PROYECTO DE RESOLUCIÓN

La Honorable Cámara de Diputados de la Nación

RESUELVE

Dirigirse al Poder Ejecutivo Nacional, en ejercicio de las facultades conferidas por los artículos 75 inciso 32 de la Constitución Nacional y 204 del Reglamento de la Honorable Cámara de Diputados de la Nación, para que, por intermedio de la Jefatura de Gabinete de Ministros, la Secretaría de Innovación, Ciencia y Tecnología, el Centro Nacional de Ciberseguridad, la Secretaría de Inteligencia de Estado, el Ministerio de Seguridad Nacional, la Agencia de Acceso a la Información Pública y demás organismos competentes, informe de manera precisa, documentada y circunstanciada sobre los siguientes puntos vinculados con la creación, puesta en funcionamiento, capacidades operativas, transferencia de recursos y actuación del Centro Nacional de Ciberseguridad frente a incidentes recientes:

1. Informe si se encuentran formalmente celebrados los acuerdos previstos en el artículo 31 del DNU 941/2025 para la transferencia de bienes, activos, patrimonio, compromisos, derechos y obligaciones desde la Secretaría de Inteligencia de Estado (SIDE) y la ex Agencia Federal de Ciberseguridad (AFC) hacia el Centro Nacional de Ciberseguridad (CNC), indicando fecha de suscripción, autoridades intervinientes y criterios utilizados para determinar qué activos fueron considerados "destinados exclusivamente a funciones relacionadas a la ciberseguridad".

2. Remita copia íntegra de los acuerdos, actas, convenios, inventarios o instrumentos suscriptos entre la Secretaría de Inteligencia de Estado y el Centro Nacional de Ciberseguridad para la transferencia de bienes, activos, patrimonio, compromisos, derechos y obligaciones vinculados a la ex Agencia Federal de Ciberseguridad. En caso de encontrarse en elaboración, indique estado de avance, autoridades intervinientes y fecha estimada de suscripción.

3. Indique el criterio formal utilizado para determinar qué bienes, activos, licencias, plataformas, bases de datos, contratos, servicios, archivos técnicos, repositorios documentales o capacidades operativas fueron considerados "exclusivamente relacionados con ciberseguridad" y transferidos al CNC, y cuáles permanecieron bajo órbita de la Secretaría de Inteligencia de Estado o de la Agencia Federal de Ciberinteligencia. Informe si dicho criterio fue plasmado en actos administrativos, dictámenes o instrumentos internos y acompañe copia.

4. Informe si existen dictámenes jurídicos emitidos por la Procuración del Tesoro de la Nación, la Sindicatura General de la Nación (SIGEN), la Agencia de Acceso a la Información Pública (AAIP) o áreas legales de la Jefatura de Gabinete de Ministros

respecto de la legalidad, alcances y mecanismos de implementación de la transferencia funcional, patrimonial y operativa dispuesta por el DNU 941/2025.

5. Informe si el Centro Nacional de Ciberseguridad cuenta actualmente con:

   a) reglamento interno de funcionamiento;

   b) estructura orgánico-funcional definitiva;

   c) protocolos operativos de gestión de incidentes;

   d) manuales internos de actuación;

   e) mecanismos de auditoría interna;

   f) régimen de conflictos de interés;

   g) código de conducta específico para personal técnico;

   h) protocolos de trazabilidad y custodia de información sensible.

   En cada caso, remita copia o indique estado actual de elaboración e implementación.

6. Informe si el CNC funciona actualmente en inmuebles propios, alquilados, cedidos o compartidos con organismos integrantes del Sistema de Inteligencia Nacional, detallando situación jurídica, autoridad administradora, modalidad de ocupación y nivel de acceso compartido existente con otros organismos.

7. Informe si existen mecanismos formales de coordinación operativa, interoperabilidad, intercambio de información o utilización compartida de infraestructura entre el CNC y la actual Agencia Federal de Ciberinteligencia (AFC), detallando protocolos vigentes, niveles de acceso, autoridades intervinientes y mecanismos de control existentes.

8. Informe si el CNC participa actualmente de la Comunidad Informativa Nacional (CIFN) creada por la Ley 25.520, indicando:

   a) modalidad de participación;

   b) frecuencia de reuniones;

   c) organismos intervinientes;

   d) productos compartidos;

   e) agentes acreditados;

   f) protocolos de circulación de información aplicables.

