



H. Cámara de Diputados de la Nación

PROYECTO DE RESOLUCIÓN

LA HONORABLE CÁMARA DE DIPUTADOS DE LA NACIÓN

RESUELVE

Solicitar al Poder Ejecutivo Nacional que, por intermedio de la Jefatura de Gabinete de Ministros y del Centro Nacional de Ciberseguridad (CNC), en el ámbito de sus respectivas competencias, informe sobre el estado actual de la ciberseguridad en la República Argentina, las medidas adoptadas para prevenir y mitigar ataques informáticos y la capacidad de respuesta y recuperación ante incidentes que puedan comprometer las infraestructuras críticas de información, los activos digitales estratégicos del Estado nacional y los sistemas tecnológicos utilizados en la prestación de servicios públicos esenciales.

El presente requerimiento se circunscribe a las funciones de prevención, protección, coordinación y respuesta institucional en materia de ciberseguridad, sin comprender actividades de inteligencia, contrainteligencia ni información legalmente clasificada cuya fiscalización corresponda a los mecanismos específicos previstos por el ordenamiento jurídico.

A tal efecto, se solicita que informe:

1. EVALUACIÓN DE RIESGOS Y VULNERABILIDADES

a) Si el Centro Nacional de Ciberseguridad ha realizado evaluaciones sobre el nivel de exposición de las infraestructuras críticas de



H. Cámara de Diputados de la Nación

información y los sistemas tecnológicos utilizados en la prestación de servicios públicos esenciales frente a ciberataques de gran escala.

b) Si se han identificado vulnerabilidades, riesgos técnicos o patrones de ataques informáticos que puedan comprometer dichos sistemas, indicando los sectores afectados y las medidas preventivas adoptadas, sin divulgar información que pudiera incrementar su exposición.

c) Si se han evaluado las consecuencias que podrían producir ataques informáticos simultáneos contra distintos servicios esenciales, particularmente en los sectores energético, financiero, sanitario, de transporte y telecomunicaciones.

d) Si el Centro Nacional de Ciberseguridad ha efectuado evaluaciones técnicas de los recientes ciberataques registrados en Japón y de los incidentes informáticos denunciados durante 2026 en países de América Latina, particularmente aquellos que afectaron organismos públicos, infraestructuras estratégicas y servicios esenciales, indicando si se han identificado vulnerabilidades o modalidades de ataque que pudieran reproducirse en la República Argentina y qué medidas preventivas se han adoptado al respecto.

e) Si existen mecanismos permanentes de recepción, análisis y difusión de alertas técnicas sobre amenazas cibernéticas que puedan afectar infraestructuras críticas o servicios esenciales del país.



H. Cámara de Diputados de la Nación

2. PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

- a) Si existe un inventario nacional actualizado de infraestructuras críticas de información y activos digitales estratégicos cuya afectación pudiera comprometer la seguridad, la continuidad de los servicios esenciales o el funcionamiento de organismos del Estado nacional.
- b) Qué criterios técnicos y administrativos se utilizan para identificar y clasificar dichas infraestructuras, indicando los organismos responsables de su protección y los mecanismos de coordinación establecidos.
- c) Qué medidas de prevención y protección se han implementado, dentro de las competencias del Centro Nacional de Ciberseguridad, respecto de los sistemas tecnológicos vinculados con la generación, transporte y distribución de energía eléctrica, las redes de gas, las telecomunicaciones, el transporte, el abastecimiento de agua potable y los establecimientos sanitarios.
- d) Si se han promovido, coordinado o realizado auditorías de seguridad informática, evaluaciones de vulnerabilidades o pruebas de resistencia durante los últimos veinticuatro meses, indicando su alcance, resultados generales y medidas correctivas adoptadas.
- e) Si existen estándares mínimos de ciberseguridad, protocolos de continuidad operativa y procedimientos de recuperación aplicables a los operadores públicos y privados de infraestructuras críticas.



H. Cámara de Diputados de la Nación

f) Si se han identificado deficiencias en la protección de sistemas tecnológicos esenciales y qué medidas se han recomendado para subsanarlas.

