Al contestar refiérase
al oficio n.° 04809

22 de abril, 2026
DFOE-CIU-0168

Señor
Edel Reales Novoa
Gerente, Secretaría del Directorio
ASAMBLEA LEGISLATIVA

Estimado señor:

Asunto: Respuesta a solicitud de opinión acerca del texto del proyecto de ley denominado Ley marco para la protección de las infraestructuras críticas y la ciberseguridad, expediente legislativo n.° 24939

Se atiende oficio n.° AL-CPECTE-0906-2026, mediante el cual la señora Nancy Patricia Vílchez Obando, Jefe Área de Comisiones Legislativas V de esa Asamblea Legislativa, solicitó opinión de la Contraloría General sobre el texto del proyecto denominado Ley marco para la protección de las infraestructuras críticas y la ciberseguridad, expediente legislativo n.° 24939.

Al respecto, el Órgano Contralor se referirá a aquellos asuntos relacionados con sus competencias constitucionales, como Órgano Auxiliar de la Asamblea Legislativa en el control superior de la Hacienda Pública.

a) Aspectos Generales del Proyecto

El proyecto de ley busca establecer un marco regulatorio para la gestión del riesgo de ciberseguridad y la resiliencia de las infraestructuras y servicios críticos del país. Su finalidad es asegurar la confidencialidad, integridad, disponibilidad y seguridad operacional tanto de las tecnologías de la información (TI) como de las tecnologías industriales y operacionales (ICS/OT) y sus componentes físicos y digitales, aplicando “un enfoque basado en riesgos con resultados verificables”. La propuesta de ley pretende aplicarse a todas aquellas instituciones públicas y proveedores privados que posean, gestionen y operen infraestructuras o servicios críticos TIC, o que administren datos sensibles de la ciudadanía. Su designación se realizará basándose en criterios como el impacto potencial sobre la población y la economía, efecto cascada, escala y probabilidad de amenaza.

Se establecen responsabilidades obligatorias para prevenir y mitigar riesgos, entre las que destacan el implementar un programa formal con matriz de riesgos y realizar

pruebas periódicas de detección y respuesta, contar con un sistema de gestión de seguridad de la información fundamentado en la norma ISO/IEC 27001 o equivalente, e informar de forma obligatoria al Centro Nacional de Respuesta a Incidentes de Ciberseguridad (CSIRT-CR) sobre los incidentes de ciberseguridad en un plazo máximo de 72 horas. Además, desarrollar y mantener actualizados planes de continuidad operativa y recuperación ante desastres.

Para lograr este cometido, la iniciativa pretende crear la Dirección Nacional de Ciberseguridad (DNC) como el órgano técnico rector en ciberseguridad, dotado de autonomía técnica y competencia horizontal sobre los sujetos obligados de todos los sectores. Esta entidad estará adscrita administrativamente a la Superintendencia de Telecomunicaciones (SUTEL). Para estructurar la DNC, se pretende trasladar a la SUTEL, el CSIRT-CR, responsable de coordinar la atención y mitigación de los incidentes, y el Centro Nacional de Operaciones de Ciberseguridad (SOC-CR), encargado de prevenir incidentes, detectar vulnerabilidades y monitorear alarmas, ambos se ubican actualmente en el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT).

El proyecto busca dotar a la DNC de varias fuentes de recursos para operar, tales como un 0,014% de los recursos del Presupuesto Nacional girados al MICITT en materia de ciberseguridad, asignaciones provenientes de los cánones y tarifas de la SUTEL, fondos de cooperación e ingresos por el cobro de multas. Asimismo, otorga a la SUTEL la potestad de imponer sanciones administrativas en caso de incumplimiento de la ley, aplicando multas económicas a las entidades infractoras que van desde uno hasta quince salarios base, según sea la falta, catalogada como leve, grave o gravísima. Igualmente busca modificar la Ley Nacional de Emergencias y Prevención del Riesgo N.° 8488 para incluir explícitamente el riesgo cibernético; así como la Ley de la Autoridad Reguladora de los Servicios Públicos N.° 7593 y la Ley General de Telecomunicaciones N.° 8642 para facultar a la SUTEL en labores de regulación, vigilancia y control de la ciberseguridad nacional.

