

WORLD TELECOMMUNICATION
DEVELOPMENT CONFERENCE



IPEC-25

Regional Economic Dialogue (RED)

Montevideo, Uruguay, 6-7 October 2025

Construcción de un ecosistema de confianza y seguridad digital en América Latina y el Caribe

Sebastián Cabello, SmC+



Evaluación del estado de la regulación en gobernanza de datos y ciberseguridad en los países de América Latina y el Caribe



Alcance del estudio

33 países de América Latina y el Caribe

- | | | |
|-------------------|-------------|------------------------------|
| ANTIGUA Y BARBUDA | DOMINICA | PANAMÁ |
| ARGENTINA | ECUADOR | PARAGUAY |
| BAHAMAS | EL SALVADOR | PERÚ |
| BARBADOS | GRANADA | REPÚBLICA DOMINICANA |
| BELICE | GUATEMALA | SAN CRISTOBAL Y NIEVES |
| BOLIVIA | GUYANA | SAN VICENTE Y LAS GRANADINAS |
| BRASIL | HAITI | SANTA LUCIA |
| CHILE | HONDURAS | SURINAM |
| COLOMBIA | JAMAICA | TRINIDAD Y TOBAGO |
| COSTA RICA | MÉXICO | URUGUAY |
| CUBA | NICARAGUA | VENEZUELA |



Relevamiento secundario

Análisis de políticas y normativa a partir de información de acceso público

OBJETIVO PRINCIPAL

Análisis normativo

Realizar una revisión del **marco normativo existente en materia de protección de datos personales(*) y ciberseguridad** en los países de América Latina y el Caribe (ALC)

Sistematización

Sistematizar la información sobre el marco normativo estatal de protección de datos personales y ciberseguridad.

Índice

Desarrollar un **índice o indicador del estado de situación** de la protección de datos personales y ciberseguridad en los países de América Latina y el Caribe.

Barreras

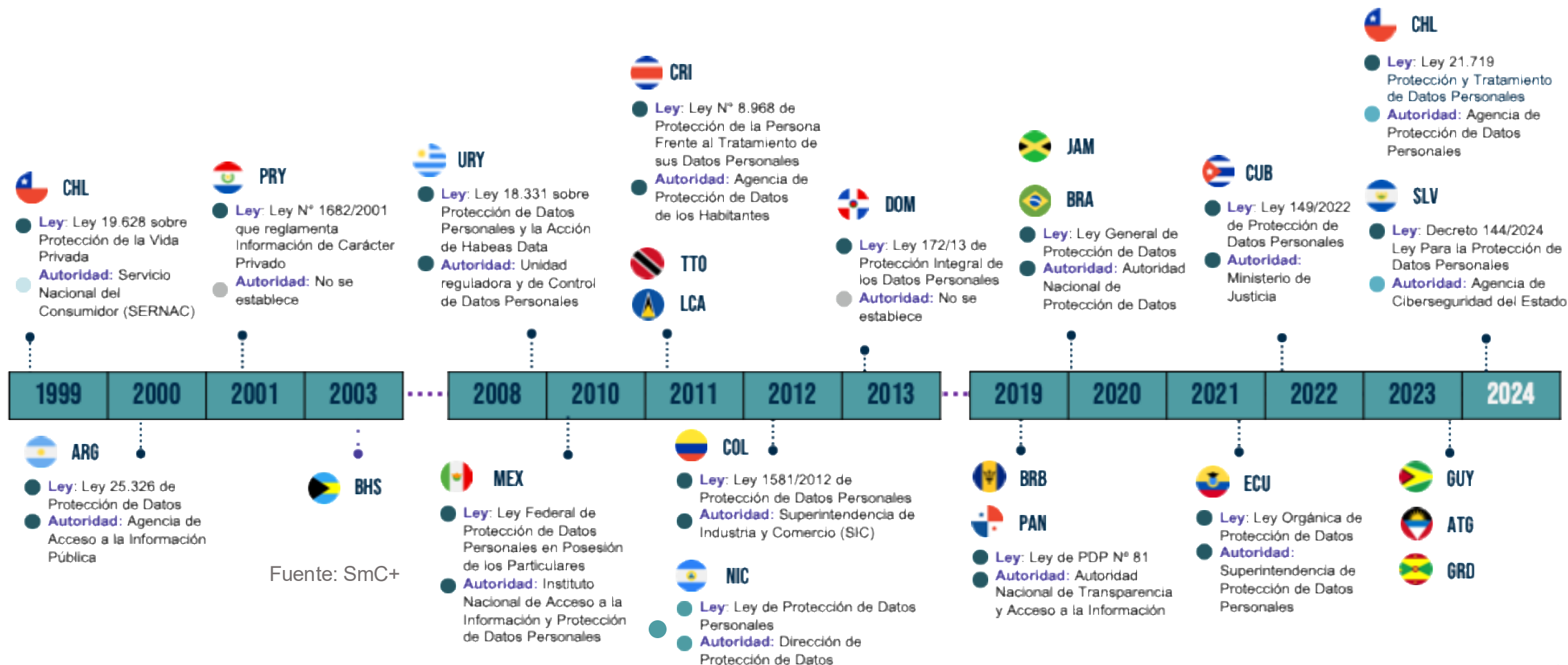
Identificar los **principales retos y barreras** que enfrentan los países de América Latina y el Caribe para implementar políticas efectivas de protección de datos personales y ciberseguridad.