9. Informe la cantidad total de agentes actualmente afectados al Centro Nacional de Ciberseguridad, discriminando:

   a) personal permanente;

   b) personal no permanente;

   c) contrataciones bajo artículo 9° Ley 25.164;

   d) locaciones de servicios;

   e) personal de gabinete;

   f) personal transferido desde la SIDE y/o la ex Agencia Federal de Ciberseguridad;

   g) personal en comisión de servicios proveniente de otros organismos;

   h) personal que mantenga habilitaciones especiales vinculadas al Sistema de Inteligencia Nacional.

10. Informe la estructura orgánico-funcional actualmente vigente del CNC, indicando direcciones, coordinaciones, áreas técnicas, cantidad de cargos, situación de cobertura, vacantes existentes y autoridades responsables.

11. Detalle el personal jerárquico designado, indicando:

    a) nombre completo;

    b) cargo;

    c) fecha de designación;

    d) acto administrativo correspondiente;

    e) antecedentes laborales inmediatos;

    f) pertenencia previa a organismos de inteligencia, seguridad, defensa o ciberseguridad estatal.

12. Informe si los agentes transferidos desde la SIDE y/o la ex Agencia Federal de Ciberseguridad mantienen actualmente:

    a) acceso a sistemas;

    b) credenciales activas;

    c) acceso a plataformas;

    d) acceso a repositorios documentales;

e) acceso a infraestructura tecnológica;

f) acceso a instalaciones;

g) doble dependencia funcional;

h) comisiones de servicio;

i) cualquier otro vínculo operativo con organismos integrantes del Sistema de Inteligencia Nacional.

13. Informe el régimen jurídico aplicable al personal transferido desde la SIDE y/o la ex Agencia Federal de Ciberseguridad, indicando si continúan bajo esquemas vinculados a la Ley 25.520 o si fueron incorporados plenamente al régimen general del empleo público nacional.

14. Informe el régimen de habilitaciones de seguridad aplicado al personal del CNC, indicando:

    a) criterios de otorgamiento;

    b) autoridad competente;

    c) procedimientos de evaluación;

    d) niveles de habilitación existentes;

    e) mecanismos de revisión y auditoría;

    f) compatibilidad con habilitaciones previamente otorgadas por la SIDE.

15. Informe si se encuentra implementada la Asignación por Responsabilidad en Tareas de Ciberseguridad prevista en el artículo 28 del DNU 941/2025, indicando:

    a) cantidad de agentes alcanzados;

    b) montos actualmente vigentes;

    c) criterios de otorgamiento;

    d) procedimiento de evaluación;

    e) acto administrativo correspondiente.

16. Remita el inventario de hardware transferido desde la ex Agencia Federal de Ciberseguridad y/o la SIDE hacia el CNC, indicando:

    a) tipo de equipamiento;

b) marca y modelo;

c) número de serie o identificador patrimonial;

d) fecha de incorporación;

e) valor de inventario;

f) ubicación física actual.

17. Informe específicamente si fueron transferidos:

a) servidores y equipamiento de centros de cómputos;

b) equipamiento de red;

c) appliances de seguridad;

d) plataformas SIEM;

e) infraestructura SOC;

f) hardware criptográfico;

g) laboratorios forenses;

h) sistemas de monitoreo y telemetría;

i) equipamiento de análisis de malware;

j) plataformas de respuesta a incidentes.

18. Remita el inventario de software, licencias, suscripciones, plataformas y servicios tecnológicos transferidos desde la ex AFC y/o la SIDE al CNC, indicando:

a) producto;

b) fabricante;

c) modalidad de licenciamiento;

d) vigencia;

e) soporte vigente o vencido;

f) organismo usuario;

g) finalidad operativa.

19. Informe si el CNC posee actualmente acceso directo, indirecto o interoperabilidad con bases de datos que contengan datos personales, biométricos, registrales,

financieros, migratorios, tributarios, previsionales o sanitarios pertenecientes a organismos del Sector Público Nacional, indicando:

a) organismo titular;

b) fundamento jurídico aplicable;

c) finalidad del acceso;

d) mecanismo de autorización;

e) controles existentes;

f) trazabilidad de accesos implementada.

20. Detalle las bases de datos, registros técnicos, archivos operativos, repositorios documentales o plataformas de información transferidas desde la ex AFC al CNC, especificando:

    a) naturaleza del activo;

    b) volumen aproximado;

    c) sistema de custodia;

    d) mecanismos de trazabilidad;

    e) procedimientos de desclasificación, depuración o segregación implementados antes de la transferencia.

21. Informe si el CNC utiliza infraestructura cloud propia, estatal, híbrida o provista por terceros privados nacionales o extranjeros para almacenamiento, procesamiento, correlación o resguardo de información vinculada a incidentes de seguridad informática, infraestructuras críticas o bases de datos estatales, indicando:

    a) proveedores involucrados;

    b) jurisdicción aplicable;

    c) mecanismos de cifrado implementados;

    d) criterios utilizados para garantizar soberanía, integridad y trazabilidad de la información.

