La Ciberseguridad en Latinoamérica: Riesgos y Oportunidades



Por **Arwyn Victor Galera**, estudiante de la Licenciatura en Ciencia Política. Universidad Nacional de Córdoba, Argentina. Contacto: arw274@hotmail.com.

Cita sugerida: Galera, A. (08 de octubre de 2024). *La Ciberseguridad en Latinoamérica: Riesgos y Oportunidades* [Columna de opinión]. Centro de Estudios Estratégicos de Relaciones Internacionales. Link: https://www.ceeriglobal.org/la-ciberseguridad-en-latinoamerica-riesgos-y-oportunidades/

Contexto

El desarrollo continuo del ciberespacio obliga a poner la mirada en la seguridad. En las últimas décadas, organismos privados y gubernamentales desarrollaron tecnologías dirigidas a la recolección y almacenamiento de datos para analizar y tratar de generar políticas públicas basándose en la información recopilada sobre las personas. Estos desarrollos produjeron nuevos escenarios y problemas que entrecruzan lo "real" y lo "virtual". En este sentido, en alguna parte del mundo, cada 39 segundos se produce un ataque a los sistemas cibernéticos de empresas o entidades estatales, dejando expuestas las deficiencias de los actores para hacer frente a la sofisticación de las modalidades de daño. A raíz de este contexto, la presente columna busca exponer a la región latinoamericana en relación a la ciberseguridad, dada la creciente dependencia de los países al ecosistema digital y el incremento de amenazas en el espacio, como así también, dar cuenta de una oportunidad para la región de extender sus dominios de soberanía sobre el ciberespacio.

La pandemia de COVID-19 marcó un punto de inflexión para los Estados latinoamericanos. Los rápidos cambios y adaptaciones al ciberespacio dejaron al descubierto la brecha digital existente entre los países de ingresos altos y bajos. Durante este período, la región se convirtió en un objetivo ideal para los ciberdelitos debido a la falta de infraestructura y la limitada capacidad para responder a las vulnerabilidades de sus sistemas cibernéticos. Un ejemplo de esto fue lo ocurrido en 2020, cuando Telecom Argentina, uno de los principales proveedores de servicios de internet del país, sufrió un secuestro de datos en sus sistemas, seguido de una demanda de rescate por parte de los atacantes. De manera similar, en 2022, Costa Rica experimentó un ataque en el que se secuestraron datos de varios

ministerios gubernamentales, los cuales fueron posteriormente puestos a la venta en la Dark Web, lo que llevó al gobierno a declarar una emergencia nacional en ciberseguridad. Como resultado, la seguridad en el tránsito por la «autopista de la información» se ha convertido en una cuestión estratégica para América Latina.

Riesgos

Ahora bien, priorizar estratégicamente la seguridad cibernética no debe traducirse en una mayor contratación de empresas privadas vinculadas al creciente mercado de ciberseguridad. Se estima que este mercado podría duplicarse para 2027, impulsado por los altos costos que enfrentan las organizaciones con cada ataque. Bajo este contexto, empresas como Microsoft, CISCO, McAfee y Amazon, entre otras, buscan consolidar su posición dominante en este sector.

Además, se proyecta que para 2025 el costo anual de los ciberataques en Latinoamérica alcanzará los 90 mil millones de dólares, con un promedio de más de 18,5 millones de ataques por año. Esta situación podría aumentar las vulnerabilidades cibernéticas de varios países de la región, ya que la creciente dependencia de soluciones de empresas multinacionales como Microsoft, CISCO, entre otras, limita la capacidad de los Estados para desarrollar infraestructuras cibernéticas propias. En este contexto, la soberanía digital adquiere mayor relevancia, ya que la centralización del control de tecnologías clave en manos de corporaciones extranjeras deja a los gobiernos con escaso margen de maniobra ante ciberataques o fugas masivas de información.

Oportunidades

Dentro de la región, en marzo del presente año, Chile promulgó la “Ley Marco de Ciberseguridad”, convirtiéndose en el primer país latinoamericano en crear un marco regulatorio de vanguardia. En este sentido, la ley dispone la creación de la Agencia Nacional de Ciberseguridad (ANCI), encargada de regular, fiscalizar y sancionar a entidades públicas y privadas para incrementar las capacidades de las instituciones en materia de ciberseguridad. Por otro lado, también se prevé la articulación y cooperación mixta de agentes del ámbito público, privado e internacional para generar inversión en investigación y desarrollo de industrias en ciberseguridad. Con esta ley, el país expande sus dominios en el ciberespacio, protege su infraestructura crítica y se prepara para futuros ataques, a la vez que fomenta una cultura de prevención sobre la seguridad digital entre sus ciudadanos.

A partir de esta experiencia, se abren las oportunidades para pensar marcos de diálogo y cooperación en latinoamérica. La necesidad de proteger los intereses nacionales de cada país y mejorar la seguridad de las infraestructuras críticas, podría desarrollar que la región adopte un enfoque coordinado en la regulación y gobernanza del ciberespacio, de esta manera evitar la ampliación de las brechas digitales y desigualdades de acceso al internet y tecnologías.

En este marco, la existencia de agendas regionales en organismo regionales como el SICA, con su Agenda Regional Digital , Agenda Digital del Mercosur, o la Agenda Digital de la Alianza del Pacifico, con sus lineamientos y objetivos, podrían ser un espacios de coordinación y participación para sus integrantes, donde se impulse el entorno seguro y el respeto de los derechos de la ciudadanía en el internet.

Conclusión

Para finalizar, la ciberseguridad ha emergido como una prioridad estratégica para América Latina en medio de su creciente integración al ecosistema digital. Los riesgos que enfrentan los países de la región, como los ciberataques a infraestructuras críticas, la falta de capacidad de respuesta y la brecha digital,

requieren un enfoque coordinado y una visión clara de soberanía digital. No obstante, también hay oportunidades significativas para desarrollar políticas públicas que impulsen la colaboración y sinergia público-privada, inversión en investigación y desarrollo, fomento de una cultura de prevención y educación en ciberseguridad.

La experiencia de Chile con su "Ley Marco de Ciberseguridad" es un ejemplo del tipo de liderazgo que la región necesita para avanzar hacia una mayor resiliencia en el ciberespacio. A través de iniciativas como esta, América Latina puede fortalecer su posición, no solo en defensa de sus intereses nacionales, sino también en la construcción de un entorno digital más inclusivo y seguro. Al integrar agendas regionales como las del SICA, Mercosur o la Alianza del Pacífico, la región tiene la oportunidad de cerrar brechas, proteger los derechos de los ciudadanos y preparar a sus sociedades para los desafíos de un futuro cada vez más digital.

Este es un artículo de opinión. Las opiniones y contenido no reflejan o representan necesariamente la postura del CEERI como institución.