ARI 60/2023
7 de julio de 2023

Gobernanza público-privada de la ciberseguridad en América Latina: momento agridulce

Jorge M. Vega | Doctor en Seguridad Internacional

Tema

En América Latina la ciberseguridad es reconocida por países y organismos regionales como una responsabilidad multisectorial compartida. Sin embargo, la implementación práctica de esta dinámica colaborativa presenta claroscuros y carece de mediciones internacionales específicas que permitan su seguimiento y comparación.

Resumen

La ciberseguridad es una problemática de naturaleza transversal que afecta por definición a gobiernos, empresas y ciudadanos. Su gestión requiere, por ende, de enfoques posgubernamentales de gobernanza que fortalezcan la cooperación intersectorial y promuevan la consolidación de una cultura cibernética madura. Así lo expresan los principales estándares internacionales y lo refleja, por ejemplo, la Agencia de la Unión Europea (UE) para la Ciberseguridad (ENISA) en sus lineamientos y modelos para una "cibergobernanza" efectiva.[1]

Este análisis se centra en las empresas y la ciudadanía como actores principales de la ciberseguridad bajo un enfoque de gobernanza. Su objetivo es complementar la multiplicidad de análisis focalizados en el Estado, haciendo luz sobre los otros dos protagonistas de la tríada. La atención está puesta, por un lado, en sus responsabilidades, el estado de la educación y formación, y su aporte al desarrollo de una cibercultura común. Por otro lado, en el vínculo público-privado, es decir, en los puntos de contacto (deseables y reales) entre gobiernos y empresas.

Los resultados del análisis evidencian una disociación entre declamaciones y prácticas. Si bien los organismos regionales y las estrategias nacionales receptan casi sin excepción la centralidad de una gobernanza inclusiva y el dinamismo del vínculo público-privado, las puntuaciones obtenidas en diversas mediciones internacionales son bajas y el sector privado manifiesta desconocer las iniciativas públicas en la materia, desconfiar de la ayuda estatal y no considera que sus aportes sean tenidos en cuenta en el diseño de políticas públicas.

[1] ENISA (2023), "Building effective Governance frameworks for the implementation of National Cybersecurity Strategies".

Análisis

La gobernanza es una esfera prioritaria de la ciberseguridad. La interacción cooperativa entre actores públicos y privados es una condición necesaria (aunque no suficiente) para su gestión efectiva, porque las causas del problema radican en responsabilidades compartidas entre Estado y sociedad. Esta perspectiva es el fundamento de los estándares internacionales, que abogan por el diseño de políticas cibernéticas inclusivas de los intereses empresariales y sociales, apuntando a generar entornos de confianza que favorezcan su abordaje colaborativo.[2]

Los organismos regionales latinoamericanos son tributarios de esta perspectiva. Las normas, recomendaciones e iniciativas de la Organización de Estados Americanos (OEA), de la Alianza del Pacífico y del Sistema de la Integración Centroamericana (SICA) apuntan en esa dirección. La heterogeneidad geográfica y competencial del listado precedente evidencia que estamos en presencia de estándares comunes que aplican tanto a los regímenes cooperativos sobre seguridad y defensa como a los mecanismos de integración económica.

Este abordaje se replica a nivel doméstico. Buena parte de los países que disponen de estrategias o planes nacionales sobre ciberseguridad incluyen entre sus objetivos la creación de una cultura de ciberseguridad y entre sus postulados o premisas a la cooperación intersectorial (empresas, individuos, academia y ONG). Además, mencionan específicamente la colaboración público-privada como herramienta o vector asociativo. Tales son los casos, por ejemplo, de Brasil, Chile, Colombia, México, Panamá y Paraguay, que se mencionarán más adelante.

Sin embargo, existe un déficit en su implementación puesto de manifiesto a través de diversas mediciones internacionales. Estas refieren, entre otros puntos, a niveles incipientes de madurez en la incorporación efectiva de asociaciones público-privadas en las estrategias nacionales y en el desarrollo de una cultura cibernética en empresas y usuarios.[3] También evidencian que las empresas desconocen las iniciativas públicas en la materia, desconfían de la ayuda estatal y consideran que sus aportes no son considerados en el diseño de políticas.[4]

Panorama regional

La ciberdiplomacia latinoamericana presenta diferentes niveles, enfoques y velocidades. Su alcance temático abarca actualmente tanto los riesgos y amenazas propios de la ciberdelincuencia como la denominada cibereconomía, es decir, a la aplicación de las Tecnologías de la Información y las Comunicaciones (TIC) y la transformación digital

