ARI 17/2023
15 de marzo de 2023

El sector de ciberseguridad en América Latina: apuntes para leer un mapa del estado en construcción

Jorge M. Vega | Doctor en Seguridad Internacional | @JorgeMVega1

Tema

En América Latina las capacidades estatales para gestionar una política de ciberseguridad efectiva están en construcción, conviviendo múltiples y cambiantes niveles de madurez entre subregiones y países. La complejidad del panorama regional impone la formulación de aportes analíticos policy oriented como el presente, que contribuyan a su cabal comprensión.

Resumen

La gestión de la ciberseguridad es un imperativo estratégico para la administración pública contemporánea. Los principales baremos internacionales coinciden en definir la gobernanza institucional, la cooperación internacional y la colaboración público-privada como sus aspectos prioritarios. La creación de una estructura gubernamental acorde deviene un requisito fundacional, cuyo diseño está asociado fundamentalmente a la creación de instancias rectoras competentes y mecanismos que aseguren la coordinación interagencial.

Este análisis procura caracterizar el estado de la situación del respectivo entramado institucional en América Latina. Para ello recurre a una combinación de fuentes internacionales, cuyo empleo permite la comprensión de los hallazgos desde latitudes extrarregionales y la comparabilidad de los datos en una región de configuración y capacidad estatal heterogénea. El foco está puesto, entonces, en la organización del sector, indagando sobre su adecuación a estándares y la presencia de modelos comunes o particularidades nacionales.

Los resultados de la investigación presentan a América Latina como una región con capacidades estatales incipientes –aunque crecientes– en el campo de la ciberseguridad; también como una región con sustantivas disparidades entre subregiones y países. Se destaca como tendencia, asimismo, el cambio continuo en la disposición de la arquitectura institucional responsable, factor que hace más complejo su estudio, el diseño de iniciativas de cooperación técnica norte-sur y la consolidación de colaboraciones entre el ámbito público y el privado.

Análisis

El sector público de la ciberseguridad en América Latina está en construcción. A pesar de registrarse avances en la dirección correcta desde fines del siglo XX, el desarrollo de una política de ciberseguridad efectiva se encuentra todavía en etapas iniciales o formativas. Esta situación impele a poner el acento analítico en su organización y funcionamiento, aspecto liminar de su proceso evolutivo dada la centralidad del diseño institucional como condición de contexto necesaria para concebir estrategias sectoriales y políticas contribuyentes.

Los estudios sobre el asunto bajo una perspectiva regional son embrionarios, porque su análisis se circunscribe generalmente a casos nacionales y porque los enfoques de corte regional se focalizan en otros aspectos o dimensiones de interés, por ejemplo, en el ciclo de vida y contenido programático de las estrategias sectoriales existentes.[1] No obstante, son de insoslayable consideración diversas mediciones internacionales que proliferaron en el último quinquenio y permiten construir una mirada regional a partir de datos nacionales comparables.

Con ello se hace referencia a los índices desarrollados por la Unión Internacional de Comunicaciones (UIT), la e-Governance Academy (eGA) y la Organización de Estados Americanos (OEA) en colaboración con el Banco Interamericano de Desarrollo (BID). Si bien cada institución se apoya en una metodología de cuño propio, todas incluyen a América Latina en su universo de análisis y coinciden en identificar a la gobernanza institucional como dimensión prioritaria de investigación, aportando así datos de interés sobre los países de la región.

Sin pretensiones de exhaustividad, este análisis se plantea mitigar ese vacío analítico aportando elementos que funcionen como hoja de ruta para interpretar el mapa del Estado del sector ciberseguridad en América Latina. Sus destinatarios son tanto los hacedores latinoamericanos de políticas públicas de cara a la mejora continua de la gestión sectorial, como los *partners* públicos y privados extrarregionales interesados en la ciberseguridad como objeto de iniciativas de diplomacia cibernética y articulación público-privada.