22. Informe si empresas privadas proveedoras de servicios tecnológicos, ciberseguridad, almacenamiento, monitoreo, análisis de amenazas, procesamiento de datos o infraestructura digital poseen actualmente acceso, administración, procesamiento,

alojamiento o resguardo de información crítica vinculada a organismos del Sector Público Nacional, detallando:

a) empresa involucrada;

b) tipo de servicio prestado;

c) modalidad contractual;

d) nivel de acceso otorgado;

e) mecanismos de auditoría implementados;

f) jurisdicción aplicable en materia de tratamiento y resguardo de datos.

Informe si el CNC contrató servicios tercerizados indicando proveedor, modalidad de contratación, procedimiento utilizado, nivel de acceso otorgado y mecanismos de supervisión implementados de:

a) monitoreo;

b) análisis forense;

c) respuesta a incidentes;

d) threat intelligence;

e) pentesting;

f) análisis de malware;

g) almacenamiento de logs;

h) administración remota;

i) gestión de infraestructura crítica;

24. Informe el estado actual de implementación de:

a) la Estrategia Nacional de Ciberseguridad;

b) el Plan de Recuperación ante Desastres (PRD);

c) el inventario oficial de Infraestructuras Críticas de Información;

d) el registro nacional de equipos de respuesta ante incidentes;

e) los protocolos nacionales de respuesta a incidentes.

25. Informe el estado de implementación operativa del CERT.ar bajo dirección del CNC, indicando:

    a) dotación actual;

    b) cobertura horaria;

    c) infraestructura tecnológica;

    d) cantidad de incidentes reportados;

    e) cantidad de incidentes gestionados;

    f) métricas de respuesta;

    g) tiempos promedio de mitigación.

26. Informe si el CNC cuenta actualmente con capacidad operativa permanente de:

    a) monitoreo en tiempo real;

    b) SOC (Security Operations Center);

    c) laboratorios forenses propios;

    d) infraestructura de análisis de malware;

    e) plataformas SIEM;

    f) plataformas XDR;

    g) herramientas EDR;

    h) herramientas de threat intelligence;

    i) plataformas de simulación de adversarios.

27. Informe la cantidad actual afectaos al CNC de:

    a) analistas de incidentes;

    b) analistas forenses;

    c) especialistas en malware;

    d) especialistas en threat intelligence;

    e) ingenieros de seguridad ofensiva;

    f) criptógrafos;

g) operadores SOC;

h) especialistas en respuesta a incidentes;

28. Informe si el CNC realizó evaluaciones técnicas, pruebas de penetración o ejercicios de red team sobre organismos del Sector Público Nacional desde su creación, indicando:

    a) cantidad de evaluaciones;

    b) organismos alcanzados;

    c) criterios de priorización;

    d) porcentaje de recomendaciones implementadas.

29. Informe específicamente si se realizaron ejercicios de simulación, pruebas de penetración o ejercicios de red team sobre:

    a) RENAPER;

    b) Banco Central;

    c) Ministerio de Salud;

    d) ANSeS;

    e) Jefatura de Gabinete;

    f) organismos vinculados a infraestructura crítica.

30. Informe si existen organismos nacionales que aún no hayan implementado los lineamientos técnicos previstos en la Disposición CNC 1/2026, detallando:

    a) grado de incumplimiento;

    b) riesgos detectados;

    c) medidas correctivas implementadas;

    d) cronograma de adecuación previsto.

31. Informe si el CNC celebró acuerdos de cooperación, asistencia técnica o intercambio de información, indicando contraparte, objeto, fecha de suscripción y vigencia con:

    a) organismos extranjeros;

    b) agencias internacionales;

    c) CSIRTs internacionales;

d) plataformas tecnológicas;

e) proveedores privados;

f) empresas de ciberseguridad;

32. Informe si el CNC mantiene participación en redes internacionales de intercambio de amenazas, FIRST, MISP, CSIRTs o plataformas de intercambio de indicadores de compromiso, indicando alcance y modalidades de participación.

33. Respecto de los incidentes públicamente atribuidos al colectivo "Chronus Team" ocurridos entre marzo y abril de 2026, informe:

a) fecha y vía de toma de conocimiento;

b) organismos afectados;

c) acciones de coordinación realizadas;

d) alertas tempranas emitidas;

e) equipos movilizados;

f) informes técnicos producidos;

g) indicadores de compromiso compartidos;

h) volumen estimado de datos comprometidos;

i) estado actual de mitigación.

