos preparamos ante un ataque. Eso ha cambiado. O sea, qué debemos hacer si pasan los ataques o cuándo pasarán. Mantenemos esa zozobra.

No sabemos cuándo nos va a tocar. Si bien es cierto que la resiliencia exige algo más allá de la técnica, para la conciencia colectiva necesitamos integrar todas esas gene-

raciones en el mismo lenguaje de la seguridad.

Jeimy J. Cano M.
¿Hoy, cuáles elementos de la ciberseguridad son completamente diferentes a los que se conocían antes en seguridad de la información?

John César Arango

Para mí lo nuevo es que se trata de un apoyo bastante bueno. En el caso de una empresa en la que hice un análisis de tráfico para descubrir un problema, la inteligencia artificial me indicó exactamente cuáles eran los filtros a utilizar. Eso me pareció ´descrestante´ y me ahorró mucho tiempo.

Pero también y pensándolo como docente, he visto ya trabajos en los que la productividad de las personas a veces decae debido a que mantienen el uso de la inteligencia artificial de una forma inapropiada.

Gonzalo Romero

Estoy completamente de acuerdo; la inteligencia artificial (IA) es una herramienta con la que no contábamos antes, algo tan útil para identificar anomalías, para predecir ataques, para responder en tiempo real a las situaciones. Me parece que es una ventaja, un beneficio grandísimo que tenemos como gestores de seguridad en las organizaciones. Me parece que nos apoya y nos ayuda.

John César Arango
Ahora la seguridad se volvió un juego y le apostamos al juego, pero ahora ya no lo es, y dejó de serlo para convertirse en algo mucho más complejo, están acabando con la infraestructura, la reputación y la imagen de nuestro negocio.

Andrés Almanza
Gonzalo mencionó algo que vale la pena reflexionar: en el pasado nos

distraíamos con las cajas, hoy no. Por ejemplo, ahora al poner todo el CM, el XDR, ahora está de moda el NDR, el EDR, el DDR y el PPPR, por mencionar algunos. Entonces, ¿no estaremos heredando esos problemas del pasado a hoy? Lo que pasa es que ahora es software y ahora es desarrollo. ¿Hay otro cambio? Ahora hay cajas de hardware, cajas negras. Y hay sorpresas. Ahora es software con inteligencia artificial que yo puedo acomodar a como yo diga, a como yo indique, a como yo quiera predecir y evolucionar y progresar.

Jeimy J. Cano M.

¿Habría que actualizar las prácticas de seguridad de la información frente a los retos que tienen la empresa en el contexto digital? ¿Cómo se debería hacer ese cambio?

John César Arango

Estamos viviendo un cambio empresarial bastante importante. Entre las leyes está, por ejemplo, la Ley de Protección de Datos Personales la 1581. Varias cosas han exigido que muchas empresas se monten en dos voces de las leyes y eso nos permite de alguna manera que vayan en esa transformación.

Ahora veo que la gente se va volviendo más consciente de la seguridad, de la ciberseguridad; cada día necesitan más proveedores y varias empresas para eso. La gente no entiende que la nube es una responsabilidad compartida y muchas veces insegura.

Sería bueno que las empresas se vincularan a esos grupos de respuesta de incidentes, además de tener un servicio con unos terceros expertos en auditoría, para revisar ese tipo de cosas. Obviamente estamos hablando ya de empresas media pymes y grandes.

Gonzalo Romero

Absolutamente. En el contexto digital actual, caracterizado por la alta capacidad de integración, el uso creciente de inteligencia artificial y la sofisticación de las amenazas, es indispensable revisar y actualizar continuamente las prácticas de seguridad de la información. Ya no basta con defender perímetros; hoy el enfoque debe ser dinámico, basado en riesgos, y profundamente integrado con la estrategia del negocio.

El cambio debe comenzar por transformar la cultura organizacional: la seguridad no puede seguir viéndose como un área aislada o como una carga operativa, sino como un habilitador de confianza, continuidad y evolución digital. Esto exige adoptar marcos de referencia modernos como CSF y AI RMF de NIST, Zero Trust, fortalecer la gobernanza de datos, automatizar procesos críticos y, sobre todo, empoderar a las personas.

La verdadera resiliencia operacional y de negocio no se construye solo con tecnología, sino con conciencia, corresponsabilidad y liderazgo compartido.

Jeimy J. Cano M.