Notas sobre estándares aplicables

Las fuentes internacionales de referencia –UIT, eGA y OEA-BID– presentan una visión compartida sobre las buenas prácticas que deberían orientar la gobernanza institucional del sector. En términos generales, promueven la creación de autoridades específicamente competentes (rectoras de alcance transversal y ejecutoras por dependencias) y de mecanismos de coordinación intragubernamental entre dependencias clave. Ello en el más alto nivel ejecutivo institucional y a través de asignaciones específicas e inequívocas de funciones.

[1] 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".

En lo específico, el Índice Nacional de Ciberseguridad (INCS) del eGA enmarca el tema en su dimensión "Desarrollo de Políticas de Ciberseguridad" y plantea como indicadores la presencia de una autoridad central responsable y de un formato de coordinación de la política sectorial. En sintonía, el Índice de Ciberseguridad Global (ICG) de la UIT refiere a la existencia de una agencia nacional responsable (y de mediciones) como parte del conjunto de "medidas institucionales" de naturaleza organizativa que promueve.

En el ámbito continental, el Observatorio de la Ciberseguridad en América Latina y el Caribe auspiciado por la OEA y el BID se apoya en el "Modelo de Madurez de la Capacidad de Ciberseguridad" (MMCC). Su dimensión "Política y Estrategia de Ciberseguridad" incorpora el campo "organización" para cotejar la existencia de una entidad nacional coordinadora, con un presupuesto consolidado y métricas de seguimiento. El MMCC clasifica los resultados en cinco etapas de madurez: inicial, formativo, consolidado, estratégico y dinámico.

Cabe destacar otro común denominador de sendas mediciones internacionales: la valorización de las Estrategias Nacionales de Ciberseguridad (ENC) como herramienta principal para la gestión del sector, a tal punto que la UIT las califica como "piedra angular de las medidas institucionales".[2] En concreto, el planteamiento subyacente se refiere a las ENC como condición facilitante para una gobernanza institucional adecuada, siendo las estrategias, la organización y la coordinación interdepartamental variables de una misma dimensión analítica.

El INCS y el MMCC tratan específicamente el abordaje institucional de la ciberseguridad en el ámbito militar y de defensa. La mirada del INCS esta puesta en la existencia de una unidad en las Fuerzas Armadas especializada en planificar y conducir tales operaciones. El MMCC dedica un capítulo a la defensa cibernética en el marco de su dimensión política y estratégica. Pondera la existencia de una estrategia, de una estructura conjunta de mando y control, la intervención del ministerio responsable y la coordinación entre los actores del sistema de defensa.

Datos con enfoque regional

Las mediciones de la UIT y del eGA permiten visualizar el estado del sector de ciberseguridad en América Latina bajo una perspectiva global, comparando su desarrollo con el de otras regiones y agregaciones de países. Siguiendo a Aguilar Antonio, este ejercicio arroja resultados desfavorables para la región, toda vez que según el ICG 2018 América Latina sólo supera en calificación a Asia y a Oceanía y, tomando los datos del INCS 2019, sólo a Oriente Medio y África, presentando en ambos casos resultados por debajo de la media global registrada.[3]

[2] Unión Internacional de Telecomunicaciones (2021), "Índice Mundial de Ciberseguridad", p. 9.
[3] Aguilar Antonio, J.M. (2020), "La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas", *Revista de Estudios en Seguridad Internacional*, vol. 6, nº 2, pp. 31-32.