34. Informe las articulaciones institucionales efectuadas por el CNC, en relación con los incidentes atribuidos a "Chronus Team", con:

a) la Agencia de Acceso a la Información Pública;

b) la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI);

c) el Ministerio Público Fiscal;

d) organismos afectados;

e) autoridades judiciales;

f) fuerzas de seguridad;

35. Informe si las notificaciones previstas en la Ley 25.326 y normativa concordante fueron cursadas en tiempo y forma respecto de incidentes que involucraron datos

personales, indicando organismos intervinientes y medidas adoptadas ante eventuales incumplimientos.

36. Respecto de las filtraciones vinculadas al RENAPER y a la circulación ilegal de datos personales y biométricos desde 2021, informe qué acciones desplegó el CNC desde su creación para:

    a) auditar el estado actual de seguridad del organismo;

    b) verificar implementación de lineamientos técnicos;

    c) emitir recomendaciones;

    d) coordinar acciones con el Ministerio del Interior y la AAIP;

    e) evaluar riesgos asociados a la circulación ilegal de datos biométricos.

37. Respecto de incidentes que hayan afectado al Ministerio de Salud, obras sociales nacionales u organismos vinculados a sistemas sanitarios durante el período enero–mayo de 2026, detalle:

    a) organismos afectados;

    b) naturaleza del incidente;

    c) tipo de información comprometida;

    d) acciones desplegadas por el CNC;

    e) estado actual de mitigación.

38. Informe cuántos incidentes de seguridad informática que involucraron organismos públicos nacionales se registraron durante el período enero–mayo de 2026, discriminando:

    a) salud pública;

    b) registros estatales;

    c) infraestructura crítica;

    d) seguridad;

    e) defensa;

    f) organismos financieros.

39. Informe si el CNC elaboró matrices de riesgo o evaluaciones de impacto respecto de la exposición masiva de datos personales pertenecientes al RENAPER, Ministerio de Salud, Banco Central u otros organismos afectados por incidentes recientes.

40. Informe si el CNC emitió reportes públicos, alertas ciudadanas o recomendaciones preventivas dirigidas a la población ante la circulación ilegal de datos personales, credenciales filtradas o incidentes de seguridad relevantes.

41. Indique si el CNC posee actualmente facultades, herramientas técnicas o capacidades operativas para:

    a) monitoreo de tráfico;

    b) análisis masivo de datos;

    c) correlación automatizada de información;

    d) monitoreo de redes vinculadas a infraestructuras críticas;

    e) procesamiento automatizado de grandes volúmenes de información sensible.

    Para cada caso, informe:

    i) marco jurídico aplicable;
    ii) mecanismos de autorización;
    iii) organismos intervinientes;
    iv) controles existentes;
    v) si dichas capacidades alcanzan información perteneciente a ciudadanos, usuarios, proveedores o terceros vinculados a organismos públicos nacionales;
    vi) si existe intervención, supervisión o dictamen previo de la Agencia de Acceso a la Información Pública.

42. Informe qué mecanismos de control parlamentario, auditoría externa y rendición de cuentas fueron previstos para supervisar el funcionamiento del CNC y la utilización de capacidades técnicas provenientes del Sistema de Inteligencia Nacional.

43. Informe si se realizaron auditorías internas o externas sobre el proceso de transferencia patrimonial, tecnológica y de personal previsto en los artículos 31 y 33 del DNU 941/2025, indicando:

    a) organismos intervinientes;

    b) alcance;

    c) resultados;

d) observaciones formuladas;

e) medidas correctivas implementadas.

44. Informe las comunicaciones cursadas por el CNC a la Comisión Bicameral Permanente de Fiscalización de los Organismos y Actividades de Inteligencia del Honorable Congreso de la Nación desde su creación, indicando fecha, objeto y documentación remitida.

45. Informe el estado de articulación existente entre el CNC y el Ministerio de Seguridad Nacional, en particular con la Dirección de Investigación de Cibercriminalidad y con el "Plan Federal de Lucha contra el Fraude Ciberasistido 2026–2027", detallando distribución de competencias, mecanismos de coordinación y autoridades intervinientes.

46. Toda otra información que el Poder Ejecutivo considere pertinente para esclarecer el estado de organización, operatividad, capacidades técnicas, mecanismos de control institucional y actuación concreta del Centro Nacional de Ciberseguridad creado por el DNU 941/2025.