3. SISTEMA FINANCIERO Y PROTECCIÓN DE DATOS

a) Qué mecanismos de coordinación institucional existen entre el Centro Nacional de Ciberseguridad, el Banco Central de la República Argentina y las autoridades competentes para prevenir y responder a incidentes informáticos que puedan afectar la continuidad de los servicios financieros.

b) Si se han desarrollado evaluaciones técnicas o ejercicios conjuntos sobre escenarios de interrupción de sistemas de pagos, transferencias bancarias y otras plataformas financieras esenciales, indicando sus resultados generales.

c) Qué acciones de asistencia técnica, prevención o coordinación ha desarrollado el Centro Nacional de Ciberseguridad para fortalecer la protección de los sistemas informáticos utilizados por organismos nacionales que administran datos personales.

d) Si existen protocolos de comunicación, coordinación y respuesta ante incidentes que comprometan grandes volúmenes de información personal almacenada en sistemas del Estado nacional.

e) Si se han establecido mecanismos de cooperación con las autoridades competentes en materia de protección de datos



H. Cámara de Diputados de la Nación

personales para prevenir y mitigar las consecuencias de accesos ilegítimos, filtraciones o secuestros de información.

4. ORGANIZACIÓN Y FUNCIONAMIENTO DEL CENTRO NACIONAL DE CIBERSEGURIDAD

a) Cuál es el estado actual de implementación y funcionamiento del Centro Nacional de Ciberseguridad creado mediante el Decreto 941/2025, indicando su estructura orgánica, autoridades designadas, dotación de personal y dependencias operativas.

b) Qué capacidades técnicas y operativas posee actualmente para prevenir, detectar, analizar y coordinar respuestas frente a incidentes informáticos que comprometan infraestructuras críticas de información o servicios públicos esenciales.

c) Si cuenta con sistemas permanentes de monitoreo, mecanismos de alerta temprana y equipos especializados de respuesta a incidentes, indicando su grado de funcionamiento y cobertura institucional.

d) Qué protocolos de actuación conjunta se han aprobado para coordinar la intervención de organismos nacionales, autoridades provinciales y operadores privados ante incidentes informáticos de alcance nacional.

e) Qué acciones concretas ha desarrollado desde su creación y cuáles son los objetivos operativos previstos para los próximos doce meses.



H. Cámara de Diputados de la Nación

f) Si se han establecido protocolos formales de coordinación e intercambio de alertas entre el Centro Nacional de Ciberseguridad y los organismos competentes del Sistema de Inteligencia Nacional, respetando las funciones específicas de cada organismo y los regímenes legales de protección de la información.

g) Qué procedimientos se encuentran previstos para que el Centro Nacional de Ciberseguridad reciba y utilice alertas técnicas sobre amenazas que puedan comprometer infraestructuras críticas o servicios esenciales, sin requerir la divulgación de información clasificada ni de actividades propias de los organismos de inteligencia.

h) Si se han identificado dificultades de coordinación, superposiciones de competencias o limitaciones operativas que afecten el cumplimiento de sus funciones y qué medidas se han adoptado para resolverlas.

5. INCIDENTES DE CIBERSEGURIDAD REGISTRADOS EN ARGENTINA

a) Cuántos incidentes de ciberseguridad fueron registrados por los organismos nacionales competentes durante los años 2024, 2025 y lo transcurrido de 2026, conforme a los registros disponibles para el Centro Nacional de Ciberseguridad y sus organismos antecesores, discriminados por año, sector afectado, modalidad y gravedad.

b) Cuántos de dichos incidentes afectaron organismos del Estado nacional, infraestructuras críticas de información o sistemas



H. Cámara de Diputados de la Nación

tecnológicos utilizados en la prestación de servicios públicos esenciales.

c) Cuántos incidentes registrados provocaron interrupciones de servicios, accesos ilegítimos, filtraciones de información o secuestro de datos mediante programas de ransomware, indicando su impacto general y duración cuando tales datos se encuentren disponibles.

d) Si los registros técnicos permiten identificar modalidades recurrentes de ataque o vulnerabilidades comunes en determinados sectores, indicando las medidas preventivas recomendadas.

e) Qué procedimientos de notificación, asistencia técnica y coordinación se aplicaron frente a los incidentes de mayor gravedad registrados durante el periodo señalado.

f) Si se realizaron evaluaciones posteriores a dichos incidentes para determinar las deficiencias de seguridad detectadas y verificar la implementación de medidas correctivas.

