PROYECTO DE LEY

PROYECTO DE LEY PLAN NACIONAL DE INFRAESTRUCTURAS CRÍTICAS DE LA ENERGÍA

El Honorable Senado y la Honorable Cámara de Diputados sancionan con fuerza de ley:

Art. 1° - Objeto. La presente ley tiene por objeto definir un mecanismo de identificación de Infraestructuras Críticas en la República Argentina y un plan común para evaluar y mejorar su protección en el sector de la energía del país, a fin de contribuir a la protección de la población y el medio ambiente.

Art. 2° - **Definiciones.** A los efectos de la presente ley, se consideran los siguientes conceptos:

a) Infraestructuras críticas (IC). Las Infraestructuras Críticas son aquel elemento, sistema o parte de éste que resulta indispensable para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la integridad física, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, afectaría significativamente al Estado y su población.

b) Infraestructuras críticas interprovinciales. La infraestructura crítica situada en una o más provincias cuya perturbación o destrucción afectaría gravemente al menos a dos provincias.

c) Análisis de riesgos. El estudio de hipótesis de amenazas posibles, para evaluar las vulnerabilidades y las posibles repercusiones de la perturbación o destrucción de infraestructuras críticas.

d) Información sensible. Datos específicos sobre una infraestructura crítica que, de revelarse, podrían utilizarse para planear y actuar con el objetivo de provocar una perturbación o la destrucción de instalaciones de infraestructuras críticas.

e) Protección. Todas las acciones destinadas a garantizar la funcionalidad, continuidad e integridad de las infraestructuras críticas con el fin de prevenir, paliar y neutralizar una amenaza, riesgo o vulnerabilidad.

f) Propietarios u operadores. Las entidades responsables del mantenimiento o funcionamiento diario de las infraestructuras críticas.

Art. 3° - Responsabilidad. La responsabilidad de proteger las infraestructuras críticas del país, corresponde a las Provincias, al Estado Nacional y a los propietarios u operadores de tales infraestructuras.

Art. 4° - **Comisión Nacional de Infraestructuras Críticas en Energía.** Créase la Comisión Nacional de Protección de las Infraestructuras Críticas en Energía, que dependerá de la Secretaría de Energía de la Nación y de la Jefatura de Gabinete de Ministros, que estará integrada por lo menos por 5 miembros, profesionales expertos en materia energética y que tendrá como funciones:

a) coordinar el plan nacional de IC con cada una de las provincias;

b) mantenerse a la vanguardia de las mejores prácticas de prevención de riesgos en infraestructuras críticas, a nivel local e internacional;

c) realizar inducción y capacitaciones a los puntos de contacto de IC y a las autoridades competentes de cada provincia;

d) colaborar en la identificación de infraestructuras críticas en el país y a solicitud de alguna provincia; e) realizar reuniones anuales con los puntos de contacto IC de cada una de las provincias a fin de actualizar criterios y elevar los estándares de buenas prácticas aplicadas.

Art. 5° - Identificación. Cada provincia identificará infraestructuras críticas que se ajusten a los criterios establecidos en el art. 6° y a las definiciones del art. 2°, incs. a) y b). El Comité de Infraestructuras Críticas de la Energía podrá, a petición de las provincias, asistirlas en la identificación de potenciales infraestructuras críticas. La identificación de infraestructuras críticas potenciales será un proceso permanente para cada Provincia y para el Comité.

Art. 6° - Criterios. Los criterios a que se refiere el artículo 5° son los siguientes: impacto en la vida humana, de forma tal que existiera riesgo de pérdida de vida o grave amenaza a la salud e integridad física de las personas, considerando el número de víctimas potenciales; el impacto económico, medido en función de la magnitud de las pérdidas económicas o el deterioro de productos o servicios; el impacto ambiental; el impacto público, medido en función de la incidencia de la confianza de la población, el sufrimiento físico y la alteración de la vida cotidiana, incluida la pérdida de servicios esenciales. Además, las provincias podrán disponer criterios sectoriales de acuerdo a las características de los diferentes sectores de las infraestructuras críticas ubicadas en sus territorios.

Art. 7° - **Sectores**. El sector energía objeto de la presente ley, comprenderá los siguientes subsectores, siendo prioritario el sector de las tecnologías de las infraestructuras críticas:

a) Electricidad: infraestructuras e instalaciones de generación, transporte y distribución del suministro eléctrico.

b) Petróleo: producción de petróleo, refinado, tratamiento, almacenamiento y distribución por oleoductos.

c) Gas: producción de gas, refinado, tratamiento, almacenamiento y transporte por gasoductos.