Pablo JULIANO

FUNDAMENTOS

Señor Presidente:

El presente proyecto de resolución tiene por objeto requerir al Poder Ejecutivo Nacional información precisa, documentada, integral y circunstanciada acerca del proceso de creación, organización, transferencia patrimonial, integración funcional, capacidades operativas, mecanismos de control institucional y actuación concreta del Centro Nacional de Ciberseguridad (CNC), organismo creado mediante el Decreto de Necesidad y Urgencia N° 941/2025 en el marco de una profunda reorganización de las estructuras estatales vinculadas a la ciberseguridad, la administración de infraestructuras críticas y las capacidades técnicas previamente concentradas en organismos integrados al Sistema de Inteligencia Nacional.

La información solicitada resulta indispensable para que esta Honorable Cámara pueda ejercer adecuadamente las facultades de control político e institucional que la Constitución Nacional le confiere respecto de organismos que administran infraestructura tecnológica estratégica, herramientas de monitoreo y respuesta ante incidentes, plataformas críticas, sistemas de análisis técnico y potencial acceso a grandes volúmenes de información perteneciente al Estado Nacional y, eventualmente, a millones de ciudadanos cuyos datos personales son tratados por organismos públicos.

El presente pedido de informes no se limita a indagar sobre aspectos meramente administrativos o presupuestarios. Lo que aquí se encuentra en discusión es la configuración concreta de un nuevo esquema institucional de ciberseguridad estatal surgido a partir de la transferencia de recursos, personal especializado, infraestructura tecnológica, herramientas de monitoreo, capacidades operativas y conocimiento técnico acumulado provenientes de estructuras históricamente vinculadas al Sistema de Inteligencia Nacional hacia un organismo formalmente ubicado bajo órbita civil.

Precisamente por ello, el Congreso de la Nación no puede limitarse a conocer la existencia formal del organismo ni la mera descripción normativa de sus competencias. Resulta imprescindible determinar cuáles fueron las capacidades efectivamente transferidas, cuáles permanecieron bajo control de la Secretaría de Inteligencia de Estado, qué mecanismos de coordinación continúan existiendo entre ambas estructuras y cuáles son los límites jurídicos, institucionales y operativos actualmente vigentes respecto de las facultades, herramientas técnicas y capacidades concretas del Centro Nacional de Ciberseguridad.

La necesidad de dicho control parlamentario adquiere especial relevancia a la luz de los múltiples incidentes de seguridad informática y filtraciones masivas de información pública conocidos durante el período enero–mayo de 2026, algunos de ellos

atribuidos públicamente al colectivo denominado "Chronus Team", que habrían afectado organismos nacionales, provinciales y entidades públicas vinculadas a salud, seguridad, infraestructura crítica, administración estatal y registros públicos sensibles.

La magnitud de tales episodios, sumada a la escasa información oficial disponible respecto de las capacidades reales de respuesta, coordinación, monitoreo, detección y mitigación desplegadas por el nuevo organismo, torna imprescindible esclarecer con qué recursos humanos, tecnológicos y presupuestarios cuenta actualmente el CNC, cuáles son las herramientas efectivamente utilizadas para la protección del ciberespacio de interés nacional y qué mecanismos de articulación mantiene con otras estructuras estatales, organismos de inteligencia, agencias regulatorias y proveedores tecnológicos.

El Centro Nacional de Ciberseguridad fue creado mediante el artículo 23 del Decreto de Necesidad y Urgencia N° 941/2025 como organismo descentralizado en la órbita de la Secretaría de Innovación, Ciencia y Tecnología de la Jefatura de Gabinete de Ministros, atribuyéndosele expresamente el carácter de "autoridad nacional en materia de ciberseguridad" y "Autoridad de Aplicación de la normativa vigente y aplicable en la materia".

Conforme surge del propio decreto, el CNC posee amplísimas facultades vinculadas a la planificación, coordinación, supervisión y ejecución de políticas destinadas a proteger el ciberespacio de interés nacional, las infraestructuras críticas de información, los activos digitales estratégicos del Estado Nacional y los sistemas tecnológicos utilizados para la prestación de servicios públicos esenciales.

El artículo 24 del DNU 941/2025 le asigna funciones de enorme relevancia institucional: actuar como órgano rector en materia de protección del ciberespacio; elaborar e implementar políticas nacionales de ciberseguridad; coordinar respuestas ante incidentes; dirigir el CERT.ar; desarrollar capacidades de monitoreo y detección; promover estándares técnicos; coordinar equipos de respuesta; implementar estrategias nacionales; supervisar buenas prácticas y realizar evaluaciones de vulnerabilidades sobre infraestructuras críticas del Sector Público Nacional.