b) Opinión del Órgano Contralor

En concordancia con lo establecido en los numerales 183 y 184 de la Constitución Política, en los que se constituye a este órgano contralor como el rector en el control y la vigilancia de la Hacienda Pública, es oportuno indicar que la Contraloría General de la República, realiza su análisis en función de su ámbito de competencia, razón por la cual los asuntos técnicos o de otra naturaleza contenidos en el citado proyecto de ley que se apartan de esa premisa, no serán abordados, considerando que por su especialidad le corresponde a otras instituciones emitir opinión o criterio conforme a las facultades que les asigna el ordenamiento jurídico.

Inicialmente, de previo a referirnos a las disposiciones del proyecto de ley en cuanto a sus implicaciones presupuestarias, de diseño institucional y de control interno, es oportuno indicar que la Contraloría General, a partir de la fiscalización que ha venido

ejecutando sobre seguridad de la información en las entidades del Sector Público, valora como indispensable y positivo el espíritu del proyecto de ley para dotar al Estado de un marco jurídico que permita transitar hacia una gestión ordinaria y preventiva de los riesgos informáticos, evitando así reproducir las vulnerabilidades que han sido evidenciadas. En este sentido, el órgano contralor en diversos informes ha mantenido el criterio sobre la necesidad de fomentar el abordaje del tema a partir de un enfoque sistémico y transversal en la Administración con el fin de que, mediante la prevención y la oportuna administración de los riesgos y eventos, se garantice la seguridad y la continuidad de los servicios públicos en la población.

En diversas fiscalizaciones, la Contraloría General ha documentado que el país opera bajo un modelo de gobernanza de ciberseguridad obsoleto y fragmentado. Mediante el Informe N.° DFOE-SOS-IF-00014-2022, se evidenció que el Centro de Respuesta de Incidentes (CSIRT-CR) funciona con un esquema estático desde 2012, incapaz de ejecutar las etapas indispensables para detectar, responder y recuperar ágilmente los sistemas, al punto de omitir múltiples ataques y tardar hasta 44 días en notificar a las entidades vulneradas. Esta inoperancia técnica se agravó por la inactividad intermitente de la Sala de Análisis de Situación Nacional (SASN) durante la crisis de 2022, lo cual derivó en altos costos de recuperación, la paralización de miles de funcionarios y un grave impacto a la transparencia de la Hacienda Pública (según lo advertido en el informe DFOE-CAP-OS-00001-2023).

Aunado al colapso operativo, existe una profunda incertidumbre financiera para sostener la protección tecnológica una vez que finalice el estado de emergencia, especialmente porque muy pocas instituciones poseen mecanismos de defensa adecuados (Informe N.° DFOE-CAP-SGP-00003-2022). Ante esta deficiente cultura de prevención, la ciberseguridad debe asumirse como una inversión preventiva ineludible. Por ello, tal como se previno mediante la reciente Advertencia N.° ADV-002-2025, resulta indispensable y urgente que las instituciones del Estado asuman su responsabilidad legal actualizando, aprobando e implementando sus Marcos de Gestión de Tecnologías de la Información y planes estratégicos. Solo mediante el estricto cumplimiento de la Ley General de Control Interno se logrará subsanar la alta vulnerabilidad a la que hoy se exponen los recursos y servicios públicos

Ahora bien, a partir de lo anterior se identifica que el Estado costarricense requiere una reforma estructural urgente y profunda en su gobernanza de ciberseguridad, ya que el modelo operativo, centralizado en un CSIRT-CR estático desde 2012, ha demostrado ser obsoleto, fragmentado e ineficiente para detectar, notificar y mitigar amenazas de manera oportuna ante una crisis. La ciberseguridad requiere dejar de gestionarse como una actividad reactiva o temporal vinculada únicamente a decretos de emergencia. Es imperativo consolidarla como una inversión preventiva, permanente e ineludible y que cuente con sostenibilidad financiera en el largo plazo. Esto resulta fundamental para evitar los altos costos económicos de recuperación, garantizar la continuidad operativa de los servicios públicos y proteger la transparencia y rendición de cuentas de la Hacienda Pública ante la ciudadanía.