Art. 8° - IC Interprovinciales. La provincia en cuyo territorio se encuentre una IC potencial deberá informar de inmediato a las demás provincias que puedan verse afectados de forma significativa por la IC potencial. La Comisión podrá intervenir en las comunicaciones entre las provincias potencialmente afectadas, pero no tendrá acceso a información pormenorizada que pudiera permitir la identificación inequívoca de una infraestructura concreta. La provincia o municipio que tenga motivos para creer que puede verse afectado de forma significativa por una IC potencial que todavía no haya sido identificada como tal, podrá informar a la Comisión sobre su deseo de iniciar debates bilaterales o multilaterales al respecto. La Comisión comunicará sin demora este deseo la provincia en cuyo territorio se encuentre la IC potencial y se esforzará por facilitar un acuerdo entre las partes.

Art. 9° - Información. La provincia en cuyo territorio se encuentre una infraestructura designada como IC informará anualmente a la Comisión del número de IC designadas por sector y del número de provincias que dependen de cada IC designada. Sólo las provincias que puedan verse afectadas de forma significativa por una IC conocerán su identidad. Las provincias en cuyo territorio se encuentre una IC informarán al propietario u operador de dicha infraestructura de la designación de ésta como IC. La información relativa a la designación de una infraestructura como IC se clasificará en el nivel adecuado. El proceso de identificación y designación de IC con arreglo al artículo 5° y al presente artículo se completará en el período de 6 meses de entrada en vigencia de la ley y se revisará periódicamente.

Art. 10° - Plan de Seguridad. Cada operador de una IC deberá elaborar un plan de seguridad, cuyo procedimiento identificará los elementos infraestructurales críticos de las IC y las soluciones de seguridad que existen o se están aplicando para su protección. Cada provincia valorará si cada IC designada que se encuentre en su territorio dispone de un plan de seguridad o de medidas equivalentes para hacer frente a cualquier riesgo. En caso de que una provincia estime que existe ya un plan de seguridad y que el mismo se actualiza regularmente, no se requerirá ninguna otra intervención. Cada provincia garantizará la aplicación del plan de seguridad o equivalente en el plazo de un año desde la designación de la infraestructura crítica como IC y su revisión periódica. Este plazo podrá prolongarse en circunstancias excepcionales previo acuerdo con la autoridad de la provincia y previa notificación a la Comisión.

Art. 11° - Responsables de enlace para la seguridad. El responsable de enlace para la seguridad ejercerá la función de punto de contacto para cuestiones de seguridad entre el propietario u operador de la IC y la autoridad competente de la provincia. En caso de que una provincia estime que no existe ningún responsable de enlace para la seguridad ni cargo equivalente en relación con una IC designada, garantizará, mediante las medidas que considere oportunas, que se designe un responsable de enlace para la seguridad o cargo equivalente.

Art. 12° - Informes. Cada provincia llevará a cabo una evaluación de amenazas relativa a los subsectores de las IC en el plazo de un año desde la designación de una infraestructura crítica situada en su territorio como IC dentro de dichos subsectores. Cada provincia presentará cada

dos años a la Comisión datos generales resumidos sobre los tipos de riesgos, amenazas y vulnerabilidades encontrados en cada uno de los sectores en los que se hayan designado IC que estén situadas en su territorio. La Comisión, en cooperación con las provincias, podrá elaborar una plantilla común para la presentación de estos informes. Cada informe se clasificará con el nivel que considere necesario la provincia miembro de origen del informe.

Art. 13° - Mejores prácticas. La Comisión apoyará, a través de las autoridades de la provincia interesada, a los propietarios u operadores de IC designadas facilitándoles acceso a las mejores prácticas y métodos, y fomentando la formación y los intercambios de información sobre novedades técnicas relacionadas con la protección de infraestructuras críticas.

Art. 14° - Información sensible. Las provincias, la Comisión y los órganos de vigilancia competentes garantizarán que la información sensible sobre protección de IC comunicada a las provincias o a la Comisión no se utilice para fines distintos de la protección de infraestructuras críticas. El presente artículo se aplicará también a la información no escrita intercambiada en reuniones en las que se debatan cuestiones sensibles.