El algoritmo ¿está haciendo lo que tiene que hacer? ¿El algoritmo tiene la matemática correcta que tiene que utilizar? ¿El algoritmo está dando resultados consistentes? ¿El algoritmo está bien diseñado, bien hecho?

Gonzalo Romero

John César resume una serie de detalles clave a tener en cuenta y estoy totalmente de acuerdo con ellos; desde mi perspectiva, debemos orientar las prácticas de seguridad hacia la continuidad del negocio, revisando exhaustivamente el alcance y las métricas del plan de contingencia, conformado en ultimas por el plan de continuidad de negocios, el análisis de impacto de negocio, el plan de recuperación ante desastres y la gestión de incidentes dentro de nuestras organizaciones; de esta manera, estaremos avanzando en el despliegue de nuestra resiliencia operacional, tanto humana como corporativa.

Traigo a colación la situación que describió el propio Sr. Bryan Krebs con el ataque de denegación de servicios que sufrió su muy reconocido blog "KREBS ON SECURITY" a mediados de mayo; con un pico de 6.3 Tbps, ha sido uno de los ataques más grandes jamás registrados. Según él, a pesar del ataque, el sitio web estuvo activo en todo momento y no presentó interrupción alguna. Esto es lo que yo denomino *Resiliencia Operacional*.

En palabras coloquiales, me pueden estar intentando incluso destruir, pero yo estoy en línea, activo. Yo estoy ofreciendo mis servicios como si nada estuviese sucediendo tras bambalinas; a eso es a lo que debemos apuntarle, más allá del análisis previo y posterior al incidente, que sucedió con las "cajas", etcétera.

Creo que por aquí va el asunto: debemos capacitar a los CISO para que diseñen, desplieguen y gestionen cada vez mejores y más robustos planes de contingencia; ahora bien, una cosa muy bonita es tener el documento del plan. Pero ¿cuándo y cuántas veces al año se ejecuta el plan? acaso solo debe desplegarse cuando el auditor lo requiere? el objetivo radica única y exclusivamente en el cumplimiento? a partir de lo descrito por Krebs, el ejercicio del CISO con su equipo de trabajo, y apalancado en el área

de IT, incluye el estar muy atento a los resultados del análisis de tráfico de red de sus plataformas y servicios; en este caso particular, nota efectivamente que su mapa de calor está en rojo, pero sus servicios están plenamente activos y disponibles.

Una pregunta suelta: ¿ustedes saben cuál es el país que estadística e históricamente participa más en el FIRST, un evento anual muy reconocido que congrega a los CERT y CSIRT de todo el mundo? Japón.

Yo tuve el privilegio de participar como conferencista en el evento del 2014, celebrado a finales del mes de junio en Boston, Massachusetts, Estados Unidos. Este evento sucedió 3 años después del tsunami más devastador en la historia nipona.

Jamás olvidaré que cuando terminó la plenaria de apertura del evento, todos los japoneses tenían unos papelitos en sus manos y de repente se levantaron de sus puestos y nos entregaron a cada uno de los que asistíamos el papelito, que mostraba los recuadros de lo que parecía una corta “tira cómica”; todos casi nos ponemos a llorar. ¿Saben qué decía el papelito? Pues decía "¿Cómo protegerse de un tsunami?" Es uno de los ejemplos más claros y concisos de cooperación y solidaridad que haya visto; desde ese momento, me quedó muy claro quiénes son los japoneses: aprenden de sus situaciones y de sus errores, pero no se quedan ahí, comparten su propia realimentación como parte de su proceso de mejora continua.

Jeimy J. Cano M.
Nuestra pregunta número cuatro: ¿Cómo debería transformarse la formación de los profesionales en seguridad cibernética y qué competencias nuevas se deben considerar? ¿Cómo actualizar las que tenemos a la fecha dentro los retos y escenarios que se viven en la actualidad?

John César Arango
Hace un año fui profesor de una especialización de desarrollo de software y lo primero que les pregunté en mi materia.

Y lo primero que les pregunté fue si sabían qué era AWS y ninguno conocía el término. Me pareció increíble eso. El enfoque obviamente tiene que ser interdisciplinario, hoy en día debemos tener en cuenta la inteligencia artificial, la ciencia de datos, el análisis forense digital, internet de las cosas, blockchain, computación en la nube, entre otras. Además de integrar esas competencias blandas tales como comunicación, liderazgo, pensamiento crítico, resolución de problemas.

