DECLARACIÓN DEL PARLAMENTO LATINOAMERICANO Y CARIBEÑO SOBRE LA AGENDA REGIONAL DE CIBERSEGURIDAD PARA AMÉRICA LATINA Y EL CARIBE

El Parlamento Latinoamericano y Caribeño (PARLATINO),

CONSIDERANDO:

Que el Parlamento Latinoamericano y Caribeño reconoce que, en un contexto de acelerada digitalización de las actividades sociales, culturales, económicas y políticas, los países de América Latina y el Caribe enfrentan una creciente exposición a amenazas cibernéticas, ciberdelitos y riesgos que afectan de manera directa la seguridad, los derechos, la economía y el desarrollo de nuestras sociedades. Asimismo, subraya que estos desafíos requieren respuestas coordinadas y estratégicas para garantizar entornos digitales seguros, resilientes e inclusivos

Que la ciberseguridad constituye hoy un componente esencial del desarrollo sostenible y de la prosperidad de nuestros pueblos, debiendo asumirse como una prioridad estratégica de los Estados y como una política pública indispensable para generar confianza, fortalecer la resiliencia institucional y proteger los ecosistemas económicos y sociales de la región.

Que el avance de tecnologías emergentes como la inteligencia artificial y el cómputo cuántico representa una oportunidad para la innovación, la productividad y la transformación digital; sin embargo, también incrementa la complejidad de los riesgos y amenazas en el entorno digital. Por ello, resulta fundamental que los países de la región articulen sus estrategias en materia de inteligencia artificial con sus Estrategias Nacionales de Ciberseguridad, a fin de fortalecer la prevención, la respuesta y la resiliencia frente a los desafíos del presente y del futuro.

Que el PARLATINO considera urgente que los países de América Latina y el Caribe impulsen marcos normativos e institucionales claros, modernos, coherentes y eficaces, que permitan diferenciar y articular adecuadamente los ámbitos de la ciberseguridad, la seguridad pública, la ciberdefensa y los ciberdelitos, con claridad competencial, responsabilidad compartida y pleno respeto al orden democrático y al Estado de Derecho.

Que la región enfrenta desafíos estructurales relevantes, entre ellos la ausencia, en algunos países, de Estrategias Nacionales de Ciberseguridad; la fragmentación regulatoria; la brecha de talento especializado; el aumento y sofisticación de los ciberdelitos; la vulnerabilidad de las infraestructuras críticas; los riesgos asociados a las cadenas de suministro digitalizadas; la limitada articulación regional; y la insuficiencia de recursos financieros para fortalecer capacidades institucionales y técnicas.

Que el PARLATINO hace un llamado a los Estados, parlamentos, organismos internacionales, sector privado, academia y sociedad civil a promover una agenda regional de cooperación y diálogo multisectorial que consolide la ciberseguridad como un eje transversal del desarrollo de América Latina y el Caribe.

Que el PARLATINO destaca la importancia de fortalecer la discusión regional en torno a instrumentos internacionales relevantes, incluida la Convención de Naciones Unidas contra el Cibercrimen, a fin de contribuir a la armonización de esfuerzos y al fortalecimiento de respuestas coordinadas frente a las amenazas digitales.

Que los pueblos de América Latina y el Caribe tienen derecho a desarrollarse en entornos digitales seguros, resilientes, inclusivos y confiables, y que la transformación digital de la región debe construirse con seguridad, cooperación y visión de futuro.

El PARLATINO declara que los pueblos de América Latina y el Caribe deben avanzar hacia un:

1. **Diseño de marcos normativos y legislación de ciberseguridad moderna, asequible y efectiva**, asegurando que los marcos nacionales estén alineados con estándares y buenas prácticas internacionales, a fin de garantizar coherencia, interoperabilidad y confianza en los entornos digitales.
2. **Reconocimiento de la ciberseguridad como una responsabilidad compartida**, que involucra a los Estados, parlamentos, sector privado, academia y sociedad civil, bajo principios de corresponsabilidad y cooperación regional.
3. **Fortalecimiento de las líneas base de ciberseguridad** para prevenir, detectar y combatir el ciberdelito, protegiendo infraestructuras críticas, cadenas de suministro digitalizadas y ecosistemas sociales y económicos.
4. **Promoción de la colaboración regional y multisectorial** para resolver los problemas de ciberseguridad, mediante mecanismos de coordinación, intercambio de información, capacitación y construcción de capacidades técnicas e institucionales.
5. **Impulso de la cooperación multisectorial**, incluyendo proyectos piloto entre los sectores público y privado, que permitan generar innovación, confianza y resiliencia en los sistemas digitales de la región.
6. **Construcción de un modelo equilibrado de seguridad, innovación y desarrollo**, que garantice la neutralidad tecnológica, fomente la competitividad y asegure que la transformación digital se realice en entornos seguros, inclusivos y confiables.

Panamá 24 de marzo 2026