Art. 15° - **Punto de contacto.** Cada provincia designará un punto de contacto para la protección de infraestructuras críticas. El punto de contacto coordinará las cuestiones relativas a la protección de infraestructuras críticas en la provincia respectiva, con las demás provincias y con la Comisión. La designación de un punto de contacto no impedirá la participación de otras autoridades de la provincia en aspectos relativos a la protección de infraestructuras críticas.

Art. 16° - **Aplicación.** Las provincias adoptarán las medidas necesarias para dar cumplimiento a lo establecido en el período de un mes a partir de la vigencia de la presente norma. Informarán de ello inmediatamente a la Comisión y comunicarán el texto de dichas medidas y su correspondencia con la presente Directiva.

Art. 17° - Sanciones. Las autoridades nacionales y provinciales, los puntos de contacto en cada provincia, los responsables de enlace para la seguridad y los propietarios u operadores, serán responsables penalmente por el incumplimiento de esta ley, además de otras sanciones que pudieren corresponder.

FUNDAMENTOS

Sra. presidenta

El proyecto traído a consideración pretende lograr la protección de las infraestructuras críticas (IC) de la República Argentina en materia energética.

Las infraestructuras críticas se presentan frágiles ante riesgos de ataques, errores humanos y aún desastres naturales que pudieran afectar la seguridad edilicia, informática y las tecnologías de soporte de información de esas estructuras, pudiendo ocasionar grandes inconvenientes en países enteros. Los riesgos ante los potenciales desastres que tales hechos pudieran ocasionar pueden mitigarse con mejores y más estrictas regulaciones en la materia.

Las infraestructuras críticas deben protegerse para evitar perjuicios que no sólo pueden resultar en pérdidas multimillonarias y daños colectivos sino también en daños que afecten a las personas de manera individual. No obstante, como paso necesario simultáneo al objetivo de lograr un avance normativo a nivel nacional, sería necesario avanzar en una mayor difusión del tema en todos los sectores del país, público y privado, resultando esencial la coordinación de esfuerzos a fin de generar la conciencia debida para aunar criterios y lograr una prevención adecuada de posibles desastres.

En este sentido, debe destacarse la función del Estado como organismo fundamental necesario para definir la dirección de las políticas públicas necesarias para proteger las Infraestructuras de Información Críticas (I2C). Si bien los organismos privados tienen el mayor interés en el desarrollo de estos temas, los esfuerzos comunes no podrían lograr el efecto cascada necesario hacia todos los sectores sino a través del Estado.

Esto adquiere mayor relevancia en nuestro país a partir del gran número de empresas del estado y/o con participación estatal mayoritaria que resultan clave para el desarrollo energético del país, como, por ejemplo: YPF S.A., IEASA, AYSA, Nucleoeléctrica Argentina S.A., entre otras. En este sentido, se denomina infraestructura crítica a los elementos, sistemas o parte de sistemas que se encuentran al servicio de un país y son esenciales en el desarrollo y mantenimiento de las actividades socioeconómicas, salud, seguridad, integridad física, y bienestar social de la población, en la cual una perturbación o destrucción de dichas infraestructuras afectaría el normal desarrollo de las actividades a tal punto que podría enviar al colapso a un sistema, una parte de él o a más de un sistema que sean interdependientes. Dicho de otra manera: las Infraestructuras Críticas (IC) serían aquellas instalaciones estratégicas cuyo funcionamiento es esencial para una sociedad determinada y respecto de las cuales cualquier perturbación, interrupción o destrucción podría ocasionar graves consecuencias sobre los servicios afectados y sobre las personas. Las IC se pueden ver afectadas por acciones perjudiciales, intencionales o no, ya sea provenientes del mundo físico o del mundo virtual. Entre

los eventos físicos se puede mencionar a los actos de sabotaje, vandalismo, fenómenos meteorológicos como terremotos o tsunamis, entre otros. Respecto al mundo virtual, existe una infinidad de batallas cibernéticas que han ocasionado y pueden ocasionar desastres en las IC. A partir de esto último, ha tomado relevancia la ciberseguridad en relación a las IC. Las IC se encuentran detrás de los sistemas político-económico de las naciones. Asimismo, las Tecnologías de Infraestructuras Críticas (TIC) - que son las que sostienen a las IC- permiten desarrollar las cualidades y capacidades para el manejo de grandes volúmenes y velocidad de información y transmisión de la misma, así como información relevante, procesamiento de datos, efectividad y eficacia de los procesos. También deben mencionarse las Infraestructuras de Información Críticas (I2C), que son IC sustentadas en Tecnologías de Infraestructuras Críticas.