La amplitud de dichas competencias coloca al CNC en una posición institucional particularmente sensible. No se trata simplemente de un organismo administrativo adicional dentro del organigrama estatal, sino de una estructura con potencial acceso a infraestructura tecnológica estratégica, sistemas críticos, plataformas de monitoreo, análisis de amenazas, información sensible y circuitos operativos vinculados a la protección digital del Estado Nacional.

La arquitectura institucional resultante del DNU 941/2025 procura separar formalmente dos funciones que históricamente coexistieron dentro de estructuras vinculadas

al Sistema de Inteligencia Nacional: por un lado, la ciberseguridad entendida como protección del ciberespacio de interés nacional, de las infraestructuras críticas y de los activos digitales estratégicos del Estado; y por otro, la ciberinteligencia, vinculada a la producción de inteligencia sobre amenazas, actores y operaciones en el entorno digital.

Sin embargo, la sola separación formal de competencias no agota los interrogantes institucionales que plantea el nuevo esquema. Por el contrario, la ausencia de información pública suficiente sobre la transferencia efectiva de capacidades técnicas, personal especializado, plataformas, accesos, licencias, repositorios, sistemas críticos y herramientas de monitoreo torna imprescindible el ejercicio pleno del control parlamentario respecto de los alcances reales de dicha reorganización.

Ello resulta particularmente relevante si se considera que el CNC fue conformado, en buena medida, a partir de estructuras previamente insertas dentro del Sistema de Inteligencia Nacional, con personal técnico formado bajo regímenes especiales de inteligencia, acceso a información sensible y capacidades tecnológicas cuyo alcance real no ha sido suficientemente explicitado ante el Congreso de la Nación ni ante la ciudadanía.

Los artículos 31 y 33 del DNU 941/2025 constituyen probablemente el núcleo más sensible de toda la reorganización institucional dispuesta por el Poder Ejecutivo Nacional.

El artículo 31 establece la transferencia al Centro Nacional de Ciberseguridad de "los bienes muebles, activos, patrimonio, compromisos, derechos y obligaciones" asignados a la ex Agencia Federal de Ciberseguridad y vinculados "exclusivamente" a funciones relacionadas con ciberseguridad. Por su parte, el artículo 33 dispone que la propia Secretaría de Inteligencia de Estado coordinará el proceso de reasignación del personal proveniente de dicha estructura.

La formulación normativa elegida por el decreto presenta múltiples zonas de indeterminación que justifican plenamente el presente pedido de informes. La utilización de expresiones abiertas y no delimitadas —como "funciones relacionadas exclusivamente con ciberseguridad"— impide conocer con precisión cuáles fueron los criterios utilizados para decidir qué plataformas, sistemas, bases de datos, contratos, licencias, herramientas de monitoreo, repositorios documentales o capacidades técnicas debían permanecer dentro del Sistema de Inteligencia Nacional y cuáles debían ser transferidos hacia la órbita civil del CNC.

La ausencia de publicidad respecto de esos criterios no constituye un problema meramente administrativo. Se trata de una cuestión central desde el punto de vista republicano, institucional y democrático. Cuando el Estado reorganiza estructuras vinculadas a inteligencia, monitoreo tecnológico, protección de infraestructuras críticas y procesamiento

masivo de información, resulta indispensable que existan mecanismos claros de delimitación funcional, trazabilidad institucional y control parlamentario efectivo.

La preocupación se profundiza si se considera que la propia SIDE conserva, conforme el decreto, la coordinación del proceso de transferencia y reasignación de capacidades. En otras palabras: el organismo históricamente ubicado en la cúspide del Sistema de Inteligencia Nacional mantiene un rol decisivo en la determinación concreta de qué recursos, herramientas, plataformas y capacidades permanecerán bajo su órbita y cuáles pasarán al nuevo organismo civil.

El proceso de transferencia involucra, además, no solamente bienes materiales o infraestructura tecnológica, sino también personal especializado, habilitaciones de seguridad, conocimiento técnico acumulado, accesos operativos y redes funcionales construidas históricamente dentro de estructuras de inteligencia.

Buena parte del personal técnico proveniente de la ex Agencia Federal de Ciberseguridad fue formado bajo esquemas de compartimentación, confidencialidad y habilitación propios de la Ley 25.520. Ello plantea interrogantes relevantes respecto del régimen jurídico actualmente aplicable, las eventuales dobles dependencias funcionales, la continuidad de accesos a sistemas sensibles y la existencia de mecanismos efectivos de trazabilidad y control institucional.

La cuestión adquiere aún mayor relevancia si se considera que el CNC podría eventualmente operar sobre sistemas críticos del Sector Público Nacional, intervenir ante incidentes de seguridad informática de gran escala y administrar capacidades técnicas potencialmente aptas para el monitoreo, correlación y procesamiento automatizado de grandes volúmenes de información estatal.

