Amenazas emergentes en ciberseguridad: implicaciones para América Latina y el Caribe

Nayia Barmpaliou,
Jefa de Políticas e Iniciativas Públicas
Centro para la Ciberseguridad,
Foro Económico Mundial

La ciberseguridad en la era de la hiperconectividad y las pandemias

La pandemia mundial del COVID-19 ha marcado un punto de inflexión fundamental en nuestra senda mundial y ha acentuado como nunca antes nuestra dependencia de la infraestructura digital. Si bien esta crisis ha expuesto las deficiencias estructurales que nuestra sociedad ha venido acarreando en múltiples sistemas –tales como salud, economía, empleo y educación–, también ha resaltado el papel catalizador de la tecnología en la forma en que hemos enfrentado colectivamente la pandemia.

En un lapso de tres meses, experimentamos una aceleración de la transformación digital que se había anticipado que ocurriría en tres años.[15] Con el tiempo, nuestra transición a la era "digital de todo" ha reconfigurado profundamente nuestra vida profesional y personal. Incluso en el entorno más disruptivo de la pandemia, Internet y la infraestructura digital global han hecho posible la provisión de servicios esenciales, han permitido a las empresas continuar operando y han sostenido nuestros contactos sociales individuales. El resultado de esta transición ha sido un extraordinario aumento de la superficie de ataque cibernético, en el contexto de un ecosistema digital de vulnerabilidades ya amplificadas que incluye más de 20.000 millones de dispositivos de Internet de las cosas (IoT, por sus siglas en inglés) conectados en todo el mundo.[16]

Incluso antes de la pandemia, las brechas de ciberseguridad y las filtraciones de datos se estaban convirtiendo en los principales obstáculos de la economía digital. Los cibercriminales aprovechan rápidamente los nuevos vectores de ataque y se benefician de los vacíos en la cooperación de las fuerzas del orden público en las diferentes jurisdicciones, dada la naturaleza inherentemente transnacional de sus actividades maliciosas. A su vez, el riesgo de ataques cibernéticos en infraestructura crítica y fraude o robo de datos ha sido siempre una prioridad para los líderes empresariales a nivel mundial. Según el Informe de Riesgos Globales 2020 del Foro Económico Mundial,[17] el riesgo de ciberataques a la infraestructura crítica y el fraude o robo de datos se clasificaron entre los 10 principales riesgos con mayor probabilidad de ocurrir, mientras que la reciente Perspectiva de Riesgos del

COVID-19 del Foro Económico Mundial[18] identificó los ciberataques como la tercera mayor preocupación debido a nuestra actual y sostenida transición hacia los patrones de trabajo digital.

Los datos disponibles respaldan estas preocupaciones; se estima que los daños por delitos cibernéticos alcanzarán los US$6 billones para 2021, lo que equivale al producto interno bruto (PIB) de la tercera economía más grande del mundo.[19] Además del costo financiero, el cibercrimen y los ciberataques socavan la confianza de los usuarios en la economía digital. Las encuestas indican que, de la población mundial con acceso a Internet, menos del 50% confía en que la tecnología mejorará sus vidas, lo que demuestra una creciente y profunda falta de confianza con respecto a la privacidad de los datos.[20]

Estas tendencias son particularmente pertinentes para la región de América Latina y el Caribe (ALC), que en los últimos cinco años ha sido testigo de una enorme expansión en el uso de las tecnologías de la información y la comunicación (TIC). A medida que la región avanza cada vez más hacia la economía digital, aumenta la necesidad de garantizar la confianza digital. Los protocolos de gestión de riesgos de seguridad digital y protección de la privacidad constituyen responsabilidades compartidas por los gobiernos, el sector privado y los usuarios individuales en una economía cada vez más impulsada por los datos.[21] Gracias a la priorización de la creación de capacidad de seguridad cibernética en la agenda de desarrollo de la región, producto de los esfuerzos coordinados e intensificados del Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA) en los últimos años, la necesidad de integrar la ciberseguridad y la lucha contra el cibercrimen en las estrategias y políticas digitales de la región también se ha reflejado al más alto nivel como parte de la "Propuesta de Agenda Digital para América Latina y el Caribe".[22]