Las I2C resultan transversales al resto de las IC, dado que en general todas utilizan servicios de información para cumplir sus tareas, el funcionamiento de una represa ejemplifica lo dicho. A partir de estas últimas es que toma relevancia la ciberseguridad como mecanismo de prevención de riesgos asociada a las TI2C.

En ese sentido, el análisis de riesgos es una forma de evitar el colapso de un sistema. El análisis estudia posibles amenazas para evaluar los puntos débiles del sistema, es decir, aquellos que son considerados vulnerables a un ataque. Una vez logrado, se detalla el nivel de repercusión que tiene cada tipo de perturbación y el posible impacto sobre las infraestructuras críticas del sistema. Es por tal motivo que la información sobre protección de infraestructuras críticas es sensible al conocimiento público, dado que, de revelarse, podría ser utilizada con fines destructivos de las instalaciones.

Debe garantizarse la continuidad e integridad de las funciones de toda infraestructura crítica previniendo y neutralizando riesgos de amenaza sobre los sistemas. Las infraestructuras críticas pueden ser propiedad privada, estatales o mixta, a su vez los propietarios son los encargados de mantener y operar las mismas para asegurar la continuidad del servicio y de esta forma el funcionamiento diario del sistema. No obstante, se ha sostenido que es el Estado quien finalmente debe responder ante cualquier ataque a infraestructuras críticas y, en consecuencia, es quien debe coordinar la regulación, las estructuras de poder y todo lo necesario en materia de IC para evitar que ocurran desastres.

Entendemos que una regulación legal adecuada de Infraestructuras Críticas debe propiciar la Protección de Infraestructuras de Información Críticas (PI2C), es decir, debe comprender la protección de los soportes informáticos y digitales que sostienen a esas Infraestructuras, y que en la mayoría de los casos se encuentran vinculados en red con otras Infraestructuras Críticas diferentes.

Esto último resulta de la mayor relevancia, dado que el riesgo que recaiga sobre una de ellas, puede generar riesgo en efecto dominó hacia el resto de las IC. Nótese que la PI2C comprende al conjunto de elementos cuyo fin es garantizar la seguridad de los recursos y procesos

vinculados a la I2C. La PI2C se basa en un conjunto de leyes, personas, recursos físicos, sistemas de comunicación e información, normas y procedimientos, de carácter indispensables para la vida de la nación, a partir de los cuales se logra garantizar la continuidad de las operaciones aún en caso de desastres.

Toda situación que comprometa la seguridad de la I2C posee el potencial de afectar de manera directa a la sociedad, principalmente en los aspectos políticos, sociales y económicos, provocando en algunos casos situaciones de pánico y temor por los daños causados. Debido a su carácter crítico, es de esperar que los recursos vinculados a las I2C no estén aislados entre si de tal modo que pueda garantizarse su continuidad en situaciones de desastre. Para esto deben contemplarse arquitecturas de interconexión y servicios redundantes a escala nacional y multinacional, dependiendo de otras infraestructuras.

En términos prácticos, la PI2C apunta a reducir la probabilidad de materialización de las amenazas, limitar las consecuencias de los ataques y los problemas de funcionamiento, y finalmente permitir la vuelta a la normalidad tras la ocurrencia de un siniestro, a un costo aceptable y en un plazo razonable.

Todo ello debería quedar plasmado en normas adecuadas, preparadas de acuerdo al entorno real del país y los recursos disponibles. Se ha sostenido que la planificación estratégica del abordaje de las IC debería ser direccionado por la Administración Pública Nacional en Argentina a través de la definición de lineamientos generales, que es lo que se pretende lograr con la entrada en vigencia de esta ley. Para la República Argentina, es de suma importancia contar con un mapa estratégico a partir del cual se puedan apreciar las diferentes infraestructuras críticas. Esto resulta fundamental para dar prioridad a los sistemas que mayor impacto generan sobre el sistema nacional.

Consideramos al sistema como un conjunto de sectores, ya sea, energético, productivo, transporte, salud y financiero; cada uno de los cuales es necesario para el normal funcionamiento y desarrollo de la vida cotidiana del país: nuestro mayor interés hoy se centra en el sistema energético.

En nuestro país, resulta esencial proteger el sistema de transporte de energía eléctrica: nuestro país presenta un anillo de interconexión de extra alta tensión que ante un ataque sobre el mismo podría llevar al colapso el sistema eléctrico nacional dejando a oscuras a todo el país. La necesidad de contar con un sistema confiable quedó demostrada en junio del 2019, cuando por una falla de índole natural el sistema eléctrico argentino colapsó dejando a todo el país sin suministro eléctrico.