Por ello, el Congreso de la Nación no puede permanecer ajeno al modo concreto en que dicha reorganización se encuentra siendo implementada.

Otro de los aspectos centrales que justifican el presente pedido de informes reside en la necesidad de conocer cuál es la infraestructura tecnológica real sobre la que actualmente opera el Centro Nacional de Ciberseguridad y cuáles son los mecanismos implementados para garantizar soberanía, integridad, trazabilidad y control efectivo sobre la información sensible eventualmente administrada por dicho organismo.

En el escenario contemporáneo de ciberseguridad estatal, las capacidades tecnológicas no dependen únicamente del equipamiento físico disponible dentro de organismos públicos. Una parte sustancial de la infraestructura digital utilizada para monitoreo, almacenamiento, procesamiento, análisis de amenazas, correlación de eventos y

respuesta ante incidentes puede encontrarse tercerizada, externalizada o alojada en infraestructuras cloud administradas por proveedores privados nacionales o extranjeros.

Precisamente por ello, resulta imprescindible determinar si el CNC utiliza infraestructura cloud propia, estatal, híbrida o provista por terceros privados; cuáles son las empresas involucradas; bajo qué jurisdicción se almacenan o procesan los datos; qué mecanismos de cifrado y trazabilidad existen; y qué grado de acceso poseen terceros privados respecto de información sensible vinculada a organismos públicos nacionales.

La cuestión no es menor. En materia de ciberseguridad estatal, infraestructura crítica y protección de datos, la externalización tecnológica puede generar riesgos significativos en términos de soberanía digital, confidencialidad, dependencia tecnológica y control efectivo sobre la información estratégica del Estado.

La utilización de proveedores privados para servicios de monitoreo, almacenamiento, análisis forense, threat intelligence, correlación de eventos, administración de plataformas críticas o procesamiento de grandes volúmenes de datos exige mecanismos particularmente rigurosos de auditoría, supervisión y control democrático. Ello resulta especialmente relevante cuando la información potencialmente involucrada incluye datos personales, biométricos, sanitarios, financieros, registrales o vinculados a infraestructuras críticas.

Asimismo, corresponde conocer si empresas privadas proveedoras de servicios tecnológicos o de ciberseguridad poseen actualmente acceso, administración, procesamiento, almacenamiento o alojamiento de información estratégica vinculada al Sector Público Nacional y cuáles son los límites jurídicos, técnicos y contractuales que regulan dicha intervención.

La ausencia de información pública suficiente sobre estos aspectos impediría evaluar adecuadamente los riesgos institucionales derivados de eventuales esquemas de tercerización tecnológica o dependencia de proveedores privados en áreas particularmente sensibles para la seguridad estatal.

El CNC quedó formalmente operativo con la designación de sus autoridades en febrero de 2026. Apenas semanas después, comenzaron a conocerse públicamente incidentes de enorme gravedad vinculados con filtraciones masivas de información perteneciente a organismos nacionales, provinciales y entidades públicas.

Entre marzo y abril de 2026, el colectivo identificado públicamente como "Chronus Team" habría ejecutado operaciones coordinadas de filtración de información que afectaron —según reportes públicos y comunicaciones parciales— al Ministerio de Salud de la Nación, al Ministerio de Seguridad Nacional, a la Jefatura de Gabinete de Ministros, al

Banco Central de la República Argentina, a la Corte Suprema de Justicia, a la Gendarmería Nacional, al Instituto de Obra Médico Asistencial (IOMA) y a la Obra Social de Empleados Públicos (OSEP), entre otros organismos.

La dimensión de dichos incidentes excede ampliamente el plano técnico. Lo que se encuentra comprometido en estos casos no es únicamente la integridad de sistemas informáticos estatales, sino también la seguridad de datos personales, información sanitaria, registros públicos, bases biométricas, credenciales, documentación sensible y activos críticos pertenecientes al Estado Nacional.

A ello se suman antecedentes persistentes vinculados al Registro Nacional de las Personas (RENAPER), cuyos datos personales, fotografías y registros biométricos han circulado reiteradamente en mercados ilícitos y plataformas digitales desde el año 2021, evidenciando graves problemas estructurales en materia de protección de información sensible.

En todos estos casos, la cuestión central no reside solamente en la identificación de los responsables materiales de los ataques o filtraciones, sino en la calidad de la respuesta institucional desplegada por el Estado Nacional.