Recomendaciones

Desarrollar un informe conciso que resuma los hallazgos de la investigación y proporcione **recomendaciones para mejorar las políticas y marcos de la protección de datos personales y ciberseguridad** en los países de América Latina y el Caribe.

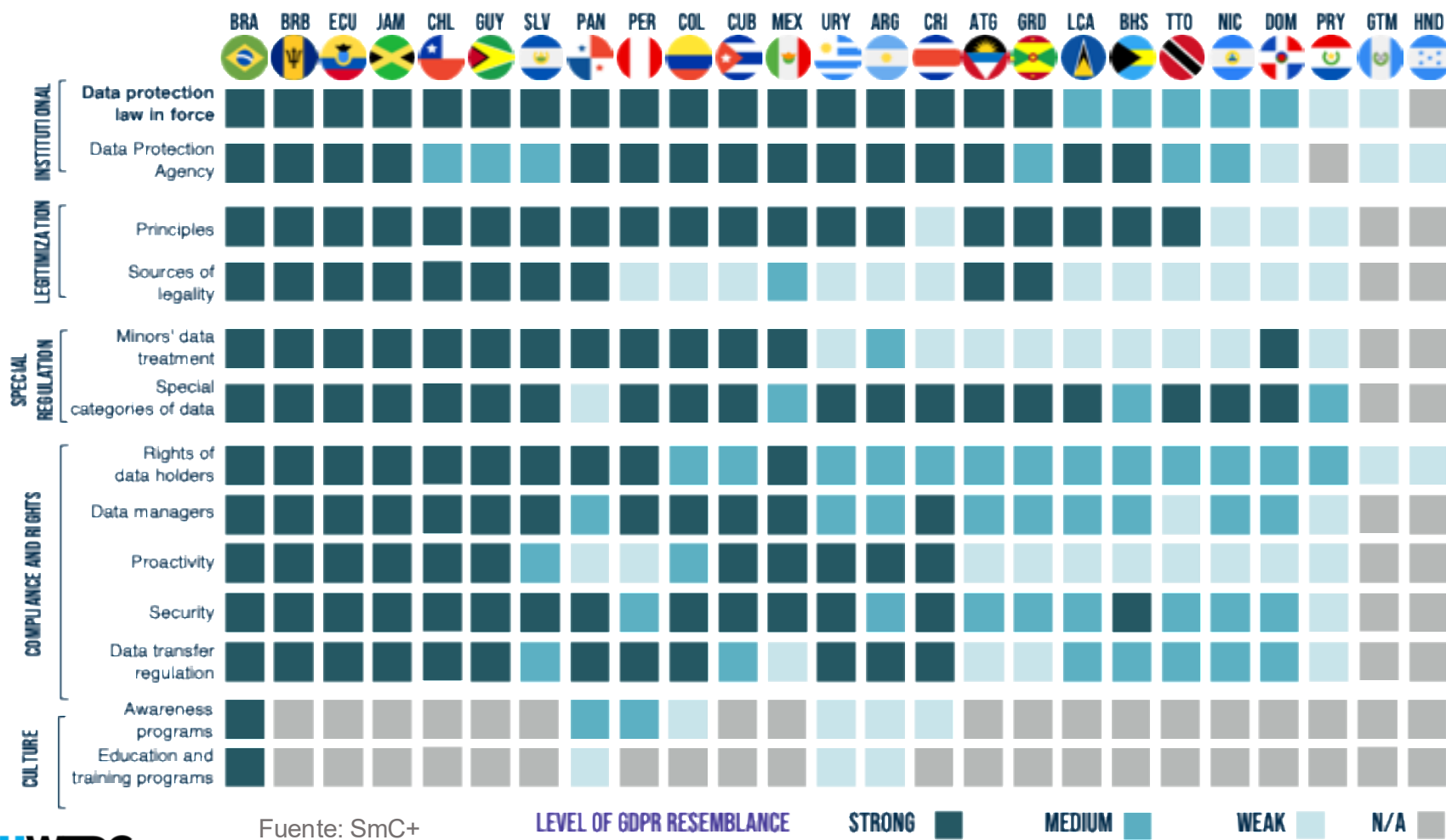
OBJETIVOS SECUNDARIOS

La protección de datos posee un historial regulatorio bastante consolidado, que tendió a converger con LGPD



Fuente: SmC+

Hoy, 17 países de ALC tienen una legislación que puede considerarse robusta con todos los principios de protección



22 países cuentan con leyes de protección de datos personales y autoridades de control con mandato de supervisión y aplicación; 11 sin ley todavía, aunque algunos (Surinam, Bolivia) con proyectos en curso

La protección de datos posee mayor madurez normativa e institucional de base, pero enfrenta retos de *enforcement*, adopción de herramientas de gestión de riesgos y cultura organizacional

Los gobiernos de la región tienen latente la necesidad de tener estrategias para afrontar los desafíos crecientes de la ciberseguridad

	CHL	CRI	DOM	ECU	URY	COL	PRY	BRA	PER
Periodo de aplicación	2023-2028	2023-2027	2022-2030	2022-2025	2024-2030	2025-2027	2025-2028	2025	2026-2028
Autoridad de aplicación	ANCI	MITI	CNCS	MINTEL	agesic	TIC	SEC. DE GOB. DIGITAL	CNCIBER	SEC. DE GOB. DIGITAL
Influencias internacionales	OAS	OAS		OAS	OAS	OAS	OAS		OECD
Herramienta normativa	DECRETO		DECRETO	RESOLUCIÓN			DECRETO	DECRETO	
Propone aprobación de Ley Marco									