Afortunadamente, el evento fue ocasionado por una falla natural que pudo ser solucionado a las pocas horas, pero en caso de que el mismo evento hubiese sido originado por un atentado, la respuesta del sistema hubiese sido otra: gran parte del país podría haber estado sin suministro

eléctrico por muchos días, logrando pérdidas económicas, materiales y humanas de una envergadura importante.

Es de destacar que la electricidad ha pasado a ser un servicio esencial para el desarrollo de la vida. Se destaca también la importancia de proteger las infraestructuras críticas en materia de hidrocarburos. Recientemente ocurrió un importante derrame de petróleo a causa de una falla en el sistema de oleoductos de la compañía Oleductos del Valle (Oldelval) entre las Estaciones de Bombeo Crucero Catriel y Medanito en la Provincia de Río Negro, el que se propagó por unos 20.000 metros cuadrados de zona afectada.

El ducto que se rompió transporta el petróleo que se produce en la Cuenca Neuquina hacia Buenos Aires; y provocó el derrame más importante en esa provincia al menos en los últimos 10 años. Otro hubiera sido el resultado si contáramos con un sistema serio de protección de las infraestructuras críticas, habiendo podido hacer seguimiento de los posibles riesgos, previniéndolos a tiempo y evitando, entre otros, el daño ambiental ocasionado. Una situación reciente de identificación de infraestructuras críticas en el país, se dio el 20 de marzo del 2020, cuando el presidente Alberto Fernández declaró la cuarentena de aislamiento social preventivo y obligatorio por la pandemia ocasionada debido a la propagación del virus covid-19. En dicha declaración, se autoriza la libre circulación al personal afectado a actividades esenciales. Estas actividades esenciales fueron: transporte público, personal de salud, personal afectado a servicios públicos como agua, electricidad y gas, personal afectado a telecomunicaciones, personal afectado a servicios funerarios, transporte de cargas y sector alimenticio, entre otros.

Se observa entonces que, sin estos servicios esenciales, las necesidades básicas de la población de nuestro país no se podrían haber satisfecho si no se realizaba un análisis prioritario de los mismos. Se pueden mencionar distintos ejemplos de sectores vinculados a las Infraestructuras Críticas en Argentina, tanto del sector privado como del público, entre ellos: sistemas cibernéticos de la administración pública y sistemas militares; telecomunicaciones; sistemas energéticos; sistemas relacionados a la provisión de agua; sistemas bancario y financiero; transporte; logística alimentaria; sistemas de salud; servicios de emergencia, sistemas de manejo de riesgos en general.

Así, por ejemplo, durante los últimos años, el expediente electrónico ha ido reemplazando paulatinamente a los expedientes en soporte papel en la Administración Pública Nacional y también Provinciales, lo que conlleva la necesidad de resguardar la información contenida en las bases de datos estatales y cuya divulgación -siempre que no se trate de documentación pública- podría generar grandes perjuicios a privados involucrados. El expediente electrónico sería un ejemplo del uso de Tecnologías de Infraestructuras Críticas (TIC) en sistemas de información. Actualmente, y no obstante las regulaciones que ya se encuentran vigente sobre la materia en Argentina y en distintos países del mundo, las Infraestructuras Críticas todavía son ignoradas por gran parte de la población, que desconoce lo esencial de su protección y la necesidad de su funcionamiento armónico, incluso entre distintos países. Las IC tampoco

aparecen lo suficientemente observadas por la ciencia, resultando pocos los estudios comparativos de IC entre distintos sistemas legales. No obstante, a los efectos del proyecto se ha tomado como fuente la Directiva 2008/114/CE del Consejo de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección. En la República Argentina la infraestructura crítica está asociada a la ciberseguridad. En julio de 2017 se creó el comité de ciberseguridad, entre cuyas funciones está la de fijar los lineamientos y criterios para la definición, identificación y protección de las infraestructuras críticas nacionales.

El comité de ciberseguridad está integrado por los ministerios de Defensa y Seguridad y el anterior Ministerio de Modernización, actual Secretaría de Gobierno de Modernización. Luego se incorporaron los ministerios de Justicia y Derechos Humanos y de Relaciones Exteriores y Culto y la Secretaría de Asuntos Estratégicos de la Jefatura de Gabinete de Ministros. En mayo de 2019 se aprobó la Estrategia Nacional de Ciberseguridad -elaborada en 2017- la cual incluye entre sus objetivos la protección de las infraestructuras críticas de información del país. Dicha estrategia define el ciberespacio como aquel que "designa al dominio global y dinámico compuesto por las infraestructuras de tecnología de la información, incluidos internet, las redes y los sistemas de información y de telecomunicaciones; tiene, entre otras, como características esenciales su dimensión global y transfronteriza, su naturaleza dual, su masividad y su vertiginosa y constante evolución".