Un asunto transversal en la política nacional

La intrusión del continuo digital en todas las áreas de actividad humana, así como los niveles sin precedentes de innovación e interdependencia tecnológicas, han hecho que sea imposible tratar la ciberseguridad de forma aislada, como un asunto técnico o un área de políticas independiente. En los últimos años, la ciberseguridad ha roto la barrera de los silos técnicos y se encuentra en la intersección de múltiples disciplinas y áreas de políticas: acceso digital y conectividad, resiliencia, justicia penal, diplomacia, seguridad y defensa internacional, y economía digital y comercio, así como las nuevas tecnologías. En tanto que las naciones intentan cosechar los beneficios de la Cuarta Revolución Industrial, la seguridad cibernética se ha ganado un lugar en el enfoque de la política global. Esto ha resultado en un incremento significativo de la adopción o revisión de estrategias nacionales de ciberseguridad que adquieren un enfoque de todo el gobierno o, incluso a veces, de toda la sociedad, así como de la puesta en marcha o la adaptación de legislación nacional sobre cibercrimen, especialmente en países en desarrollo que no contaban con tales leyes vigentes.

Este informe proporciona evidencia prometedora de que los gobiernos de la región de ALC han dado importantes pasos en el desarrollo y la eficacia de sus estrategias nacionales de seguridad cibernética, que también han servido como vehículos para mejorar la cultura y las prácticas nacionales de seguridad cibernética desde su última encuesta, realizada en 2016. Además, desde entonces, cuatro países de ALC se han unido al Convenio sobre Cibercrimen del Consejo de Europa (o "Convenio de Budapest"), cuyo objetivo es promover una política penal común contra el cibercrimen, ofreciendo un marco común de legislación nacional y cooperación internacional.

Fracaso y oportunidad del mercado para la ciberseguridad en la economía digital

El rápido avance de las tecnologías digitales pone de relieve las grandes innovaciones, pero también crea nuevas vulnerabilidades a un ritmo más rápido de lo que se las puede atender. Hasta la fecha, el desequilibrio entre el tiempo de comercialización y el "tiempo de seguridad" sigue siendo una cuestión predominante, debido a la presión de las fuerzas del mercado en favor de los productos de nuevas tecnologías, sin incentivos para priorizar los elementos de seguridad desde el inicio del ciclo de vida del producto[23].

Es llamativo que, a pesar los cambios perceptibles en el comportamiento de los consumidores con respecto a las crecientes preocupaciones sobre privacidad y seguridad, los objetivos del mercado no se estén adaptando con suficiente rapidez, lo cual conducirá inevitablemente a diferentes experimentos en términos de intervenciones y regímenes regulatorios. Por ahora, vemos que la habitual falta de un enfoque de "seguridad por diseño" en las innovaciones tecnológicas ha generado una tendencia hacia esquemas de certificación voluntaria en ciberseguridad para productos TIC, por ejemplo en la Unión Europea y Singapur, y hay más países que se centran específicamente en el IoT. En el otro extremo del espectro, esta falla del mercado ha dado lugar a la ciberseguridad como uno de los sectores más diversos y de rápida expansión en todo el mundo. Antes de la crisis del COVID-19, se esperaba que el gasto global en productos y servicios de seguridad cibernética aumentara en un 88% en los próximos ocho años.[24] La recesión económica causada por la pandemia podría conducir a la consolidación de este mercado. En el caso de ALC, a medida que la región avanza hacia una mayor madurez en su seguridad cibernética, es importante que las estrategias de implementación de ciberseguridad nacional consideren medidas orientadas a limitar el riesgo de una mayor superficie de ataque, y que se inspiren en los estándares existentes o en esquemas voluntarios.

El imperativo estratégico de ciberseguridad empresarial

En los últimos cinco años, la noción de que la estrategia de ciberseguridad forma parte integral de la estrategia comercial ha ganado más tracción e implementación real por parte de las empresas. Esto se debe en parte a la publicidad alusiva a ciertas grandes brechas en materia de seguridad, así como a mayores consideraciones legales y regulatorias, incluyendo la entrada en vigor en mayo de 2018 del Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) de la Unión Europea, el cual tiene un impacto significativo a nivel global. En la práctica, este ha sido un factor clave para que los líderes empresariales y las juntas corporativas comprendan mejor los riesgos cibernéticos de su modelo operativo comercial y logren el equilibrio adecuado entre proteger la seguridad de sus activos, mitigar las pérdidas y mantener la rentabilidad en un ambiente competitivo.