6. CAPACIDAD NACIONAL DE RESPUESTA Y RECUPERACIÓN

a) Si existe un protocolo nacional de gestión de crisis cibernéticas que contemple ataques informáticos de gran escala capaces de comprometer simultáneamente distintos servicios esenciales.

b) Qué autoridad tiene a su cargo la coordinación técnica e institucional de la respuesta y cuáles son los mecanismos previstos



H. Cámara de Diputados de la Nación

para articular la intervención de organismos nacionales, gobiernos provinciales y operadores privados.

c) Si durante los últimos veinticuatro meses se han realizado ejercicios de simulación de ciberataques contra infraestructuras críticas o servicios esenciales, indicando los organismos participantes, escenarios evaluados, resultados generales y deficiencias detectadas.

d) Si se han establecido tiempos objetivos de recuperación y mecanismos alternativos de funcionamiento ante la interrupción prolongada de sistemas informáticos utilizados en la prestación de servicios esenciales.

e) Si existen equipos especializados de respuesta inmediata con capacidad de intervención permanente y recursos suficientes para asistir técnicamente frente a incidentes simultáneos.

f) Si se han evaluado escenarios en los que un incidente informático afecte a un proveedor tecnológico compartido por varios organismos o servicios esenciales, indicando las medidas previstas para evitar la propagación de sus consecuencias.

g) Si existen procedimientos de comunicación pública para informar oportunamente a la población sobre incidentes que comprometan servicios esenciales y las medidas de contingencia que deban adoptarse.



H. Cámara de Diputados de la Nación

7. COOPERACIÓN TÉCNICA INTERNACIONAL

- a) Qué acuerdos, convenios o mecanismos de cooperación técnica mantiene el Centro Nacional de Ciberseguridad con organismos extranjeros y organizaciones internacionales especializados en prevención, detección, contención y recuperación de incidentes informáticos.
- b) Si, a raíz de los recientes incidentes de ciberseguridad registrados en Japón, se han recibido alertas técnicas, recomendaciones preventivas o comunicaciones de organismos internacionales especializados, indicando las medidas adoptadas a partir de dicha información.
- c) Si la República Argentina participa, por intermedio del Centro Nacional de Ciberseguridad o de los organismos competentes, en redes internacionales de alerta temprana e intercambio de información técnica sobre vulnerabilidades y amenazas informáticas.
- d) Si se han realizado ejercicios conjuntos de preparación y respuesta ante incidentes cibernéticos con organismos de otros países durante los últimos veinticuatro meses, indicando sus resultados generales y las recomendaciones recibidas.
- e) Qué mecanismos de asistencia técnica internacional se encuentran disponibles para fortalecer la capacidad nacional de respuesta y recuperación frente a ciberataques de gran escala.



H. Cámara de Diputados de la Nación

8. RECURSOS PRESUPUESTARIOS, TECNOLÓGICOS Y HUMANOS

- a) Cuál es el presupuesto asignado al Centro Nacional de Ciberseguridad para el ejercicio 2026, indicando los créditos vigentes, su ejecución a la fecha y su distribución por programas, actividades y principales conceptos de gasto.
- b) Qué recursos presupuestarios fueron destinados durante los ejercicios 2024 y 2025 a las funciones de ciberseguridad actualmente comprendidas en las competencias del Centro Nacional de Ciberseguridad, identificando los organismos que las ejercían y los programas presupuestarios correspondientes.
- c) Qué inversiones se han realizado durante 2026 para la adquisición, actualización y mantenimiento de sistemas de monitoreo, detección de vulnerabilidades, alerta temprana y respuesta a incidentes informáticos.
- d) Cuántos agentes integran actualmente la dotación del Centro Nacional de Ciberseguridad, discriminados por funciones técnicas, operativas y administrativas, indicando la cantidad de cargos cubiertos y vacantes.
- e) Qué programas de formación, capacitación y actualización profesional se encuentran vigentes para el personal especializado en ciberseguridad.



