

Ciberseguridad en Ecuador y Latinoamérica

Jaime Sayago-Heredia¹

¹ Pontificia Universidad Católica del Ecuador Sede Esmeraldas

* Autor para correspondencia: jaime.sayago@pucese.edu.ec

DOI: <https://doi.org/10.26871/killkanatecnica.v5i1.957>

Editorial

Palabras clave: *ciberseguridad, ciberespacio, ciberdefensa, vulnerabilidad, internet*

En 2021, la ciberseguridad fue una tendencia marcada en noticias y medios digitales por ataques a instituciones públicas y financieras en Ecuador, esto fue una llamada de atención a que nuestra región es un blanco fácil para la ciberdelincuencia. El informe de la OEA sobre el estado de la ciberseguridad en América Latina entrega una visión general sobre los ataques se llevan a cabo en la región, estos son realizados por delincuentes cibernéticos organizados, financiados y sin fronteras. Estos ataques golpean y llegar a afectar la seguridad del estado llegando a detener y paralizar infraestructura crítica del estado e instituciones ocasionando grandes pérdidas económicas, surgiendo la necesidad de los estados que fomenten políticas y estrategias en un nuevo dominio de ciberseguridad y ciberdefensa como política de seguridad nacional.

En la región de América es posible analizar que Ecuador se encuentra en la posición 19 de un total de 35 a nivel región del ranking de ciberseguridad mundial del indicador Global Cybersecurity Index 2020, este informe es desarrollado por la Unión Internacional de Telecomunicaciones (ITU, agencia de las Naciones Unidas especializada en la coordinación de las telecomunicaciones a nivel global), el cual refleja los avances logrados en materia de ciberseguridad por los 194 estados miembros.

Igualmente, el recientemente informe publicado por la National Cyber Security Index (<https://ncsi.ega.ee/>) elaborado por la prestigiosa e-Governance Academy Foundation de Estonia y que mide el nivel de preparación de los países para prevenir amenazas a la ciberseguridad y la gestión de incidentes cibernéticos. En América Latina lideran el ranking Paraguay, República

Dominicana, Panamá, Colombia y Chile, y se identifican dos áreas que han recibido nula o escasa atención por parte de los estados: la protección de servicios esenciales (incluyendo infraestructura crítica) y las ciberoperaciones militares.

En el caso de Ecuador, una de las medidas sectoriales contenidas en el Plan Nacional de Gobierno Electrónico consistía en generar iniciativas para el fortalecimiento de las TI en el país, a partir del Plan Nacional 2018-2021 que entre sus principales iniciativas esta la gestión del Esquema Gubernamental de seguridad de la información (EGSI) y el Centro de Respuesta ante incidentes informáticos EcuCERT junto con la incorporación de delitos informáticos en el código orgánico integral. A partir del Plan Nacional precisamente se genera una conciencia e importancia de la ciberseguridad y se establece una estrategia y desarrollo de fortalecimiento de la ciberseguridad en los organismos gubernamentales, estos objetivos a ser cumplidos y puestos en conocimiento a escala nacional.

Según el informe Estado de Ciberseguridad en Ecuador, elaborado por la firma Deloitte, que encuestó a cerca de 100 empresas a escala nacional: El 51% de las organizaciones tiene un responsable que cubre la seguridad física y digital. El 13% no cuenta con un experto entre su personal. Pero, además solo el 3% de las empresas aplican herramientas que amortiguan los riesgos cibernéticos de almacenamiento en la nube. De igual forma la Asociación Ecuatoriana de Ciberseguridad (AECI), realizó un estudio en el primer semestre del año 2020, en donde se identificó que en el Ecuador uno de los principales riesgos es la falta de gestión y dedicación exclusiva de ciberseguridad en las empresas o instituciones. Junto con estos porcentajes bajos de protección los tipos de ataques más frecuentes a instituciones son el phishing, ingeniería social y software espía. El Ecuador empezó a sancionar estos delitos informáticos a partir del año 2009 y desde entonces no se ha realizado una actualización a las leyes ocasionando que algunos delitos queden en la impunidad por falta de legislación.

En el Ecuador todavía tiene trabajo por hacer en materia de ciberseguridad y el desafío se concentra en la implementación de instrumentos y política sobre ciberseguridad y ciberespacio que requieren una revisión completa de la legislación en este tema, que como sabemos tiene un componente técnico junto con la interacción del ser humano; por lo tanto, es necesario implementar políticas y reglamentos a nivel país como incorporarnos a iniciativas tanto a nivel regional y mundial.