Gonzalo Romero
Desde mi perspectiva, la formación en seguridad digital necesita cambiar de raíz: no se trata solo de aprender a gestionar herramientas

o reaccionar ante incidentes; eso es parte inherente de nuestro rol y responsabilidades, claro, pero ya no es suficiente. Hoy estamos en un entorno donde los riesgos son mucho más complejos, donde hay IA involucrada, donde los datos están en todas partes y las decisiones de seguridad tienen un impacto directo sobre el negocio, en la imagen, en la reputación e incluso en la confianza social.

Entonces, lo que necesitamos es una formación mucho más integral. Hay que formar profesionales que no solo dominen la parte técnica —que sigue siendo clave— sino que también conozcan de riesgos, de comunicación, de ética, de regulación, y que tengan la capacidad de adaptarse a entornos híbridos y altamente automatizados. Y algo que es clave: si o si, tenemos que dejar de ver al área jurídica como un obstáculo; el profesional de seguridad digital tiene que empezar a comprender los aspectos normativos y legales, y ver a los equipos legales como aliados estratégicos. No son un fantasma ni un rival: son parte del mismo equipo que ayuda a cuidar la organización desde otra dimensión.

Y para actualizar las competencias que ya tenemos, hay que dejar atrás esa lógica de acumular certificaciones por cumplir; definitivamente necesitamos entrenamiento realista, inmersivo, continuo, espacios donde se simulen crisis, donde se aprenda haciendo, donde el error también sea una fuente de aprendizaje. Porque al final, no estamos formando técnicos operativos: estamos formando guardianes de la confianza digital.

Considero que debe haber una política pública; pero ¿cuándo se va a construir? No lo sé.

Andrés Almanza
Que interesante punto que tienes Gonzalo para conectarlo con las ideas de John, que es tratar a la ciberseguridad como un reto de política pública; al hacerlo de esa manera será el momento en donde vamos a poder conectar diferentes visiones y articular de alguna manera lo que se requiere desde el punto de vista de gobernanza, del ejercicio de gobierno, lo que implica desarrollar una serie de prácticas que entre todos las deben construir.

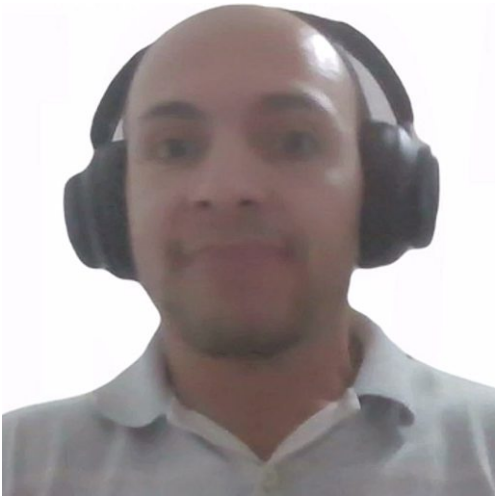
Jeimy J. Cano M.
Desde su perspectiva práctica, académica y empresarial ¿cómo viven esa experiencia y cómo van a gestionar ese tema de aquí en adelante?

John César Arango
Me parece una fortaleza que se puede complementar bastante. Es necesario trabajar en un ambiente multigeneracional. En Bolivia conocí a un muchacho, a un joven que su conocimiento lo construyó completo a través de internet. Hace una ingeniería inversa, sobre los cajeros descubre la vulnerabilidad, es un ´monstruo´, pero no le gusta ha-

blar de tecnología. Ahora no necesariamente el coach es el experto, ahora se trata de jóvenes que aportan a la organización en una manera importante. Se requiere motivarlos mucho.

Si sabemos concentrar el esfuerzo, vamos a encontrar muchas cosas buenas que nos van a ayudar en el camino hacia la resiliencia operacional, hacia la continuidad del negocio, hacia la protección de la marca hacia la protección de la reputación.

Andrés Almanza



Para complementar, dado que Gonzalo lo puso en el tintero esa práctica del mentoring y el mentoring reverso, que es útil en estos ambientes multigeneracionales que son cada vez más continuos y de hecho tú encuentras empresas que tienes las cinco generaciones que hoy existen marcadas en un ambiente organizacional.