Es relevante establecer obligaciones claras para que las entidades críticas (ya sea pública o privada que posee, gestiona u opera infraestructura y servicios críticos TIC) reporten de forma ágil y obligatoria los incidentes cibernéticos. Asimismo, es necesario dotar una estructura orgánica de rango legal, con suficiente autonomía técnica y mayores potestades para superar la obsolescencia del actual CSIRT-CR, que además, carece de herramientas normativas formales para ejecutar a cabalidad las etapas indispensables del ciclo de ciberseguridad (detectar, responder y recuperar sistemas), lo que derivó en graves debilidades institucionales y retrasos inaceptables en la notificación de ataques.

Para que este nuevo diseño institucional sea efectivo y solvente, resulta relevante, —considerando el modelo y organigrama institucional del Estado costarricense—, que la rectoría técnica en ciberseguridad recaiga sobre una estructura organizativa con mando técnico transversal, con la suficiente jerarquía para garantizar el acatamiento vinculante por parte de los sectores críticos, agilizar la ejecución presupuestaria ante emergencias y evitar la ineficacia que supone fragmentar la defensa nacional en diferentes unidades técnicas[1].

[1] Guardando las diferencias con el modelo de Estado costarricense, desde la experiencia internacional, el éxito de un modelo centralizado y de alto nivel se evidencia en múltiples referentes analizados por organismos como la OCDE, la OTAN, el BID y la OEA. En Europa, (OECD. (2020). The Digital Transformation of Estonia: A Case Study. OECD Library) Estonia consolidó su Autoridad del Sistema de Información (RIA) como una agencia ejecutiva central con mandato imperativo y transversal sobre toda la red de ministerios, logrando imponer disciplina interinstitucional y un uso eficiente de los recursos. A nivel latinoamericano,(OEA & BID. (2020). Observatorio de la Ciberseguridad en América Latina y el Caribe) Uruguay destaca con la Agencia de Gobierno Electrónico y Sociedad de la Información (AGESIC), un órgano que opera directamente bajo la cúpula de la Presidencia de la República. La debida estructura jerárquica le ha permitido gestionar crisis y emitir normativas estrictas sin enfrentar vacíos de competencia institucional.

Sobre la necesaria vinculación de la propuesta de ley con el ordenamiento jurídico actual

Si bien la inclusión del riesgo cibernético en la Ley Nacional de Emergencias y Prevención del Riesgo (Ley N.° 8488) es un avance necesario, el proyecto de ley omite articularse con el Sistema Nacional de Gestión del Riesgo vigente, esto contraviene directamente el principio de integralidad del proceso de gestión, ya que ignora la estructura normativa y funcional actual —sostenida por la Política y el Plan Nacional—, la cual ya define las competencias, recursos y métodos de todas las instituciones del Estado mediante un modelo consolidado de coordinación multiinstitucional.

En este contexto, el mecanismo de coordinación propuesto entre la nueva Dirección Nacional de Ciberseguridad (DNC) y la Comisión Nacional de Emergencias (CNE) podría generar incongruencias jerárquicas. Otorgar la dirección técnica de una emergencia nacional a la DNC —diseñada como un órgano de tercer nivel subordinado a un regulador económico (SUTEL)— para que coordine de forma imperativa a la CNE, ente adscrito a la Presidencia de la República, podría resultar orgánicamente disfuncional. Este diseño normativo chocaría con los artículos 9 y 10 de la Ley N.° 8488, los cuales ya establecen instancias de coordinación sectorial, operativa y territorial (como los comités asesores y de operaciones) bajo la rectoría de la CNE.