Esta mayor conciencia a nivel del liderazgo corporativo es un primer paso crucial para potenciar la toma de decisiones corporativas informadas para la planificación de la seguridad cibernética, los mecanismos de respuesta y las inversiones. El lanzamiento en 2019 del "Manual de Supervisión del Riesgo Cibernético para las Juntas Corporativas" por parte de la OEA y de la Alianza por la Seguridad en Internet[25] marcó un importante esfuerzo consultivo para crear tal conciencia en la región de ALC entre las partes interesadas de las juntas corporativas, la alta gerencia, los gobiernos y la academia, y adaptar el asesoramiento a las particularidades regionales.

Mientras tanto, a medida que las empresas más grandes han estado invirtiendo más en ciberseguridad y en innovación en materia de seguridad, los análisis recientes señalan un aumento significativo de los ataques dirigidos a pequeñas y medianas empresas (pyme). Esto crea un riesgo significativo en el ecosistema digital, especialmente teniendo en cuenta que las pyme no tienen los recursos financieros para invertir fuertemente en ciberseguridad, o simplemente la cultura de seguridad no constituye

uno de los principales impulsores de sus agendas. De hecho, los desafíos que enfrentan estas firmas para asegurar su entorno digital en términos de falta de recursos financieros o cultura de seguridad son bastante diferentes de los de las organizaciones más grandes. Al reflexionar sobre esta realidad en el contexto regional de ALC, cabe considerar que, según la Organización para la Cooperación y el Desarrollo Económicos (OCDE), la estructura económica de ALC está compuesta en un 99,5% por micro, pequeñas y medianas empresas (mipyme).[26] Por lo tanto, aumentar la conciencia de seguridad cibernética y promover la higiene básica de seguridad cibernética en las pyme de la región debería ser una prioridad crítica en los próximos años.

Las nuevas tecnologías reestructuran el panorama de ciberseguridad y de políticas

Las tecnologías "antiguas" y "nuevas" no solo están reestructurando la industria y el panorama de la ciberseguridad, sino que desafían más ampliamente las formas tradicionales de operación de la sociedad. La convergencia de las tecnologías de la información con la tecnología operativa y los sistemas heredados ya plantea grandes desafíos en todo el ecosistema digital. La aparición de nuevas tecnologías y sus aplicaciones, tales como inteligencia artificial, big data, redes de quinta generación, computación en la nube, IoT y computación cuántica, cuestionan drásticamente nuestro pensamiento convencional sobre el futuro de la economía digital. Por un lado, ofrecen inmensas oportunidades de eficiencia e innovación, pero también amplifican la superficie de ataque y pueden crear riesgos de seguridad y privacidad de datos todavía desconocidos. Por esta razón, las empresas y los gobiernos deben trabajar juntos para desarrollar una comprensión sólida de los riesgos emergentes de ciberseguridad relacionados desde una perspectiva de políticas, de los riesgos y de las operaciones. Parte del desafío será fomentar la confianza entre las diferentes partes interesadas del ecosistema para reducir la fricción en los actuales modelos regulatorios y de aseguramiento. Vale destacar que, para los países de la región de ALC y otras economías emergentes, estos problemas de seguridad incipientes deberán abordarse de una manera que no exacerbe las barreras para acceder a los beneficios de las nuevas tecnologías.