[2] Unión Internacional de Telecomunicaciones, Banco Mundial, Secretaría de la Commonwealth, Organización de Telecomunicaciones de la Commonwealth y Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (2018), "Guía para la elaboración de una estrategia nacional de ciberseguridad. Participación estratégica en la ciberseguridad", pp. 31-34.
[3] OEA y BID (2020), "Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe", Reporte Ciberseguridad.
[4] Centro de Política y Derecho de Ciberseguridad y Duke University (2023), "Informe LATAM CISO 2023: Perspectivas de Ciberseguridad de los Líderes de la Industria".

como vector para facilitar los negocios. La perspectiva securitaria tiene en la OEA a su máximo referente y la económica-privada se plasma a través de plataformas de integración subregionales, como la Alianza del Pacífico y del SICA en Centroamérica. Este mosaico de abordajes institucionales y heterogéneas connotaciones conceptuales sobre la noción de ciberseguridad presenta, sin embargo, un hilo conductor: la incorporación de una perspectiva de gobernanza para su conducción que promueve –al menos en los papeles– la cooperación intersectorial integrada, la consolidación de una cultura cibernética asertiva y la asociación estratégica entre gobiernos y empresas para compartir información, intercambiar buenas prácticas y vincular prioridades de financiación e innovación.

En la OEA la adscripción a este paradigma comienza en el plano normativo y se extiende al programático y metodológico. Tanto la "Estrategia de Seguridad Cibernética" (2004)[5] como la Declaración "Fortalecimiento de la Seguridad Cibernética en las Américas" (2012)[6] refieren expresamente a la cooperación del sector público con el privado y el académico para incrementar la educación y la concientización, sobre todo con relación a la protección de la infraestructura crítica de la información y las comunicaciones.

El Comité Interamericano contra el Terrorismo (CICTE), principal brazo ejecutor de la OEA en materia de ciberseguridad, plantea como uno de los objetivos de su Programa de Seguridad Cibernética aumentar el conocimiento e información sobre amenazas y riesgos cibernéticos entre interesados públicos y privados, la sociedad civil y los usuarios de internet. Asimismo, sus actividades de investigación y divulgación incluyen como destinatarios no sólo a los gobiernos de la región sino también a organizaciones privadas y a la sociedad civil.

Por su parte, el "Modelo de Madurez de la Capacidad de Ciberseguridad", cimiento metodológico del Observatorio de la Ciberseguridad en América Latina y el Caribe, asigna mejores calificaciones a los Estados cuanto mayor es el vínculo intersectorial. Entre las variables relevadas se encuentran, por ejemplo, la incorporación de asociaciones público-privadas en las estrategias nacionales, el desarrollo de una mentalidad de seguridad cibernética en empresas y usuarios y la existencia de mecanismos de colaboración entre sectores.

Es habitual además en la OEA la realización de publicaciones de forma colaborativa con asociaciones privadas como, por ejemplo, el libro *Tendencias de Seguridad Cibernética en América Latina y el Caribe* y el *Manual de Supervisión de riesgos cibernéticos para Juntas Corporativas*.[7] También la inclusión de artículos elaborados por universidades, *think tanks* y empresas en las publicaciones de su Observatorio (por ejemplo, el Centro de Estudios Estratégicos e Internacionales, el Foro Económico Mundial y la Universidad de Oxford).

[5] AG/RES. 2004 (XXXIV-O/04), "Adopción de una Estrategia Interamericana Integral de Seguridad Cibernética: un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética".
[6] Declaración CICTE/DEC.1/12 rev. 1.
[7] Desarrollados, respectivamente, con Symantec (2014) e Internet Security Alliance (2017).

En la Alianza del Pacífico la noción de ciberseguridad está asociada a la creación de un mercado digital regional y a la consolidación de una agenda digital compartida. Ambas líneas de acción incorporan un enfoque de gobernanza y refieren a la importancia de la cooperación y la coordinación continua entre el sector público, el privado, la academia y la sociedad civil. Así es mencionado expresamente, por ejemplo, en la Declaración Presidencial sobre el desarrollo del mercado digital regional y el impulso hacia la transformación digital (2020).