H. Cámara de Diputados de la Nación

f) Si se han identificado insuficiencias presupuestarias, tecnológicas o de recursos humanos que limiten el cumplimiento de las funciones asignadas al organismo, indicando las medidas previstas para subsanarlas.

9. MARCO NORMATIVO Y RESPONSABILIDADES INSTITUCIONALES

a) Si el Centro Nacional de Ciberseguridad ha realizado evaluaciones sobre la suficiencia del marco normativo vigente para prevenir, detectar y responder a incidentes informáticos que comprometan infraestructuras críticas de información, activos digitales estratégicos o servicios públicos esenciales.

b) Si existen estándares mínimos de seguridad informática de cumplimiento obligatorio para organismos del Estado nacional y operadores de infraestructuras críticas, indicando las normas que los establecen, su ámbito de aplicación y las autoridades responsables de verificar su cumplimiento.

c) Si los operadores públicos y privados de infraestructuras críticas se encuentran sujetos a obligaciones de notificación de incidentes informáticos, indicando su fundamento normativo, autoridad receptora, plazos y procedimientos establecidos.

d) Si se han identificado vacíos regulatorios, superposiciones de competencias o dificultades de coordinación entre los organismos nacionales responsables de la ciberseguridad.



H. Cámara de Diputados de la Nación

e) Si se encuentran en elaboración propuestas normativas destinadas a fortalecer la protección de infraestructuras críticas de información, establecer estándares de seguridad o mejorar los mecanismos de prevención y respuesta ante incidentes de alcance nacional.

f) Si existen procedimientos institucionales para verificar el cumplimiento de las recomendaciones técnicas formuladas por el Centro Nacional de Ciberseguridad a organismos públicos y operadores de servicios esenciales.

10. PLANIFICACIÓN NACIONAL FRENTE A CIBERATAQUES MASIVOS

a) Si el Poder Ejecutivo Nacional, en el ámbito de las competencias asignadas al Centro Nacional de Ciberseguridad, cuenta con un plan integral y actualizado de prevención, respuesta y recuperación frente a ciberataques masivos que puedan comprometer el funcionamiento de servicios públicos esenciales.

b) Si dicho plan contempla escenarios de ataques simultáneos contra los sistemas tecnológicos vinculados con la energía, las comunicaciones, el transporte, la salud y los servicios financieros, así como mecanismos de coordinación destinados a preservar la continuidad de sus prestaciones.

c) Si se han establecido prioridades de intervención y recuperación para aquellos servicios cuya interrupción pudiera afectar la vida, la salud, la seguridad o el abastecimiento de la población.



H. Cámara de Diputados de la Nación

d) Si existen procedimientos de actuación ante incidentes informáticos que afecten simultáneamente a organismos nacionales y provinciales, indicando los mecanismos de coordinación y asistencia técnica previstos.

e) Si se han realizado evaluaciones sobre la capacidad de recuperación de los servicios esenciales frente a ataques informáticos prolongados, indicando los resultados generales obtenidos y las deficiencias identificadas.

f) Qué medidas adicionales se proyectan adoptar durante los próximos doce meses para reducir la exposición de las infraestructuras críticas nacionales, mejorar los sistemas de alerta temprana y fortalecer la capacidad de respuesta y recuperación frente a incidentes de gran escala.

g) Si se han establecido indicadores objetivos para evaluar el grado de preparación del Estado nacional frente a ciberataques masivos, indicando cuáles son, su periodicidad de medición y los resultados generales disponibles.

REQUERIMIENTO DOCUMENTAL

Solicitar que la información requerida sea acompañada, cuando corresponda, de los antecedentes documentales, estadísticas, informes de gestión, disposiciones administrativas, protocolos generales y demás instrumentos que permitan verificar las acciones



H. Cámara de Diputados de la Nación

desarrolladas y el grado de implementación de las medidas informadas.

