**Una buena defensa en ciberseguridad para países en desarrollo**

*\*Edgar Vega Briceño*

*edgar.vega.briceno@una.cr*

<p>En los últimos años, los países en vías de desarrollo han experimentado un aumento significativo en su conectividad digital, lo cual es un motor clave para el crecimiento económico, la competitividad y la inclusión social. Sin embargo, este avance también trae consigo nuevos desafíos, especialmente en el ámbito de la ciberseguridad. </p>

<p>Una adecuada gestión de la ciberseguridad es como la defensa en un partido de fútbol. Imaginen a un equipo que, sin una defensa sólida, está expuesto a los ataques feroces del equipo rival. Asimismo, estos países enfrentan constantes amenazas de ciberataques que pueden desestabilizar sus propias economías y sociedades. </p>

<p>En el 2022 Costa Rica experimentó una crisis cibernética notable debido a una serie de ciberataques que afectaron diversas instituciones públicas. Estos incidentes pusieron de manifiesto las vulnerabilidades en la infraestructura digital del país. </p>

<p>En este contexto, la inversión en ciberseguridad es como entrenar a una defensa fuerte y coordinada. Es crucial fortalecer las redes y sistemas digitales con equipos especializados robustos, actualizaciones regulares de software y concienciación sobre la seguridad digital. </p>

<p>De manera similar, los países en desarrollo deben adoptar una estrategia integral de ciberseguridad, actualizar sus leyes, fomentar la investigación y desarrollo en ciberseguridad para protegerse contra las amenazas digitales y aprovechar al máximo las oportunidades que ofrece la tecnología. </p>

<p>Las estadísticas son claras en cuanto al aumento de los ciberataques en estos países. De acuerdo con el reporte<i>*CyberInsights*</i> de Mastercard, de diciembre de 2023, Brasil, México y Costa Rica registraron el mayor número de intentos de ciberataques durante el año pasado en América Latina. En Costa Rica, los sectores públicos (24%), de tecnología (16%), salud (13%) y financiero (12%) fueron los más expuestos a intentos de ciberataques, según el mismo reporte. </p>

<p>En primer lugar, los gobiernos deben establecer marcos regulatorios robustos que promuevan estándares de ciberseguridad adecuados para todos los sectores. Además, es crucial invertir en programas de capacitación y concienciación para educar a los usuarios sobre prácticas seguras en línea y cómo identificar posibles amenazas. </p>

<p>Por otro lado, las industrias deben priorizar la ciberseguridad como una parte integral de sus estrategias empresariales, asignar recursos adecuados para implementar medidas de protección avanzadas y contratar expertos en seguridad informática. La colaboración entre el sector privado, academia y el Gobierno es fundamental para establecer un ecosistema digital seguro y resistente.

<p>Finalmente, desde la cooperación internacional se deben fortalecer las alianzas regionales e internacionales para compartir información sobre amenazas y mejores prácticas, así como para colaborar en la respuesta conjunta a incidentes cibernéticos transfronterizos. </p>

<p>En resumen, proteger el juego digital en países en vías de desarrollo requiere un enfoque integral y colaborativo. Solo mediante la adopción de medidas preventivas y la cooperación efectiva entre gobierno, industria y academia se podrá asegurar un entorno digital seguro que fomente un desarrollo sostenible en la era digital. </p>

*\*Académico del Laboratorio LabCIBE, Sede Regional Chorotega-UNA*