En resumen, esta estrategia tiene por finalidad prevenir los riesgos a los que se encuentran expuestas las personas y las organizaciones en el ciberespacio. Posteriormente, a través de la resolución 1523/2019 de la Jefatura de Gabinete de Ministros, Secretaría de Gobierno de Modernización, se intentó impulsar la implementación de la Estrategia Nacional de Ciberseguridad aprobando la definición de infraestructuras críticas y de infraestructuras críticas de información, la enumeración de los criterios de identificación y la determinación de los sectores alcanzados.

También aprueba el glosario de términos de ciberseguridad. Continuando con la política de ciberseguridad se aprobaron también otras disposiciones, entre ellas: requisitos mínimos de seguridad de la información para organismos públicos; creación del Comité Asesor para el Desarrollo e Implementación de aplicaciones seguras; creación del Centro Nacional de Respuestas a Incidentes Informáticos (CERT.ar) en el ámbito de la Dirección Nacional de Ciberseguridad; creación del Programa Nacional de Protección de Infraestructuras Críticas de Información y Ciberseguridad; aprobación de la Política Modelo de Seguridad de la Información.

A la normativa específica mencionada, debe agregarse que existe una serie de normas nacionales que también aplican y se relacionan con la materia de ciberseguridad, entre ellas se pueden mencionar las siguientes: Ley 26.388, Delito Informático; Ley 25.326 de Protección de Datos Personales; Decreto Reglamentario N° 1558/2001; Ley 25.506 de Firma Digital y su Decreto Reglamentario N° 2628/2002; Ley 26.904 de Grooming.

Por último, existe un proyecto de ley ingresado a través de la Cámara de Diputados en el Honorable Congreso de la Nación, en fecha 17 de marzo de 2021, por el cual se dispone la creación del Instituto de Ciberseguridad Argentino en el ámbito de la Jefatura de Gabinete de Ministros de la Nación, cuya finalidad sería fortalecer el nivel de seguridad de las redes y sistemas de información dentro del territorio nacional.

Este proyecto aún no ha tenido tratamiento en el Congreso de la Nación. Cabe destacar además, que desde 2019, el BID se encuentra financiando a la Argentina en la implementación de políticas relacionadas con infraestructura crítica, seguridad de los datos personales y buenas prácticas en el uso de las TIC, con acciones puntuales hacia el fortalecimiento de las capacidades nacionales en ciberseguridad. Es así que, en Argentina, si bien existe normativa específica en la materia, nunca se dictó una ley general al respecto ni tampoco se aprobaron normas dirigidas a la Infraestructura Crítica Energética.

Es por todo lo dicho, que creemos necesaria una política integrada en infraestructura crítica para la República Argentina, que comprenda las particularidades y riesgos propios del sector energético, quedando demostrado que hoy resulta un sector crítico para nuestro país. Asimismo, entendemos que entre los elementos que deberían estar contenidos en una normativa específica e integradora de la materia, que comprenda particularmente al sector energético, estarían enumerados los siguientes: lineamientos para definir una planificación estratégica; estructura de colaboración intersectorial; flexibilidad de la normativa, es decir, que permita su rápida adaptación en tiempos de cambio e incertidumbre; estructura de investigación y desarrollo tecnológico aplicados; impulsar una cultura de la seguridad; síntesis de normas comprendidas. Además, podría contener sugerencias de esquemas adecuados de tratamiento de riesgos, vinculación, comunicación, y transferencia, siendo estos últimos elementos que por la sensibilidad de los datos cada organización debería ordenar puertas adentro.

Por todo lo expuesto, solicito a mis pares la aprobación del presente Proyecto de Ley.

Autora:

Jimena Latorre

Coautores:

Lisandro Nieri; Pamela Verasay; Margarita Stolbizer; Maximiliano Ferraro; Ximena García; Julio Cobos; Gustavo Bohuid; Paula Oliveto Lago; Laura Rodríguez Machado; Soledad Carrizo; Ana Clara Romero; Karina Banfi; Gabriela Brower de Koning; Gabriela Lena