En razón de lo descrito, se sugiere a la Asamblea Legislativa revisar la cadena de mando para que la rectoría técnica posea el peso jerárquico adecuado al más alto nivel, que pueda emitir protocolos vinculantes y apropiados que eviten una respuesta fragmentada ante una crisis nacional y en materia de prevención de riesgos y atención de emergencias. Asimismo, se sugiere que esta reforma materialice el principio rector de prevención establecido en la Ley Nacional de Emergencias, cuyo fin es reducir las causas de las vulnerabilidades y evitar que las amenazas se conviertan en desastres.

Adicionalmente, resulta indispensable armonizar las definiciones que brinda el proyecto de ley con aquellas ya estandarizadas por el Sistema Nacional de Gestión del Riesgo. Conceptos fundamentales como amenaza, infraestructura crítica, mitigación, resiliencia, riesgo, servicios críticos y vulnerabilidad ya cuentan con acepciones legalmente vinculantes en el marco vigente de prevención y atención de emergencias. Por lo que se recomienda cotejar y unificar esta terminología para evitar contradicciones normativas y malas interpretaciones durante la eventual ejecución de la ley, para lo cual se sugiere tomar en consideración las valoraciones de la CNE, en virtud del rol que ostenta de rectora en lo que refiere a la prevención de riesgos y preparativos para atender situaciones de emergencia[2].

[2] Artículo 14 de la Ley N.° 8488.

Sobre la ubicación, conformación y financiamiento de la DNC

El proyecto pretende crear la Dirección Nacional de Ciberseguridad (DNC) como órgano rector con competencia horizontal, absorbiendo al CSIRT-CR y al SOC-CR, así como trasladando la totalidad de sus recursos desde el MICITT para incorporarlos a la SUTEL. En este sentido, se tiene que de la información dispuesta en la exposición de motivos del proyecto de ley, no se observa la existencia de un estudio técnico y jurídico que justifique dicho traslado de competencias a la SUTEL como la instancia idónea para ejecutar competencias atinentes a la ciberseguridad del Estado, máxime tratándose de un órgano con desconcentración máxima de la Autoridad Reguladora de los Servicios Públicos (ARESEP) con una naturaleza jurídica y funcional ajena a dicha materia.

En ese sentido, la iniciativa de Ley no justifica cómo funciones de rectoría (tales como la planificación de la estrategia nacional, la designación de infraestructuras críticas y la atención imperativa de incidentes) guardan afinidad o conexidad con las funciones de regulación del mercado y redes de telecomunicaciones que actualmente ejecuta dicha Superintendencia, como órgano regulador en materia de telecomunicaciones. En consecuencia, resulta oportuno tener en consideración que el esquema organizativo propuesto podría desnaturalizar el control de la seguridad nacional. Delegar la defensa transversal de las infraestructuras críticas de todo el Estado en un regulador de redes y del mercado de telecomunicaciones representa un riesgo operativo y una disfuncionalidad jerárquica que se contrapone con la finalidad que busca el proyecto de ley.

Aunado a lo anterior, la Contraloría General resalta que el diseño institucional propuesto generaría una contradicción jerárquica al pretender que la nueva DNC ejerza una rectoría transversal e imperativa sobre todo el Estado desde un tercer nivel de subordinación —adscrita a la SUTEL, que a su vez pertenece a la ARESEP—. Esta posición subalterna limitaría su autoridad legal y vinculante frente a otras entidades centralizadas y autónomas, desvirtuando los objetivos de la ley.

Asimismo, vale considerar que este diseño vacía de contenido la pretendida autonomía técnica de la DNC al someterla a una dependencia administrativa y financiera absoluta. Dado que el Consejo de la Sutel y la Junta Directiva de la Aresep controlarían el nombramiento de su director, su planificación organizativa y la aprobación de sus presupuestos anuales, creándose un exceso de intermediación institucional que en la práctica, puede influir negativamente en la respuesta inmediata que exige el país ante una crisis o vulnerabilidad cibernética[3].