Resulta indispensable conocer si el CNC emitió alertas tempranas, qué mecanismos de monitoreo y detección poseía al momento de los incidentes, qué acciones de contención y mitigación fueron implementadas, qué informes técnicos se produjeron, qué organismos fueron efectivamente asistidos y cuál fue la articulación existente con la Agencia de Acceso a la Información Pública, el Ministerio Público Fiscal, la UFECI y los organismos afectados.

Asimismo, corresponde determinar si las obligaciones legales de notificación previstas en la Ley 25.326 y en la normativa de protección de datos personales fueron efectivamente cumplidas respecto de los ciudadanos potencialmente afectados por dichas filtraciones.

La articulación entre el CNC, como autoridad técnica, y la Agencia de Acceso a la Información Pública, como autoridad de protección de datos personales, resulta esencial para una respuesta estatal coherente frente a incidentes de esta naturaleza. La ausencia de mecanismos formales, protocolos claros o circuitos de coordinación institucional entre ambos organismos constituiría una grave deficiencia institucional que este Cuerpo tiene el deber de conocer y, en su caso, subsanar mediante los instrumentos normativos y de control parlamentario a su disposición.

El artículo 100 inciso 11 de la Constitución Nacional faculta al Jefe de Gabinete de Ministros a concurrir al Congreso de la Nación e informar sobre la marcha del

gobierno. El artículo 101 establece asimismo la obligación de concurrencia periódica para brindar información respecto de la gestión estatal. En ejercicio de esas facultades de control, y de conformidad con lo dispuesto por el artículo 75 inciso 32 de la Constitución Nacional y el artículo 204 del Reglamento de la Honorable Cámara de Diputados de la Nación, este Cuerpo se encuentra plenamente habilitado para requerir información sobre el funcionamiento de organismos del Poder Ejecutivo Nacional, incluyendo aquellos creados mediante decretos de necesidad y urgencia.

El control parlamentario sobre organismos creados mediante DNU adquiere particular relevancia en virtud de lo dispuesto por el artículo 99 inciso 3 de la Constitución Nacional y por la Ley 26.122, que establece el régimen de control legislativo sobre los decretos de necesidad y urgencia. La Comisión Bicameral Permanente prevista en dicha ley y la Comisión Bicameral Permanente de Fiscalización de los Organismos y Actividades de Inteligencia poseen competencia concurrente respecto de los actos derivados del DNU 941/2025, en tanto involucra la reorganización de estructuras vinculadas al Sistema de Inteligencia Nacional.

Asimismo, la Ley 27.275 de Derecho de Acceso a la Información Pública consagra el principio de máxima divulgación y la presunción de publicidad de toda información producida u obtenida por el Estado. El presente pedido de informes se enmarca también en ese régimen jurídico, que obliga a los organismos públicos a suministrar la información requerida salvo configuración expresa, fundada y excepcional de alguna causal legal de reserva.

La reorganización de capacidades provenientes del Sistema de Inteligencia Nacional hacia estructuras de ciberseguridad civil exige mecanismos reforzados de transparencia, trazabilidad institucional y control democrático. En ausencia de información pública suficiente sobre la transferencia de recursos, plataformas, personal especializado, herramientas de monitoreo y capacidades técnicas sensibles, el riesgo institucional no reside únicamente en eventuales deficiencias operativas, sino también en la posible consolidación de zonas grises entre inteligencia estatal, monitoreo tecnológico y administración masiva de información sensible perteneciente a millones de ciudadanos.

En un Estado constitucional de derecho, la protección del ciberespacio y de las infraestructuras críticas no puede desarrollarse al margen de los principios republicanos de publicidad de los actos de gobierno, división de poderes, control parlamentario y tutela efectiva de los derechos fundamentales.

La creación del Centro Nacional de Ciberseguridad constituye una decisión institucional de enorme alcance que involucra la reorganización de capacidades técnicas sensibles, la transferencia de patrimonio y personal proveniente del sistema de inteligencia

hacia la órbita civil y la asunción de responsabilidades primarias en materia de protección de datos, infraestructuras críticas y seguridad digital del Estado Nacional.

La magnitud de los incidentes ocurridos durante los primeros meses de funcionamiento del organismo, sumada a la ausencia de información oficial sistemática sobre las capacidades reales del nuevo esquema institucional y sobre la respuesta efectivamente desplegada frente a filtraciones masivas de información pública, torna imprescindible el ejercicio pleno de las facultades de control que la Constitución Nacional y el Reglamento de esta Honorable Cámara confieren a los señores Diputados y señoras Diputadas de la Nación.

Por las razones expuestas, solicito a mis pares el acompañamiento del presente proyecto.

Pablo JULIANO