Entonces, el mentoring Reverso ha venido tomando fuerza este ejercicio que busca conectar experiencias con innovación en el contexto de los seres humanos para que los mayores, pues aprendan de los jóvenes cómo es que ellos ven los problemas.

La experiencia en vez de ser una capa que rechaza el uno del otro, lo que hace que al quitarla y dejarse en la piel de los seres humanos hace dos personas se conecten. Una experiencia interesante fue acompañar un proceso en el que una persona con u se convirtió un alto nivel de experiencia, se convirtió en mentor de un joven, y en esa conexión fue muy satisfactorio ver los aprendizajes de ambas partes. Entonces se construyó un espacio muy humano.

En contextos multigeneracionales es clave que se gestionen desde la humanidad y menos desde el conocimiento, así es posible que haya aportes y crecimientos entre todas las visiones que se encuentran en estos espacios de intercambio de experiencias y aprendizajes.

El contexto digital actual, ha venido reescribiendo la forma en cómo el humano se desenvuelve, por tanto, suelo decir que los avances tecnológicos de esta era están empujando cada día más, a las personas a saber ser más y solo aquellos que logren eso, serán los que más capital, valor y potencial mostraran en el futuro.

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.*

Calendario de eventos

ACIS
ASOCIACIÓN COLOMBIANA DE INFORMÁTICA, SISTEMAS Y TECNOLOGÍAS AFINES

2025

FEB
3 - 13
CURSO VIRTUAL: ARQUITECTURA DE SOFTWARE
4:00 PM - 7:00 PM

MAR
12 - 17
II PROGRAMADORES DE AMÉRICA 2025
Salvador bahía, Brasil

MAR
27
ASAMBLEA ACIS

JUN
11 - 14
ENCUENTRO REDIS
Rionegro, Antioquia

JUN
16-19
SIMPOSIO DE GESTIÓN DE DATOS 2025
Escuela de Ingenieros Julio Garavito

JULIO
30 Y 31
JORNADA INTERNACIONAL DE SEGURIDAD INFORMÁTICA

AGO
28 Y 29
JORNADA DE GESTIÓN DE PRODUCTOS Y PROYECTOS TI

SEP
ACISTIC 2025

AGO - SEPT
30, 1-5
MARATÓN WORLD FINALS 2025
BAKÚ, AZERBAIYÁN

OCT
14 - 18
REDUC@TE

OCT
18
MARATÓN NACIONAL DE PROGRAMACIÓN 2025

NOV
8
MARATÓN REGIONAL LATINOAMERICANA DE PROGRAMACIÓN 2025

ACIS
ASOCIACIÓN COLOMBIANA DE INFORMÁTICA, SISTEMAS Y TECNOLOGÍAS AFINES

¡AFILIATE YA!

Y DISFRUTA DE ESTOS BENEFICIOS

- Actualización en formación profesional y académica de manera constante.
- Candidatura a participación profesional en proyectos de ACIS.
- Candidato a Director o CoDirector de Grupo de Interés (GI).
- Candidatura a participar en consultorías solicitadas a ACIS por el sector privado y público.
- Candidatura a participar en eventos nacionales o internacionales como delegado de ACIS.
- Candidato a Miembro de Consejo Editorial de la Revista Sistemas.
- Descuentos especiales en cursos y eventos exclusivos en el área de las TIC.
- Referencia profesional para vinculación como Perito en procesos de arbitraje.
- Referencia para participación en Juntas Directivas.
- Inclusión en el gremio de Ingenieros de Sistemas más importante del país.
- Recepción trimestral de la revista SISTEMAS en formato digital.
- Acceso diferido a la base de Webinars de ACIS.
- Acceso exclusivo a oportunidades laborales a través de nuestro portal de empleo.
- Participación como conferencista o participante en las charlas semanales.
- Correo personal con @acis.org.co
- Asista a las funciones del Teatro Nacional con un 20% de descuento. Consulte la Programación y solicite el descuento a cursos@acis.org.co.
- 30% de descuento en los libros de la Casa Editorial ALFAOMEGA, consulte el Catálogo

Afiliación General

Afiliación + Precio de estudio de formulario

$ 323.400 + $ 60.000

Afiliación para recién egresados

Descuento de 20% para recién egresados, (2 años) + Precio de estudio de formulario

$ 258.800 + $ 60.000

301 5530540 suscripciones@acis.org.co www.acis.org.co