Asimismo, su Hoja de Ruta de la Agenda Digital (2016) –que incluye un apartado específico sobre seguridad digital– fue construida de forma conjunta con el sector privado. En sintonía, el Grupo de Agenda Digital (GAD) creado en consecuencia tiene entre sus funciones promover la articulación con el sector privado. La Declaración Presidencial de Puerto Vallarta (2018) reforzó esta mirada, imponiendo que el desarrollo de acciones sobre la Agenda Digital deba canalizarse a través de un mecanismo permanente de interlocución público-privado.

En el SICA la idea de gobernanza está presente en la Estrategia Regional Digital (ERDI) (2015), cuyo objetivo es facilitar la implementación de iniciativas públicas y privadas basadas en el diálogo y el intercambio de experiencias. A su vez, la Agenda Regional Digital 2022-2025 que operacionaliza la ERDI, incluye como objetivo estratégico del área de trabajo sobre economía digital el impulso de acuerdos estratégicos con líderes tecnológicos y el establecimiento de alianzas público-privadas que aceleren la transformación digital en la región.

Panorama nacional

En América Latina, 13 países disponen de una estrategia sobre ciberseguridad. Buena parte incorpora referencias sobre su gestión bajo un enfoque de gobernanza intersectorial y sobre la importancia de la colaboración público-privada como herramienta principal. El abordaje formal del asunto es, por ende, análogo al descrito en el plano regional. A título ilustrativo, se indica el contenido respectivo de las estrategias sobre ciberseguridad de Brasil, Chile, Colombia, México, Panamá y Paraguay.

- Brasil: la Estrategia Nacional de Seguridad Cibernética (2020) plantea entre sus acciones estratégicas fortalecer la cibergobernanza y ampliar la asociación entre el sector público, el privado, la academia y la sociedad.
- Chile: la Política Nacional de Ciberseguridad (2017) tiene por objetivos desarrollar una cultura de ciberseguridad con relación al uso responsable de las TIC y la educación, y promover una industria de la ciberseguridad alineada con los objetivos nacionales.
- Colombia: la Política Nacional de Seguridad Digital (2016) define a la gobernanza y a la cultura ciudadana como dimensiones estratégicas. Su objetivo general refiere a la cooperación, colaboración y asistencia entre partes interesadas.
- México: la Estrategia Nacional de Ciberseguridad (2017) tiene por principio rector la colaboración de múltiples actores y como ejes transversales la cultura de

ciberseguridad y la colaboración con la sociedad civil, la academia y las empresas.

- Panamá: la Estrategia Nacional de Ciberseguridad (2021) plantea como principio la responsabilidad de todos los sectores en la temática y presenta entre sus pilares el fomento de una cultura nacional de ciberseguridad.
- Paraguay: el Plan Nacional de Ciberseguridad (2017) tiene por principio la responsabilidad compartida entre todos los miembros de la sociedad. Entre sus ejes se menciona la sensibilización, la cultura y la coordinación intersectorial en I+D+I.

Este reconocimiento formal no se armoniza con la práctica institucional que reflejan diversas mediciones e investigaciones internacionales.

Tal es así que, según el Reporte Ciberseguridad 2020 de la OEA y el Banco Interamericano de Desarrollo (BID), sólo un país (Colombia) alcanza el nivel más alto (dinámico) en el desarrollo de una estrategia de ciberseguridad, categoría que conlleva el empleo extendido de asociaciones público-privadas. La amplia mayoría sólo obtiene un nivel inicial, formativo o consolidado en este punto, con las excepciones de Uruguay y Chile que alcanzan un nivel estratégico.[8]

Dicho reporte también pone de manifiesto la escasez de mecanismos formales e informales de colaboración entre actores públicos y privados para luchar contra la delincuencia cibernética. De hecho, ningún país de la región alcanza un nivel dinámico en este aspecto, agrupándose la amplia mayoría en un nivel inicial o formativo respecto de sendos tipos de marcos legales. Sólo Chile, Costa Rica y Paraguay ostentan un nivel consolidado en ambos casos y Uruguay es el único país en alcanzar un nivel estratégico en alguno de ellos (marcos informales).

Tales hallazgos se condicen con los resultados exhibidos en el Informe LATAM CISO 2023,[9] confeccionado según una encuesta practicada a directores de seguridad de la información (o cargos similares) en 195 organizaciones latinoamericanas públicas, privadas y no gubernamentales de diferentes tamaños y sectores.