Cuando la documentación contenga información técnica cuya divulgación pudiera comprometer la seguridad de los sistemas protegidos, se solicita proporcionar versiones públicas, datos agregados o informes de resultados que permitan ejercer el control parlamentario sin revelar vulnerabilidades explotables, configuraciones sensibles ni información legalmente clasificada.

El presente requerimiento no comprende la identificación de fuentes, métodos, operaciones o actividades reservadas de inteligencia y contrainteligencia, cuya fiscalización se encuentra sujeta al régimen legal específico del Sistema de Inteligencia Nacional.

RAMIRO GUTIÉRREZ

DIPUTADO NACIONAL. -



H. Cámara de Diputados de la Nación

FUNDAMENTOS

Señor Presidente:

El presente proyecto de resolución tiene por objeto solicitar al Poder Ejecutivo Nacional información sobre el estado actual de la ciberseguridad en la República Argentina, las capacidades operativas del Centro Nacional de Ciberseguridad y las medidas adoptadas para prevenir, detectar y responder a ataques informáticos que puedan comprometer infraestructuras críticas, activos digitales estratégicos y servicios públicos esenciales.

La creciente dependencia de sistemas informáticos para el funcionamiento del Estado y de actividades indispensables para la población ha incorporado nuevas vulnerabilidades a la seguridad nacional. Una intrusión informática puede interrumpir servicios de energía, afectar operaciones bancarias, comprometer registros públicos o paralizar sistemas hospitalarios, con consecuencias que exceden ampliamente el ámbito tecnológico.

Los recientes incidentes internacionales y regionales obligan a examinar si nuestro país dispone de mecanismos suficientes para



H. Cámara de Diputados de la Nación

anticipar estas amenazas y reducir sus consecuencias. La experiencia demuestra que las vulnerabilidades informáticas pueden ser aprovechadas por organizaciones criminales que operan desde distintas jurisdicciones, mediante ataques capaces de propagarse entre sistemas interconectados y afectar simultáneamente a numerosos usuarios.

La cuestión adquiere particular relevancia cuando los sistemas comprometidos pertenecen a organismos estatales o empresas responsables de prestaciones esenciales. En estos casos, la capacidad de respuesta no puede depender exclusivamente de las medidas individuales de cada institución, pues una interrupción prolongada puede comprometer derechos de los ciudadanos y el normal desenvolvimiento de actividades económicas y sociales.

La gravedad de esta amenaza ha quedado expuesta recientemente en Japón, donde una sucesión de ciberataques contra empresas, prestadores de servicios y organismos públicos provocó una situación de alarma nacional. Durante las primeras semanas de octubre de 2026, más de veinte grandes compañías informaron incidentes de seguridad informática, con posibles filtraciones de millones de registros personales. Entre los casos más relevantes se encuentra el ataque contra IDC Frontier, empresa proveedora de servicios en la nube vinculada al grupo SoftBank, cuya afectación alcanzó a



H. Cámara de Diputados de la Nación

centenares de organizaciones que dependían de su infraestructura tecnológica.

La magnitud de estos acontecimientos llevó al gobierno japonés a emitir advertencias especiales y recomendar el fortalecimiento de los sistemas de protección. El 9 de octubre, Masaaki Taira, responsable de la estrategia de ciberseguridad del partido gobernante, calificó la situación como un estado de emergencia en el ciberespacio, expresión que reflejó la gravedad de los incidentes, aunque no constituyó una declaración formal de emergencia nacional.

América Latina tampoco permanece ajena a este fenómeno. Un relevamiento publicado por ESET sobre el primer semestre de 2026 identifica una persistente actividad de amenazas informáticas en la región, particularmente mediante campañas de suplantación de identidad, programas maliciosos y ataques de ransomware.

Aunque estos últimos representan una proporción reducida del total de detecciones, sus consecuencias pueden comprometer la continuidad operativa de las organizaciones afectadas.