La ciberseguridad en una arquitectura global fragmentada y polarizada

En la era de un orden global multipolar y multiconceptual, el contexto geopolítico y social influye en el desarrollo de la tecnología y a la vez también se ve afectado por la tecnología. Por un lado, la aparición de nuevas tecnologías tiene el potencial de reorganizar significativamente las dinámicas y alianzas geopolíticas, mientras que actualmente la convergencia de nuevas tecnologías con aplicaciones tradicionales desempeña un papel importante en la amplificación de las tensiones existentes alrededor de los valores de gobernanza de una Internet abierta y descentralizada, versus el enfoque en la "cibersoberanía", o el uso del ciberespacio como un entorno para la competencia estratégica. Tal polarización puede socavar tanto la seguridad en el ciberespacio como la confianza para la cooperación global contra los desafíos comunes de ciberseguridad. Los enfoques divergentes de las principales potencias cibernéticas en relación con la forma en que se aplica el derecho internacional en el ciberespacio, la cual se encuentra en discusión en los foros relevantes de Naciones Unidas,[27] reflejan un entorno internacional bastante conflictivo, exacerbado aún más por los llamados a la "autonomía estratégica" digital, lo que incluso sería problemático lograr en un contexto de rápido cambio tecnológico y cadenas de valor globales.

En este marco, las organizaciones regionales se han posicionado como actores clave en la promoción de la estabilidad regional, la seguridad y los esfuerzos para fomentar la confianza en el ciberespacio mediante medidas de generación de seguridad. La región de ALC también ha demostrado un progreso significativo en esta dirección, cuando en 2017 el Comité Interamericano contra el Terrorismo de la OEA instauró el Grupo de Trabajo sobre Medidas de Fomento de Cooperación y Confianza en el Ciberespacio.[28]

La necesidad de un cambio de paradigma en la cooperación público-privada

La naturaleza intrínsecamente compleja y diseminada del ecosistema digital, junto con las múltiples dimensiones de la política cibernética pública y corporativa, ha creado con el tiempo una arquitectura complicada de partes interesadas. La digitalización ha transformado nuestra sociedad en un "sistema de sistemas", donde las funciones críticas se distribuyen entre los actores públicos y privados en ubicaciones dispersas y con interdependencias complejas. Por lo tanto, los últimos años nos han enseñado que la cooperación público-privada en materia de ciberseguridad requiere pensar fuera de los formatos tradicionales y rígidos para superar las barreras y ser verdaderamente efectivos. Para abordar esta elevada complejidad y responsabilidad compartida, necesitamos una nueva generación de alianzas público-privadas que invaliden el "pensamiento en silos" y adopten un enfoque sistémico para navegar la dinámica compuesta de los factores de políticas, tecnológicos, económicos, sociales y geopolíticos que dan forma al entorno de riesgo de ciberseguridad y sus interdependencias. A medida que los países de la región de ALC aceleran su transformación digital, tienen la oportunidad de entretejer tal pensamiento sistemático en su arquitectura de cooperación público-privada, pudiendo este ser un factor diferenciador para su resistencia cibernética.

Conclusión

El carácter complejo de la ciberseguridad es un claro ejemplo de cómo nuestra actual arquitectura global fragmentada no es idónea para enfrentar los retos del siglo XXI. El efecto catalizador de la pandemia del COVID-19 en la economía ha ejercido una enorme presión sobre nuestro entorno digital para que permanezca seguro, resiliente y efectivo. La ciberseguridad es un componente integral y una herramienta clave para esta conectividad sin precedentes, y esta "nueva normalidad" ha reafirmado su valor como un bien público global.

Más allá de la protección operativa de los sistemas y redes, la ciberseguridad es, y seguirá siendo, fundamental para garantizar la integridad y la capacidad de recuperación de los procesos interconectados socioeconómicos, de gobierno y de negocios que operan en el marco de nuestro siempre complejo ecosistema tecnológico. Abordar el riesgo cibernético en todos los ámbitos requiere continuos esfuerzos y adaptación. El presente informe ofrece inestimables observaciones sobre los esfuerzos realizados a nivel nacional dentro de la región de ALC, al capturar y cuantificar el progreso de los países en diferentes dimensiones de seguridad cibernética, en comparación con el análisis de 2016, lo cual permite demostrar la mejora de la postura de seguridad cibernética de la región a lo largo del tiempo. Este trabajo puede constituir una herramienta invaluable para los encargados de la toma de decisiones de los sectores público y privado a la hora de identificar intervenciones prioritarias, mientras avanzan con el fin de mejorar aún más el estado de la ciberseguridad en la región de ALC a través de medidas concertadas y escalables de colaboración nacional, regional e internacional.