La medición de la OEA y el BID permite focalizar la mirada al interior de la región y bajo un prisma intertemporal. Según su informe de 2020, América Latina mejoró desde 2016 las capacidades estatales de ciberseguridad. Sin embargo, este avance es calificado por las propias autoridades de tales organismos como "tímido"[4] porque la madurez promedio de las capacidades sectoriales sólo oscila entre etapas iniciales y formativas, entre otros factores, por el carácter *ad-hoc* de las medidas aplicadas y la falta de articulación de políticas entre actores clave.[5]

Una visión con perspectiva geográfica sobre este panorama exhibe significativas diferencias subregionales. Según dicho informe de la OEA y el BID, los países del Cono Sur presentan el nivel más alto en las cinco dimensiones del MMCC (entre "formativo" y "establecido"), mientras que en el Grupo Andino el promedio de madurez es apenas "formativo", y en Centroamérica y México fluctúa entre "inicial" y "formativo" según la dimensión. Por su parte, el nivel de madurez del Caribe en todas las dimensiones está entre "inicial" y "formativo".[6]

En el plano específico de la gobernanza institucional, ninguno de los países alcanzó la puntuación máxima del MMCC 2020 (nivel "dinámico") en el componente organizacional relativo a las ENC. De hecho, entre América Latina y el Caribe sólo 12 países habían aprobado a esa fecha una ENC y únicamente 10 conformado un órgano central para la gestión del sector ciberseguridad.[7] En esta misma línea, según se desprende del ICG 2020, las medidas institucionales no son el pilar con mejor desempeño en casi la totalidad de los países del continente.

Un pantallazo sobre la gobernanza institucional, pero en el ámbito puntual de la defensa, muestra según el MMCC 2020 que ningún país alcanzó el nivel "estratégico". También permite identificar diferencias subregionales, porque mientras Centroamérica obtuvo de forma unánime una calificación "inicial" en defensa cibernética, su nivel promedio en Sudamérica oscila entre "formativo" y "consolidado". Cabe agregar que, según el INCS, solo siete países de toda América Latina cuentan con unidades especializadas en ciberseguridad en las Fuerzas Armadas.

A pesar de ello, Sadie Creese –directora del Centro Global de Capacidad en Seguridad Cibernética de la Universidad de Oxford[8]– afirma que la dimensión "Política y Estrategia" del MMCC ha "progresado más que otras" desde la primera medición del modelo en 2015. Asimismo, destaca que "los países con mejoras en el contenido o en los procesos de desarrollo de sus estrategias nacionales de ciberseguridad tuvieron mayores avances en todos los ámbitos, lo que indica que invertir en un enfoque estratégico tiene resultados positivos para la ciberseguridad".

[4] OEA y BID (2020), "Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe", *Reporte Ciberseguridad 2020*, p. 11.
[5] *Ibid*., p. 17.
[6] *Ibid*., p. 17.
[7] *Ibid*., p. 11.
[8] *Ibid*., p. 21.

Puntuación de precisiones nacionales

Colombia y Uruguay son los países con mejor calificación organizativa según el MMCC 2020, siendo los únicos que alcanzaron un nivel "estratégico" en este componente. En Colombia se destaca la creación de un Coordinador Nacional de Seguridad Digital (Departamento Nacional de Planeación) y de una Comisión Nacional Digital y de Información Estatal como instancia de coordinación intragubernamental. En Uruguay la conducción técnica sectorial radica en la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC).

Chile, Argentina y Panamá integran el lote de países que han alcanzado, en cambio, un nivel de madurez organizativo "consolidado". La rectoría del sector en Chile está en el Ministerio del Interior y Seguridad Pública, que preside el Comité Interministerial sobre Ciberseguridad (CICS). En Argentina la función es ejercida por la Jefatura de Gabinete de Ministros, cartera que preside el Comité de Ciberseguridad. En Panamá las tareas radican en la Autoridad Nacional para la Innovación Gubernamental y el Consejo Nacional para la Innovación Gubernamental.

Brasil, México, Paraguay y Costa Rica registraron, por su parte, un nivel "formativo" de madurez organizativa.[9] Brasil dispone en el ámbito de Presidencia de un Departamento de Seguridad de la Información y Cibernética, asesorado por un Comité Gestor de la Seguridad de la Información (CGSI) de composición interdepartamental. En México funciona, en cambio, una Subcomisión de Ciberseguridad en el marco de la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE), órgano colegiado de coordinación intragubernamental.