[3] A modo de ejemplo, aunque la iniciativa de ley dispone que la DNC puede redactar y adoptar resoluciones técnicas generales, los reglamentos técnicos formales y de mayor jerarquía deben ser sometidos a audiencia por la SUTEL y, en última instancia, dictados por la Junta Directiva de la ARESEP o propuestos al Poder Ejecutivo para su aprobación final, esta cadena de autorizaciones confirma los riesgos burocráticos, pues la DNC no tendría la autoridad jurídica final para emitir sus propios reglamentos sin pasar por el tamiz de un regulador económico y su respectiva Junta Directiva.

Por otra parte, el proyecto establece en su Transitorio II, el traslado íntegro de los recursos humanos, financieros y materiales del CSIRT-CR y SOC-CR desde el MICITT hacia la nueva DNC. Sin embargo, al omitir la forma y el plazo para ejecutar este movimiento, se genera incertidumbre sobre la operatividad y el proceso de transición institucional. Además, en cuanto al traslado de fondos del Gobierno Central (un Ministerio) hacia la estructura de un órgano desconcentrado (SUTEL/ARESEP), resulta necesario su sometimiento a lo establecido en la Ley de la Administración Financiera de la República y Presupuestos Públicos (Ley N.° 8131), en cuanto a registro, transparencia y trazabilidad de las transferencias y su impacto en la Hacienda Pública.

Asimismo, en lo que respecta a la movilidad del personal, ha de tenerse en cuenta lo establecido en la Ley Marco de Empleo Público (Ley N.° 10159), en cuanto a la valoraciones y resguardo de derechos adquiridos y situaciones jurídicas consolidadas de las personas servidoras. Por lo anterior, para mitigar el riesgo de incurrir en contingencias y costos por litigios laborales con implicaciones en la Hacienda Pública, es recomendable también tener en cuenta lo establecido en los Transitorios XI y XII de la referida Ley.

En cuanto al financiamiento de la DNC, el proyecto de ley propone extraer permanentemente un 0,014% del presupuesto del MICITT para transferirlo a la SUTEL. Sin embargo, como parte de la exposición de motivos no se observa que se haya realizado un análisis técnico o financiero que justifique la idoneidad de dicho porcentaje. Adicionalmente, establecer rentas con destinos específicos y porcentajes rígidos no es congruente con la flexibilidad y el equilibrio presupuestario, que puede requerirse para adaptar los recursos a la naturaleza dinámica de las amenazas tecnológicas. Mantener esta regla sin revisiones periódicas podría generar una insuficiencia crítica de fondos o por el contrario, crear superávits ineficientes dentro de la SUTEL.

Esta falta de análisis financiero que permita identificar más precisamente las necesidades de recursos económicos para una adecuada operación de la DNC, resulta aún más crítica al contrastar los limitados recursos propuestos con las amplias y nuevas competencias otorgadas a la DNC. Por ejemplo, el proyecto le exige asumir funciones rectoras y operativas masivas, tales como emitir normativa técnica de acatamiento obligatorio para todo el Estado, auditar a todas las entidades críticas TIC sectoriales y operar simultáneamente dos centros de alta tecnología (el CSIRT-CR y el nuevo SOC-CR). Pretender financiar esta expansión competencial con una fracción tan reducida del presupuesto representa un altísimo riesgo de desfinanciamiento, lo cual comprometería la operatividad de la DNC desde su propia creación.

Asimismo, un estudio financiero también permitiría tener más claridad sobre las implicaciones que la reducción presupuestaria tendría en las funciones que el MICITT conserva por ley. El proyecto plantea suprimir del Ministerio parte de sus recursos y, mediante su Transitorio II, trasladar la totalidad de sus plazas, bienes y sistemas ligados a la ciberseguridad hacia la nueva DNC. Dado que el MICITT mantiene su rectoría sobre la Ciencia, la Tecnología y las Telecomunicaciones según la Ley N.° 7169, esta disminución

podría limitar su capacidad operativa para cumplir obligaciones legales irrenunciables, como impulsar el gobierno digital y ejecutar políticas para reducir la brecha tecnológica en la ciudadanía; implicaciones sobre las que no se tiene claridad.