IA como herramienta de ciberseguridad									
Énfasis en presupuesto									
Énfasis en desarrollo laboral y profesional									
Soberanía digital o desarrollo doméstico									
Arquitectura Zero Trust									
Criptografía post-cuántica									

NIVEL DE ESPECIFICIDAD



Fuente: SmC+

Las Estrategias se están convirtiendo en una herramienta cada vez más importante para que los gobiernos articulen una visión a medio/largo plazo de la ciberseguridad.

PRINCIPIOS COMUNES EN LAS ESTRATEGIAS



Protección de los derechos y centrada en el ser humano

Ya sea explícitamente como un "principio rector" o como un "enfoque" en todas las acciones. Subraya la prioridad de proteger a las personas y sus derechos en el ciberespacio.



Cultura / educación en ciberseguridad

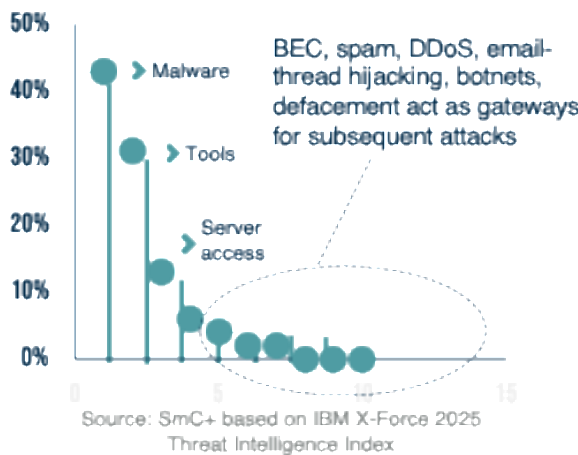
Todas las estrategias incluyen la educación y la sensibilización como áreas clave. La cultura de ciberseguridad y el desarrollo de capacidades humanas aparecen como un objetivo estratégico, misión o línea de acción, según el país. **La escasez de profesionales calificados tanto en el sector público como en el privado se considera el principal desafío. Todos priorizan el desarrollo de una fuerza laboral especializada en ciberseguridad para cerrar la brecha de talento e impulsar la resiliencia digital.**

¿Qué desafíos? ¿Qué costos?

CYBERCRIMINALS SEEK CONTROL AND MONETIZATION OVER VISIBLE CHAOS

According to IBM, in 2025 **73% of observed actions are explained by malware and tools** attackers use to keep continuous access.