Paraguay y Costa Rica localizan la coordinación nacional del sector en las carteras responsables de gestionar las TIC: Ministerio de Tecnologías de la Información y Comunicaciones (MITIC) en Paraguay y Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) en Costa Rica. Paraguay cuenta a su vez con una Comisión Nacional de Ciberseguridad encargada de la coordinación de políticas interdepartamentales, mientras que en Costa Rica el MICITT dispone de un Comité Consultivo integrado por organismos públicos, privados y académicos.

Con relación a la gobernanza de la ciberseguridad en el ámbito de la defensa, Argentina, Paraguay, Uruguay, Brasil, Chile, México y Colombia son los que presentan una mejor calificación organizacional según el MMCC 2020 (nivel "consolidado"), contando con estructuras específicas para conducir el sector. Sólo Colombia y Uruguay mantienen esta puntuación en términos de coordinación interinstitucional, siendo Colombia el único país de la región en ostentar un nivel "estratégico" en la formulación de una estrategia de defensa cibernética.

Corresponde complementar esta mirada institucional con una semblanza sobre el desarrollo regional de ENC, considerando el efecto cascada que tienen en la mejora de todos los pilares de la política sectorial. Si bien su estudio requiere un análisis específico,

[9] Al igual que Bolivia, Ecuador, Guatemala, Perú, Belice y Surinam. Completan el listado regional, pero con un nivel "inicial", El Salvador, Honduras, Nicaragua, Venezuela y Guyana.

cabe mencionar que buena parte de América Latina dispone ya de un documento de tales características: Panamá (2013), Colombia (2011, 2016), Paraguay (2017), Chile (2017), Costa Rica (2017), México (2017), Guatemala (2018), Argentina (2019), Nicaragua, (2020), Brasil (2020) y Ecuador (2022).

El informe de 2020 de la OEA y el BID vuelve a ser de utilidad a tales fines, aportando un diagnóstico comparable sobre su desarrollo y contenido. Sin perder de vista que algunos países aprobaron una ENC con posterioridad a dicha medición, sus resultados indican que Colombia está a la vanguardia del pilar (nivel dinámico-estratégico), seguido por Chile y Uruguay (nivel estratégico-consolidado), y luego por Costa Rica, Guatemala, México, Paraguay y Panamá (nivel estratégico). El resto presenta niveles formativos (como Argentina y Brasil) o bien iniciales.

Conclusión

En América Latina la capacidad estatal en ciberseguridad es una construcción en presente continuo. Así lo evidencian las principales fuentes internacionales –propias y ajenas– que miden su desarrollo o madurez. Esta afirmación comprende la gobernanza institucional de la ciberseguridad como sector de políticas, es decir, al andamiaje orgánico-funcional a partir del cual los gobiernos procuran gestionar la problemática. De suyo, no es este un tema menor, dada la centralidad del diseño organizacional para calibrar estrategias y obtener resultados.

En este contexto, interpretar el mapa del estado sectorial presenta al menos dos obstáculos para el lector interesado. Primero, las disparidades subregionales, que hacen compleja una caracterización regional uniforme y obligan a aplicar abordajes analíticos por países o grupos reducidos de países para obtener datos comparables de utilidad. Segundo, los asiduos cambios orgánicos experimentados en la conducción del sector, que exigen la monitorización permanente de normas y estructuras vigentes como requisito ineludible para análisis conducentes.

Las hojas de ruta que se diseñen a tales fines deben asumir que niveles disímiles de madurez y modelos diferentes de gobernanza son parte del paisaje habitual en el mapa latinoamericano del estado responsable de la ciberseguridad. Esto representa un desafío, pero también una oportunidad para la cooperación técnica para el desarrollo y la colaboración público-privada, otras dos dimensiones de absoluta centralidad en las buenas prácticas sectoriales promovidas por las fuentes internacionales especializadas en la gestión pública de la ciberseguridad.