Por otra parte, es relevante acotar que la iniciativa plantea facultar al Consejo de la Sutel a financiar a la DNC utilizando recursos provenientes de los cánones del espectro radioeléctrico y otras tasas de telecomunicaciones, siendo que tal propuesta contraviene directamente el principio de "servicio al costo" establecido en el artículo 3, inciso b), de la Ley de la Autoridad Reguladora de los Servicios Públicos N.° 7593, el cual exige que las tarifas contemplen únicamente los gastos estrictamente necesarios para prestar ese servicio específico. Utilizar el dinero pagado por los regulados del mercado de telecomunicaciones para financiar la defensa cibernética transversal de todo el Estado (hospitales, aduanas, ministerios) constituye un subsidio cruzado irregular que impone cargas económicas improcedentes, violentando el artículo 62 de la Ley General de Telecomunicaciones N.° 8642 y el artículo 82 de la Ley N.° 7593.

Igualmente, la propuesta de financiar a la Dirección Nacional de Ciberseguridad mediante el canon de reserva del espectro radioeléctrico contraviene el artículo 63 de la Ley General de Telecomunicaciones N.° 8642. Dicha norma establece que la recaudación de este canon es exclusiva para la planificación, administración y control del espectro por parte de la SUTEL, prohibiendo categóricamente su uso para objetivos de política fiscal o destinos ajenos a sus competencias exclusivas.

A partir de lo anterior, pretender que un órgano rector nacional —cuyas competencias abarcan infraestructuras críticas ajenas a las telecomunicaciones— se financie con fondos específicos ejecutados bajo el principio de servicio al costo, desnaturaliza por completo el diseño institucional y el rol financiero del regulador. Este mecanismo convertiría un instrumento de regulación de mercado en una carga asimétrica, obligando injustificadamente a los operadores de telecomunicaciones a sostener económicamente funciones soberanas de seguridad nacional que, por su impacto transversal, deben ser financiadas de manera transparente, planificada y sostenible mediante otros medios jurídicamente viables.

Sobre la sostenibilidad financiera y la presupuestación plurianual que sostenga las acciones de protección en la Administración

El proyecto de ley impone nuevos requerimientos a las instituciones públicas catalogadas como entidades críticas TIC, tales como establecer programas formales de gestión de riesgos, mantener inventarios, implementar planes de continuidad operativa y realizar auditorías continuas. La CGR ya ha documentado de forma previa la enorme incertidumbre que existe en el sector público sobre cómo se garantizará la continuidad presupuestaria de las licencias y la protección operativa, por lo que en la opinión y sugestión DFOE-CAP-OS-00001-2023 recomendó que no se eliminen o reduzcan las inversiones en ciberseguridad desde el presupuesto de la República procurando habilitar

recursos financieros de contingencia para dar una respuesta efectiva ante eventuales ciberataques.

Por consiguiente, se recomienda a la Asamblea Legislativa valorar el integrar obligaciones a las instituciones del Estado para planificar estas nuevas cargas preventivas y tecnológicas basándose en el principio constitucional de presupuestación plurianual. Esto podría asegurar que los requerimientos técnicos impuestos por la DNC tengan un contenido económico real y se pueda garantizar a largo plazo en los presupuestos ordinarios de cada institución, evitando que las normas se conviertan en obligaciones legalmente temporales e inaplicables por falta de fondos.

De esta forma queda atendida su gestión,

Atentamente,

Marcela Aragón Sandoval
Gerente de Área

Angie Mora Chacón
Asistente Técnico

Jose Francisco Monge Fonseca
Fiscalizador

CGR | Firmado digitalmente
Valide las firmas digitales

WRM/JMER/LBC/bsc

Ce: Sra. Nancy Patricia Vílchez Obando, Jefe Área Comisiones Legislativas V.
Despacho Contralor, CGR
División de Fiscalización Operativa y Evaluativa, CGR

G: 2026000121-2

NI: 4888-2026