IBM Top actions on objectives observed in 2024 (%)



In LATAM, the leading impacts were credential harvesting (40%) and extortion (40%), with brand reputation damage (20%)

CYBERATTACK VOLUME AND RECENT EVOLUTION

THE AVERAGE LATAM ORGANIZATION FACES ~40% MORE ATTACKS THAN THE GLOBAL AVERAGE

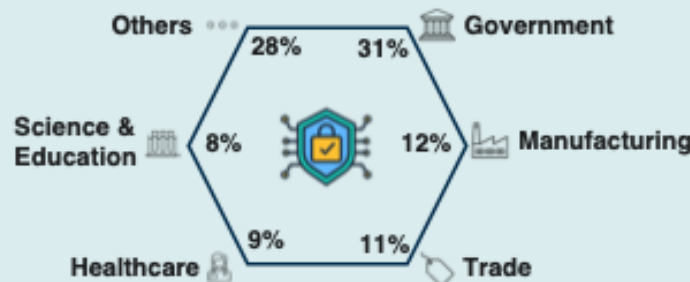
MEX Represents the highest malicious activity, with 55% of regional incidents.

31 BILLION CYBERATTACKS IN 2024

More than 1,600 cyberattacks are reported in Latin America per second

GOVERNMENTS ARE LAYING OUT NATIONAL STRATEGIES TO COORDINATE EFFORTS

MOST TARGETED INDUSTRIES OF RANSOMWARE ATTACKS IN LATAM

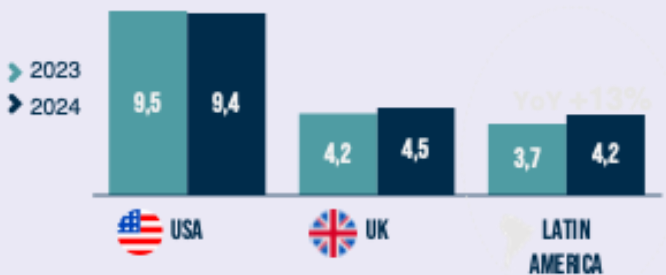


Source: SmC+ based on The State of OT Cyber Security in LATAM, 2024 Annual Report

THE RISING COST OF BREACHES AND SLOW RESPONSE TIMES

The **financial cost of cyberattacks** in Latin America is rising. The average cost of a data breach in LATAM increased from USD 3.7 million in 2023 to USD 4.2 million in 2024.

IBM Average cost of a data breach by country or region (US\$ millions)

