



Ley de Ciberseguridad

Los ataques perpetrados por un grupo cibercriminal durante abril y junio de este año a casi una treintena de instituciones públicas han sido la mayor vejación a la seguridad nacional en décadas, y encontraron un país desarticulado, desarmado y despresupuestado en materia de ciberseguridad. Nuestro equipo de defensa actual es un modestísimo Centro de Respuesta a Incidentes de Seguridad (CSIRT) compuesto de tres informáticos en horario de oficina, como trascendió en medios de prensa.

En ese contexto, varios diputados del Partido Liberación Nacional presentaron el pasado 22 de agosto el Proyecto 23.292, Ley de Ciberseguridad, que procura dotar a Costa Rica del andamiaje regulatorio indispensable para que el país se prepare a futuro con herramientas e infraestructura adecuadas.

El Proyecto es ambicioso en su alcance y refleja las mejores prácticas que a nivel internacional existen en la temática. Propone crear una Agencia Nacional de Ciberseguridad, como dependencia adscrita al MICITT, con rectoría en la materia. Habría sido deseable que esta Agencia gozara de desconcentración administrativa, pero la situación fiscal del país limita la creación de nuevos entes públicos. La Agencia estaría liderada por un director o directora, previo concurso público de atestados, requiriéndose que acredite una formación mínima de ocho años en materia de ciberseguridad. Con la finalidad de que su actuación sea independiente, solo podría removérsele ante causales determinadas previstas en la misma norma.

Bajo la dirección de la Agencia, se estructurarían tres funciones operativas para un abordaje integral de la cuestión: una función preventiva, encomendada a un Centro de Intercambio de Monitoreo de Redes (CIMR), la función reactiva, encomendada al ya existente CSIRT, y una función proactiva, a cargo del Centro de Inteligencia de Datos (CID). Este último, pese a su nombre, no tiene ninguna relación con la DIS, la UPAD, ni similar. Es importante resaltar que aquellas entidades que pertenezcan a un sector regulado, como las financieras o los servicios públicos, responderían, en primer término, a las disposiciones que sobre ciberseguridad dispongan sus reguladores sectoriales, respetando así la especialización de cada sector.

El Proyecto aborda un elemento clave: la determinación de las infraestructuras críticas de la información (ICI), que son los sistemas físicos o automatizados que permiten la prestación de servicios esenciales del Estado, cuya interrupción por un ciberataque generaría importantes consecuencias económicas, de salud o sociales para la población. El Poder Ejecutivo tendría la potestad de establecer cuáles son estas ICI, y la Agencia de identificar cuáles entidades son las que se encuentran operándolas, fijar obligaciones mínimas que deberán cumplir estos operadores, y realizar fiscalizaciones respecto del cumplimiento de estándares mínimos de seguridad de la información. Esta sección del Proyecto resulta esencial para el país, ya que sin un inventario de ICI y, sobre todo, sin facultades de fiscalización respecto de las ICI que se encuentran en manos de operadores privados, resultará imposible proteger integralmente al país frente a futuros ataques. Todos los países que cuentan con regulaciones efectivas en materia de ciberseguridad regulan sus ICI, sean operadas por organismos públicos o privados.

Uno de los principales vacíos del país, y que resulta inexplicable, es que el Estado no cuenta con un elenco de obligaciones mínimas de gestión de la seguridad de la información a cargo de las instituciones del sector público. Esto ha generado que las instituciones estatales adopten decisiones fragmentadas respecto a la ciberseguridad (si es que las adoptan), sin el cumplimiento de un estándar común, lo que incrementa exponencialmente las vulnerabilidades del país. El Proyecto aborda esta situación, estableciendo evaluaciones de riesgo, programas de seguridad de la información, evaluaciones periódicas independientes, inventarios de sistemas de información, entre otras reglas básicas.

El Proyecto es oportuno y técnicamente robusto, y abre una necesaria discusión nacional sobre la materia. Sin embargo, en mi criterio yerra al adscribir la Agencia de Ciberseguridad al MICITT. En todos los países en donde la ciberseguridad es prioridad, estas competencias están atribuidas a las carteras de defensa, seguridad o presidencia. El MICITT, pese a las mejores intenciones y funcionarios que pueda tener, es la cenicienta del Estado, con modestos USD\$10 millones de presupuesto, de los cuales ejecuta la mitad. Además, en poco más de un año, se le han atribuido responsabilidades respecto de la Agencia Nacional de Gobierno Digital, la Promotora de Innovación e Investigación, la Agencia Espacial, y se propone trasladarle también la Agencia de Protección de Datos Personales. Es difícil pensar que, en esta dispersión de tareas, con un presupuesto irrisorio, sin plazas, y en plena crisis fiscal, pueda asumir la ciberseguridad con la profundidad y urgencia que amerita. La ciberseguridad no se agota en la tecnología, y debe abordarse, más bien, como un asunto de seguridad nacional.

Fuente: [LaRepública.net](https://larepublica.net)