Los antecedentes regionales permiten comprender el alcance de estos riesgos. En septiembre de 2023, un ataque contra la infraestructura tecnológica de IFX Networks afectó a numerosas entidades públicas de Colombia, entre ellas organismos judiciales y dependencias gubernamentales.



H. Cámara de Diputados de la Nación

El incidente traído demostró cómo la vulneración de un proveedor tecnológico puede extender sus consecuencias a múltiples instituciones que utilizan sus servicios.

Estos episodios adquieren particular importancia para la República Argentina, donde una parte creciente de los servicios estatales, financieros y productivos depende de sistemas digitales interconectados. La posibilidad de que un ataque informático comprometa simultáneamente distintas prestaciones esenciales exige conocer cuáles son las capacidades reales del Estado para detectar incidentes, contener su propagación y restablecer los servicios afectados.

En nuestro país, el Decreto de Necesidad y Urgencia 941/2025 creó el Centro Nacional de Ciberseguridad como organismo descentralizado en la órbita de la Secretaría de Innovación, Ciencia y Tecnología de la Jefatura de Gabinete de Ministros. Su objeto será planificar, ejecutar y supervisar políticas, programas y acciones en materia de ciberseguridad destinadas a proteger el ciberespacio de interés nacional, las infraestructuras críticas de información, los activos digitales estratégicos del Estado Nacional y los sistemas tecnológicos empleados en la prestación de servicios públicos esenciales y actividades del Sector Público Nacional.

El artículo 24 de dicha norma le atribuye, entre otras funciones, la elaboración de políticas de ciberseguridad, la coordinación de la



H. Cámara de Diputados de la Nación

respuesta a incidentes informáticos, la realización de pruebas periódicas sobre vulnerabilidades y la elaboración de un Plan de Recuperación ante Desastres para el Sector Público Nacional.

Las atribuciones normatizadas atribuciones también permiten identificar responsabilidades institucionales concretas sobre las cuales corresponde ejercer el control parlamentario.

La creación de este organismo constituye un antecedente institucional que debe ser acompañado por una evaluación de su funcionamiento efectivo. Resulta necesario conocer si cuenta con recursos humanos especializados, presupuesto suficiente, sistemas de alerta temprana y protocolos de actuación que permitan coordinar respuestas entre organismos nacionales, autoridades provinciales y operadores privados responsables de servicios esenciales.

También corresponde determinar si se han realizado simulaciones de ataques informáticos de gran escala, cuáles fueron sus resultados y qué medidas correctivas se adoptaron frente a las deficiencias detectadas. La existencia de protocolos administrativos, por sí sola, no permite establecer si un sistema se encuentra preparado para responder ante una interrupción simultánea de servicios.

El presente requerimiento respeta la diferenciación normativa entre las actividades de ciberseguridad y las funciones propias del Sistema de Inteligencia Nacional. Por esa razón, las preguntas se circunscriben



H. Cámara de Diputados de la Nación

a las competencias civiles, técnicas y preventivas del Centro Nacional de Ciberseguridad, sin requerir información sobre operaciones de inteligencia, fuentes, métodos o actividades legalmente clasificadas.

La Cámara de Diputados de la Nación tiene la responsabilidad institucional de conocer el grado de preparación del Estado frente a amenazas que pueden afectar directamente la vida cotidiana de los argentinos. El control parlamentario sobre la ejecución de las políticas públicas de ciberseguridad permite evaluar las capacidades disponibles, identificar eventuales insuficiencias y considerar las medidas legislativas que pudieran resultar necesarias.

La experiencia internacional advierte que las consecuencias de un ciberataque pueden extenderse mucho más allá de la organización inicialmente afectada. Cuando se comprometen los sistemas que sostienen servicios esenciales, la capacidad de respuesta del Estado adquiere una dimensión de interés público que justifica plenamente este requerimiento.

La pregunta que corresponde formular es si la Argentina cuenta hoy con los recursos, la organización y los procedimientos necesarios para enfrentar un ciberataque masivo sin comprometer la continuidad de sus servicios esenciales.

Por las razones expuestas, solicito a mis pares que acompañen la aprobación del presente proyecto de resolución.