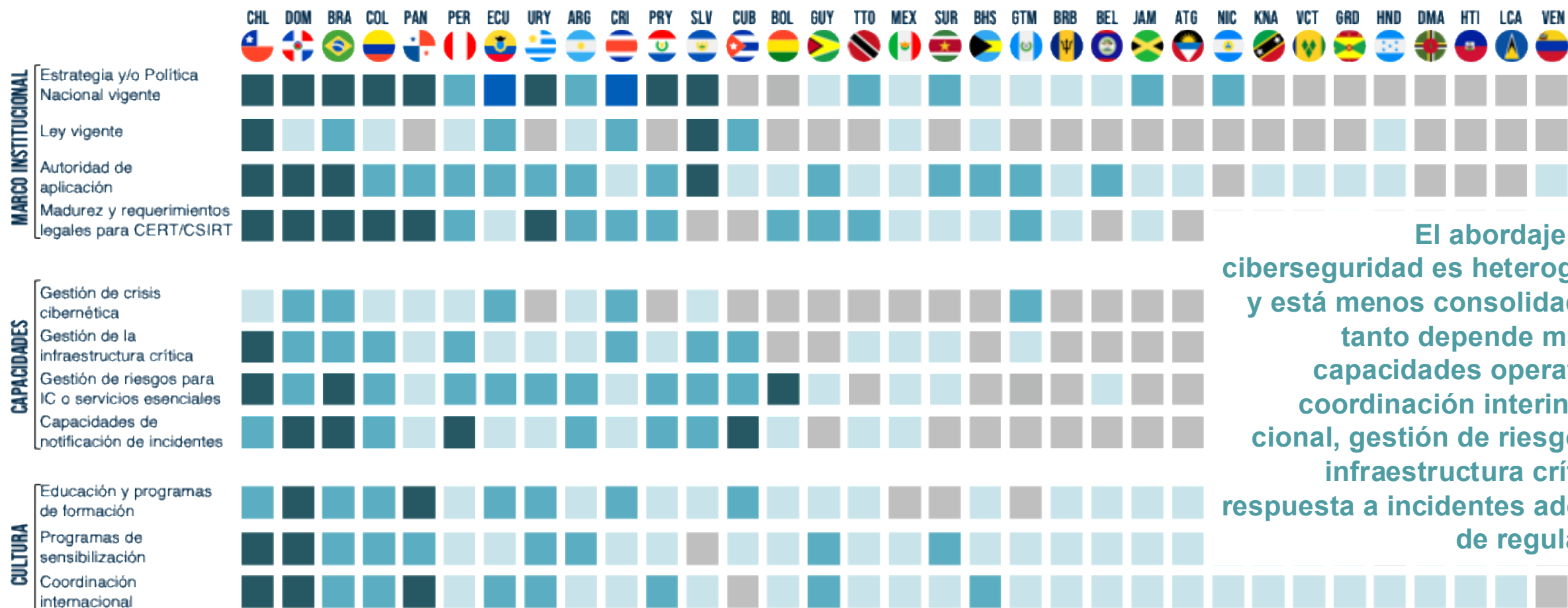


Source: SmC+ based on IBM, Cost of a Data Breach Report 2024

43% of companies that suffered attacks in 2024 reported **losing customers** due to reputational impact, as well as disruptions to critical operations.

258 DAYS Detection and containment time (global average 2024)

Solo cuatro países en la región pueden considerarse como mas maduros en su nivel de desarrollo regulatorio en ciberseguridad



El abordaje de la ciberseguridad es heterogénea y está menos consolidada en tanto depende más de capacidades operativas, coordinación interinstitucional, gestión de riesgos en infraestructura crítica y respuesta a incidentes además de regulación

Fuente: SmC+

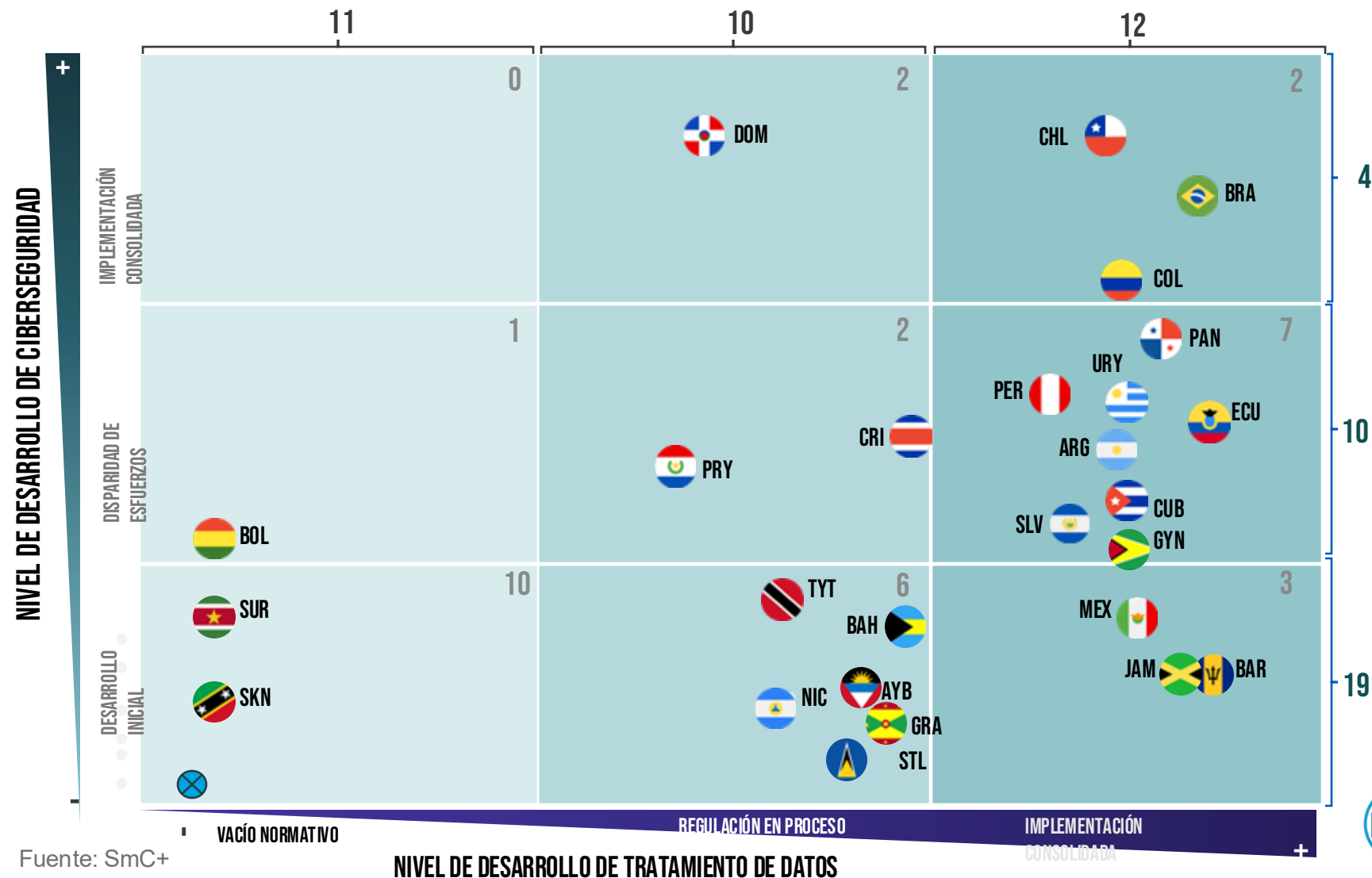
NIVEL DE MADUREZ DEL MARCO REGULATORIO:

ROBUSTO ■ INTERMEDIO ■ INCIPIENTE ■ NULO ■

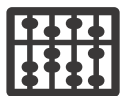
Brasil, Colombia y Chile se destacan por su abordaje integral en ciberseguridad y protección de datos

Los países de ALC muestran una variación significativa en sus niveles de desarrollo entre ciberseguridad y tratamiento de datos personales, con mayor énfasis y trayectoria en este último aspecto.

Se observa mayor nivel de desarrollo en tratamiento de datos personales (14 países en un nivel más avanzado) en comparación con aquellos en ciberseguridad (4 países avanzados). Solo tres países poseen un desarrollo de más alto nivel en ambos aspectos: Brasil, Chile y Colombia.



El desarrollo incipiente en Ciberseguridad se debe a la mayor complejidad operacional y de coordinación que demanda



Disparidad entre tratamiento de datos y ciberseguridad

La complejidad inherente para un desarrollo robusto en ciberseguridad demanda una mayor coordinación entre diversos actores y una asignación de recursos más significativa para implementar medidas concretas, como la construcción de capacidades estatales. En contraste, los avances en tratamiento de datos parecen ser más directos, ya que requieren de la vigencia de legislaciones completas.



Secuencia temporal y trayectoria regulatoria

Los países suelen iniciar sus esfuerzos regulatorios con la protección de datos y luego enfocarse en ciberseguridad. Esto sigue la trayectoria marcada por Europa, aunque es importante destacar que tanto NIS 1 como el RGPD salieron al mismo tiempo. En ALC, existen diferencias en la terminología de ciberseguridad que responde a la madurez en el abordaje del tema.



Diferencias en enfoque y componente jurídico

La protección de datos se refiere principalmente a regulaciones y políticas, mientras que ciberseguridad posee un componente operacional más diverso y complejo que dificulta su implementación. En general, la protección de datos es abordada desde el inicio de las regulaciones en los países. En materia de ciberseguridad el componente más fuerte es tecnológico/técnico y los marcos jurídicos recién se están construyendo.



Pocas legislaciones, bajos niveles de concientización

Solo Chile cuenta con legislación específica de ciberseguridad en ALC. Los bajos niveles de concientización se retroalimentan con la falta de legislaciones claras, surgiendo un ciclo de falta de conciencia y ausencia de legislación. Es importante considerar que la trayectoria en este ámbito no es unívoca, y existen estrategias en ciberseguridad que recopilan normas y guías de diferentes fuentes.



Brasil, Chile y Colombia se destacan por su enfoque integral

Brasil ha venido trabajando de manera sostenida en ciberseguridad, y al incorporar la Ley de Protección de Datos en 2018, asoció inmediatamente ambos elementos. Este enfoque integral también se observa en el caso de Colombia y Chile mas recientemente los cuales han fortalecido su cuerpo normativo, institucional y estratégico para abordar los desafíos más actuales.



Interrelación entre protección de datos y ciberseguridad es crítica

La protección de datos exige salvaguardas técnicas y organizativas de ciberseguridad; y la ciberseguridad, para ser efectiva, debe incorporar principios y obligaciones de protección de datos en su diseño