El informe indica que la mitad de los encuestados no siente que sus aportes sean tomados en cuenta en el desarrollo de políticas públicas, regulaciones e iniciativas asociadas. En sintonía, el 75% sostiene tener una baja o moderada confianza en la ayuda del Estado para dar respuesta a ataques cibernéticos. De hecho, el 32% afirma directamente desconocer a qué dependencia pública contactar o cómo contactarla en una situación como esa. Además, el 51% afirma no pertenecer a ninguna organización de intercambio de información sobre ciberseguridad.

[8] El modelo de madurez de la capacidad cibernética de la OEA y el BID plantea cinco etapas o niveles de madurez: inicial, formativo, consolidado, estratégico y dinámico.
[9] Centro de Política y Derecho de Ciberseguridad y Duke University (2023); “Informe LATAM CISO 2023: Perspectivas de Ciberseguridad de los Líderes de la Industria”, p. 22.

El horizonte no es distinto en el plano cultural. Según el citado Reporte Ciberseguridad 2020, ninguno de los países alcanza un nivel estratégico o dinámico en términos de mentalidad de seguridad cibernética en el sector privado y en la sociedad. Solo Chile, México y Uruguay alcanzan un nivel consolidado en ambos sectores.

El déficit también alcanza al plano educativo-formativo. Según el Índice Nacional de Ciberseguridad (INCS) de la *e-Governance Academy* (eGA) únicamente Argentina y Panamá incluyen el tema en el nivel primario y secundario, y sólo la mitad de los países de la región lo incorpora en el nivel universitario de grado. Ecuador y Uruguay son los únicos que disponen de doctorados sobre ciberseguridad. El INCS destaca, no obstante, que la amplia mayoría cuenta con maestrías y con asociaciones profesionales sobre ciberseguridad.

Existen no obstante diversas prácticas institucionales para destacar, por ejemplo:

- la Alianza Chilena de Ciberseguridad, que aglutina a instituciones públicas, privadas y académicas para promover la educación y sensibilizar a la ciudadanía;
- el Comité de Seguridad Digital en Colombia, encargado de los temas que afectan transversalmente a todos los sectores;
- el Centro de Ciberseguridad en Guyana, creado entre gobierno y sector privado para formar policías, empresarios y ciudadanos sobre la temática;
- y el Programa de Fortalecimiento en Ciberseguridad e Investigación del Cibercrimen en Argentina, en el marco del cual se firmaron convenios de intercambio de información con empresas multinacionales.

Conclusión

Si en Europa la cooperación público-privada en ciberseguridad vive un momento dulce, en América Latina la situación puede rotularse como “agridulce”, caracterización que no abarca únicamente al vínculo entre gobiernos y empresas sino, en general, la gobernanza intersectorial de la problemática. La deuda radica en un déficit de implementación, porque a nivel regional y nacional se reconocen estándares de vanguardia, pero su aplicación práctica adolece de claroscuros puestos en evidencia por diversas mediciones internacionales.

Cabe destacar, por otra parte, la ausencia de investigaciones específicas sobre la existencia y práctica de asociaciones público-privadas en el campo de la ciberseguridad. El modelo de medición de la OEA y el BID no incluye este punto. El Índice de Ciberseguridad Global de la Unión Internacional de Comunicaciones lo incorpora, pero los resultados no se detallan por país. Esta carencia priva a la región de contar no sólo con un diagnóstico actualizable sino, sobre todo, con un reservorio de consulta sobre buenas prácticas y lecciones aprendidas.

Puede ser útil a tales fines afianzar la cooperación técnica euro-latinoamericana. Si bien la institucionalidad de ambas regiones en la materia es muy distinta, Europa cuenta con

una consolidada trayectoria de políticas, estándares y estudios sobre gobernanza y colaboración público-privada en el campo de la ciberseguridad que serían de interés para los países de la región. Sirven como ejemplo los lineamientos y herramientas diseñadas por ENISA para formular estrategias nacionales de ciberseguridad y emplear asociaciones público-privadas.

También el caso español es una referencia de interés. Tanto por las Jornadas STIC, promovidas en América Latina y el Caribe bajo un enfoque iberoamericano por un conjunto de organismos españoles, como por el Foro Nacional de Ciberseguridad, creado por la Estrategia Nacional de Ciberseguridad 2019 para fomentar la cultura de ciberseguridad, ofrecer apoyo a la industria e I+D+i, y promover la formación y el talento en un entorno de colaboración público-privada, cuya labor se materializa a través de grupos de trabajo de liderazgo compartido.